Robert Gehring - Digitale Signaturen

Hinweise zu Form und Inhalt

Am Anfang dieser Arbeit stand die Idee, meine Diplomarbeit in einer Hypertextstruktur darzustellen. Diese sollte im Internet oder oder/und auf einer CD im HTML-Format gespeichert zugänglich gemacht werden. Dadurch sollte den vielfältigen Aspekten des Themas eine passende, moderne Form gegeben werden.

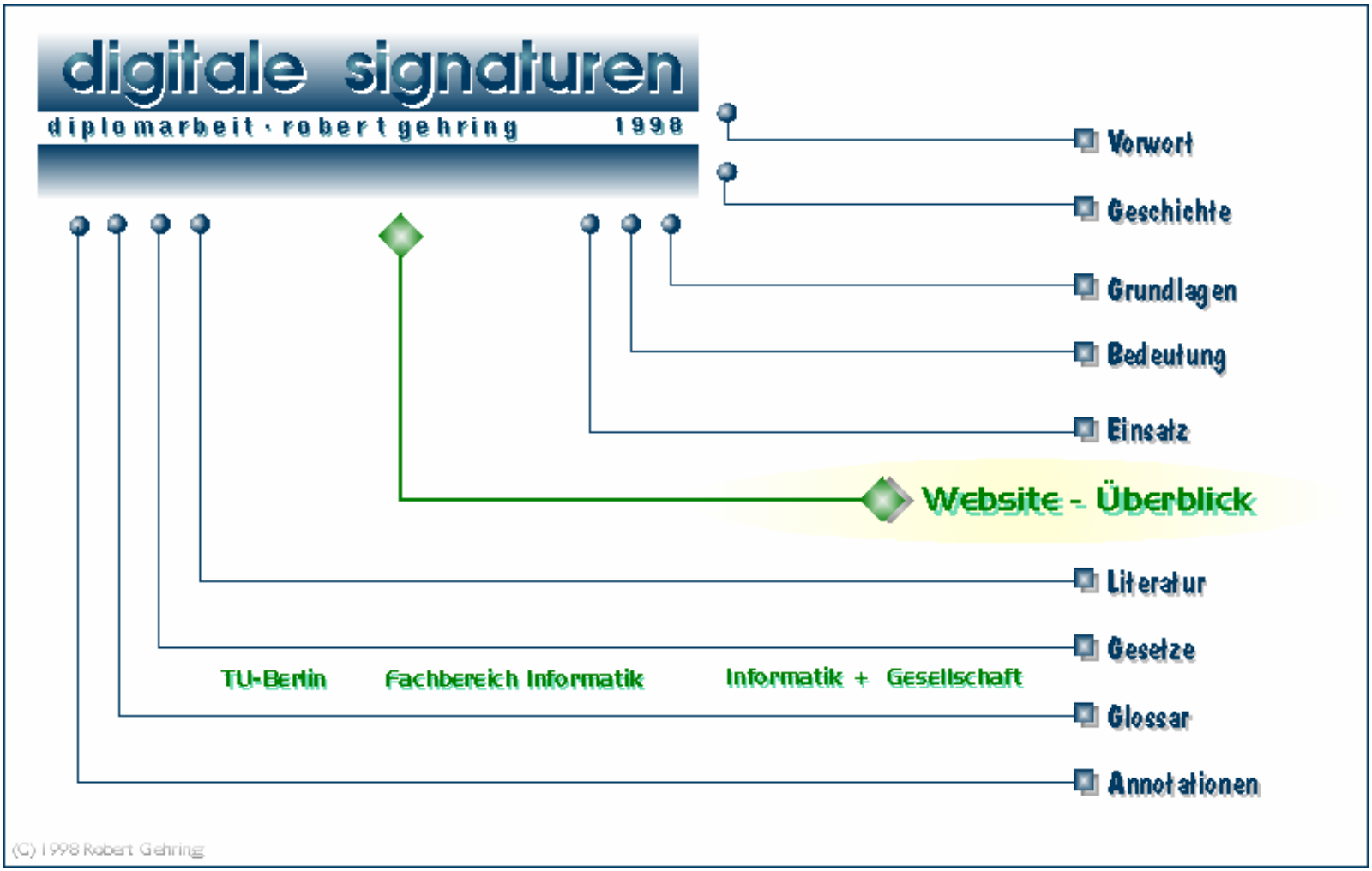
Leider verträgt sich dieser Ansatz nicht mit den meisten Diplomprüfungsordnungen, insbesondere nicht mit der DPO des Fachbereichs Informatik der TU Berlin. Dort wird eine papierne, fest gebundene Form gefordert. Der Versuch, eine Ausnahme zu erwirken, scheiterte.

Das hatte Auswirkungen auf die Form der Arbeit. So, wie sie hier vorliegt, war sie nicht geplant. Um sie in einer akzeptablen Form ausdrucken zu koennen, wurde sie aber so realisiert. Die notwendigen, schmerzlichen Einschränkungen lassen sich nicht übersehen.

Es ist vorgesehen, diese Arbeit weiterzuentwickeln. Dabei wird das vorgesehene Konzept umgesetzt werden.

Robert Gehring, 8. April 1998

Zur vorliegenden Version der Arbeit


digitale signaturen
diplomarbeit · robert gehring 1998
Vorwort
Geschichte
Grundlagen
Bedeutung
Einsatz
Website - Überblick
Literatur
Gesetze
TU-Berlin
Fachbereich Informatik
Informatik + Gesellschaft
Glossar
Annotationen
(C) 1998 Robert Gehring

Gedanken, angeregt durch Walter Benjamins Schrift:

> **``Das Kunstwerk im Zeitalter seiner technischen Reproduzierbarkeit''**

Zusammenfassung eines Internet-Artikels von http://www.cyberlaw.com zum RSA-Patent:

> **``Using the RSA Algorithm for Encryption and Digital Signatures: Can You Encrypt, Decrypt, Sign and Verify without Infringing the RSA Patent?''**

Eine kleine Presseschau zu den Themen:

> **Digitale Signaturen, Verschlüsselung, Abhören etc.**

Annotation
digitale signaturen
diplomarbeit · robert gehring

Betrachtungen, angeregt durch Walter Benjamins Schrift

``Das Kunstwerk im Zeitalter seiner technischen Reproduzierbarkeit''

von Robert Gehring

Im Jahre 1936 erschien eine Schrift mit dem auf den ersten Blick befremdlich anmutenden Titel ``Das Kunstwerk im Zeitalter seiner technischen Reproduzierbarkeit''. Autor der Schrift: Walter Benjamin. Inhalt: Schwierig zu beschreiben, was eigentlich darin steht. Es geht um Kunst und deren Wahrnehmung; um die mediale Funktion der Kunst; um Sinneswandel; um mehr. Es ist eines von jenen Stücken wissenschaftlicher Literatur, die immer neu gelesen und verstanden werden wollen. Das heißt: 1936 war es anders zu interpretieren als 1996. Aber zu beiden Zeiten war es interpretierbar und nicht bloß noch für Historiker von Interesse. Kurz gesagt, ist es eine *aktuelle* Schrift[1].

Vor über 60 Jahren geschrieben, finden sich darin Ideen, die erst jetzt - im Zeitalter des Internet - verständlich zu werden scheinen. Es fällt schwer zu sagen, daß Walter Benjamin das Internet bereits antizipiert hätte. Dem ist wohl nicht so. Allerdings hat er gespürt [2] und erkannt, daß technische Medien [3] ihre Inhalte grundsätzlich verändern, insofern die Inhalte einen Charakter haben, der primär nichttechnischen Ursprungs ist. Auch bringen sie neue, eigenständige Inhalte hervor, die von ihrer Natur aus auf einen technischen Gebrauch hin gestaltet sind [4]. Ihre Gestalt ist eine technische, der Umgang mit ihnen ein technischer und ihre Existenz ohne die Technik nicht denkbar. Mit Nietzsche könnte man von neuen, technischen, insbesondere elektronischen Medien sagen, daß sie eine ``Umwertung aller ihrer Werte'' erzwingen.

Walter Benjamin geht vom Kunstwerk aus. Nun läßt sich ein Kunstwerk allgemeiner als Werk verstehen, d.h. als Gegenstand menschlichen Handelns. Die Besonderheit des Kunstwerkes gegenüber dem Werk, das nicht Kunst ist, könnte vielleicht darin gesehen werden, daß ein Kunstwerk nicht notwendig einem Zweck dienen muß, während wir von Gebrauchsgegenständen eine Zweckdienlichkeit sehr wohl erwarten. Bei der Frage nach dem Sinn kehrt sich das Verhältnis oft um.

Beide Kategorien ähneln sich darin, daß die ihnen zugehörigen Werke der menschlichen Rezeption unterworfen sind. Dies ist zuerst die Rezeption des Schöpfers, danach ggf. die des Adressaten. Im Prozeß und im Resultat dieser Rezeption bildet sich ein Verhältnis des Rezipienten zum Werk heraus. Bei einem Kunstwerk kann dies Genuß oder Ablehnung sein, bei einem Gebrauchswerk (Ich möchte diesen Begriff in Analogie zum `Kunstwerk' wählen.) wird es in der Regel der Einsatz oder der Nichteinsatz des Werkes sein.

Einen ganz wesentlichen Unterschied zwischen Kunstwerk und Gebrauchswerk sieht Benjamin in der Einzigartigkeit eines Kunstwerkes.

> *``Das Hier und Jetzt des Originals macht den Begriff seiner Echtheit aus.''*

Ein Kunstwerk ist echt, wenn es einmalig ist. Ist es einmalig, so befindet es sich zu einem bestimmten Zeitpunkt an einem bestimmten Ort und nicht gleichzeitig irgendwo anders. Diese Einmaligkeit eines Kunstwerkes ist jedoch nur gegeben, wenn es seiner Natur nach nicht reproduzierbar ist.

> *``Der gesamte Bereich der Echtheit entzieht sich der technischen - und natürlich nicht nur der technischen - Reproduzierbarkeit."*

Diese Echtheit läßt sich nachweisen. Imitate, Fälschungen, Reproduktionen lassen sich - ggf. mit hohem Aufwand - feststellen.

> *``Die Echtheit einer Sache ist der Inbegriff alles von Ursprung her an ihr Tradierbaren, von ihrer materiellen Dauer bis zu ihrer geschichtlichen Zeugenschaft. Da die letztere auf der ersteren fundiert ist, so gerät in der Reproduktion, wo sich die erstere dem Menschen entzogen hat, auch die letztere: die geschichtliche Zeugenschaft der Sache ins Wanken."*

All' dies läßt sich nicht nur von Kunstwerken, sondern vielmehr von allen Werken mit originärer Natur feststellen. Von einer Geburtsurkunde gibt es ebenso nur ein Original wie von Dürers Bild der Mutter. Erst wenn ein Werk so geschaffen wird, daß es reproduzierbar sein soll, wenn es also zum Gegenstand einer technischen Produktion, zum Produkt gerät, wird der Anspruch auf Echtheit im Sinne eines Originals aufgegeben. Zurück bleiben -vielleicht- eine originäre Idee und ein Werk im Zustand der Verfügbarkeit. Das trifft für beide, Kunstwerke und Gebrauchswerke, zu.

> *``Die Reproduktionstechnik, so ließe sich allgemeiner formulieren, löst das Reproduzierte aus dem Bereich der Tradition ab. Indem sie die Reproduktion vervielfältigt, setzt sie an die Stelle seines einmaligen Vorkommens sein massenweises. Und indem sie der Reproduktion erlaubt, dem Aufnehmenden in seiner jeweiligen Situation entgegenzukommen, aktualisiert sie das Reproduzierte."*

Im ``*Zeitalter der Reproduzierbarkeit*" wird von den Ideen dann verlangt, daß sie zu reproduzierbaren Werken führen oder selbst reproduzierbar sind. Ansonsten sind sie unproduktiv. In diesem Sinne wundert es nicht, wenn Handlungen zu Produkten werden. Dienstleistungen sind Produkte, kann man den Werbeprospekten der Banken und Versicherungen entnehmen. Wir leben in einer *Dienstleistungsgesellschaft* , in der alle Handlungen zu Produkten gerinnen. Diejenigen Handlungen, die sich dem widersetzen, werden zum Problem. [5]

Produkte sind reproduzierbar. Handlungen, die Produkte sind, sind reproduzierbar. Sie können überall, zu jeder beliebigen Zeit, vollbracht werden. Sie können eben auch jederzeit an jeden Ort gebracht werden. Dafür kennen wir das Wort von der Globalisierung.

Wie die Produktion sich allerorten ansiedeln kann, können die Produkte durch ihre Verfügbarkeit alle Kulturen durchdringen. Mit der elektronischen Reproduzierbarkeit des Wissens, der die mechanische Reproduzierbarkeit vorausgegangen war, der Buchdruck, gelangen fast alle Kulturen in den Einflußbereich fast aller Ideen. Dies um so mehr, je besser sich das jeweilige Wissen und die Ideen elektronisch repräsentieren, sprich reproduzieren lassen. Es kann daher kein Zufall sein, daß in einer Welt, in der die Computer höchstens 256 Zeichen, bevorzugt das englische Alphabet, darstellen, chinesische Texte exotisch, englische dagegen normal sind. Die Anzahl der Chinesen ist jedoch deutlich größer als die Anzahl der Engländer, Amerikaner und Australier zusammen.

> *``Diese ... Prozesse führen zu einer gewaltigen Erschütterung des Tradierten - einer Erschütterung der Tradition, die die Kehrseite der gegenwärtigen Krise und Erneuerung der Menschheit ist."*

Die ungleiche Widerspiegelung von reproduktionsgeeigneten Ideen und solchen, die sich sperren, führt in der Folge zu einer gesteuerten Wahrnehmung. Der Wahrnehmungsapparat wird durch die Anzahl und die Intensität der Wahrnehmungen geprägt, haben Neurobiologie und Neurophysiologie belegt. So entstehen wiederum Präferenzen, welche die Aufmerksamkeit in die Richtung lenken, wo sie Bestätigung finden. Bedürfnisse nach einer spezifischen Art der Wahrnehmung bilden sich heraus.

`Unproduktive' Ideen sind immer seltener sichtbar als solche mit produktiven Ergebnissen. In der Folge werden sie nicht mehr `gern' gesehen. Ideen, an denen nur wenige teilhaben können, fallen mehr und mehr aus dem gesellschaftlichen Blickfeld heraus.[6]

Dagegen rücken solche Ideen stärker in den Mittelpunkt, die in ihrem Wesensgehalt geeignet sind, in vielen Medien dargestellt zu werden. Sie dürfen dazu weder an spezielle Formen noch an spezielle Inhalte gebunden sein. Auch müssen sie von Mediendarstellung zu Mediendarstellung leicht assoziierbar sein. Es fördert ihre Akzeptanz, wenn sie die Beziehungen der

Menschen, die das jeweilige Medium verbindet, nicht in Frage stellen.

> *``Innerhalb großer geschichtlicher Zeiträume verändert sich mit der gesamten Daseinsweise der menschlichen Kollektiva auch die Art und Weise ihrer Sinneswahrnehmung. Die Art und Weise, in der die menschliche Sinneswahrnehmung sich organisiert - das Medium, in dem sie erfolgt - ist nicht nur natürlich sondern auch geschichtlich bedingt."*

> *``In dem Maße, in dem die Medien kommunikative Bedürfnisse befriedigen und zur sozialen Kommunikation beitragen, prägen sie das gesellschaftliche Leben und das Leben des einzelnen. Wenn sich die Medien verändern, betrifft dies auch den einzelnen und die Gesellschaft."* [7]

Mit der Ausbreitung der Medien auf Bereiche, die bisher ohne Medium auskamen, breiten sich Ideen aus, die nicht ohne Medien auskommen. Verdrängt werden Ideen, die nur ohne Medium nachvollziehbar sind.

Ideen sind jedoch die Voraussetzungen zum -bewußten- Handeln. Erfahrungen sind die Folgen der Wahrnehmung des -bewußten- Handelns.

Handeln in technischen Zusammenhängen führt zu technikabhängigen Erfahrungen. Zur Beherrschung der Technik ist ein technisches Verständnis unabdingbare Voraussetzung. In diesem Sinne stimulieren die Erfahrungen die mentalen Voraussetzungen. Die Perspektive der Wahrnehmung verschiebt sich immer stärker hin zu einer technischen. Bestätigung für die Erfahrung findet sich dann am ehesten in neuerlicher Betätigung im technischen Umfeld.

> *``Das reproduzierte Kunstwerk wird in immer steigendem Maße die Reproduktion eines auf Reproduzierbarkeit angelegten Kunstwerkes."*

Nun weisen nicht alle Handlungen die gleichen Qualitäten auf. Grundsätzlich lassen sich schöpferische und konsumierende Handlungen unterscheiden. Stehen diese nicht in direkter Folge, so bedürfen sie eines vermittelnden Mediums, das aufgrund seiner gegebenen Beschränkungen auch als eine Art `Filter' wirksam wird. [8] In der vermittelnden und der Filterwirkung begründet, liegt die zunehmende Distanzierung der konsumtiven von den kreativen Handlungen. Dies gilt in der Regel sowohl räumlich als auch zeitlich. Eine solche Distanzierung führt zwangsläufig zu einem Bewußtseinswandel. Anders könnte man sagen, daß ein Traditionsverlust eintritt.

Walter Benjamin spricht auf dem Gebiet der Kunst von einer *``Säkularisierung der Kunst"*, bei der die *``Authentizität"* an die Stelle des *``Kultwertes"* trete. Übertragen würde ich folgende Aussage machen:

Mit der zunehmenden Säkularisierung menschlichen Handelns tritt die Authentizität an die Stelle der Intention und Konsequenz.

Wie ist das gemeint? Wurden die menschlichen Handlungen bisher in der Hauptsache nach ihrer Zweckmäßigkeit oder ihrer Sinnfälligkeit beurteilt, erhalten sie zunehmend Wert dadurch, *daß sie verrichtet und die Verrichtung festgehalten wird, um vermittelt zu werden* [9]. Ob sie zu dem intendierten Ergebnis führen, d.h. zweckmäßig sind, bzw. ob sie eine intendierte Aussage repräsentieren, d.h. sinnvoll sind, tritt demgegenüber in den Hintergrund. Wichtig wird immer mehr, daß eine Handlung vorgenommen wurde und von wem. Die Einmaligkeit und Bedeutung einer Handlung werden immer stärker an der Person des Verrichtenden und an den Umständen der Verrichtung und nicht mehr an ihren Ergebnissen festgemacht.

Lassen sich diese Aussagen belegen? Detaillierte empirische Untersuchungen kann ich nicht anführen. Einige Ereignisse sprechen jedoch für diese These. Da wäre zum einen die Ausweitung der Wirkungen des Urheberrechts und des Patentrechts in einem Sinne, der den Zielsetzungen ihrer Schöpfer zuwiderlaufen. So wurde im Zuge der Rechtsvereinheitlichung in der EU die Forderung nach einer besonderen Qualität eines Werkes als Voraussetzung zur Urheberrechtsfähigkeit aus dem Urheberrecht entfernt. Wie, um den Wandel zu unterstreichen, wurde eine Forderung eingeführt, daß eine Beurteilung nicht nach z.B. ästhetischen Kriterien vorzunehmen ist. Auch werden bloße Ansammlungen vom neuen Urheberrecht geschützt. Prognose: Bald ist jede Handlung vom Urheberrecht geschützt, so banal sie auch sein möge.

Ich will einige konkrete Beispiele anführen.

> Man denke beispielsweise an die `Reichstagsverhüllung' in Berlin durch Christo und seine Frau. Die Handlung wurde im öffentlichen Raum, am öffentlichen Gegenstand vorgenommen. Ihre Bedeutung erhalten hat sie durch die Anwesenheit der Öffentlichkeit und den Symbolcharakter des öffentlichen Gegenstandes. Vollzogen wurden die Handlungen nach der Regie von Christo und Frau durch andere Personen. Nichtsdestotrotz konnten sich Christo und Frau per Gerichtsbeschlußsämtliche Rechte an der Handlung sichern. Alle Rechte zur Verwertung, z.B. der Filmaufnahmen von den Feiern am verhüllten Gebäude, stehen Christo und Frau zu. Der Öffentlichkeit, als Mitschöpfer des Ereignisses, stehen keine Rechte zu.
>
> In Berlin gibt es zwei Zoos: Den Tierpark und den Zoologischen Garten. Auf der Eintrittskarte des Tierparks findet sich ein Aufdruck, der besagt, daßFotografieren erlaubt sei. Es folgt der Hinweis, daßdie Urheberrechte an den Fotos allerdings beim Tierpark liegen würden. Provozierend könnte man frage, ob das auch für die Wolken über dem Tierpark gilt. Eine Eintrittskarte für den Zoo habe ich nicht zur Hand.
>
> Ähnliche Absichten hegt man offensichtlich in der Toscana, wo sich die Kommunalpolitiker die Urheberrechte an der Landschaft, die ja schließlich durch die Bevölkerung gestaltet wurde, sichern wollen (siehe ZEIT*Punkte*``Copyright").
>
> Einen großen Teil der Gesetzgebung, die sich den sogenannten ``neuen Medien" widmet, machen Ausweitungen des Urheberrechtes aus (Siehe dazu: Multimediagesetz, Änderungen des Urheberrechtsgesetzes).
>
> Ein anderes Beispiel gibt die Patentierung von Algorithmen ab, die in den USA und z.B. auch in der Schweiz bereits gängige Praxis ist. So ist der wichtigste Algorithmus für Verfahren zur Erzeugung digitaler Unterschriften, RSA, in den USA und der Schweiz patentiert. Bis vor wenigen Jahren noch galt die Regel, daßIdeen nicht patentierbar seien. Sie genossen `bloß' den Schutz des Urheberrechts. Diese Regel gilt nicht mehr. So werden die Interessen der Ideenlieferanten als wesentlich, die Konsequenzen für die Gesellschaft als unwesentlich bewertet.
>
> Weiterhin würde ich die großen `Marken' anführen. Produkte werden unter dem Symbolwert ihrer Marke, nicht mehr unter ihrem Produktwert, gehandelt. So werden sie ideologiefrei und setzen sich nicht dem Widerstand lokaler Kulturen aus. [10]
>
> Wurde Coca Cola in den 50'er Jahren noch als Symbol des `American Way of Life' verstanden, gilt sie heute als Ausdruck einer globalen Kultur. Damit gibt es kein Problem, wenn `Coke' z.B. in China produziert, verkauft und beworben werden soll. Dies bestätigt dann wiederum den Charakter der universellen Marke. Im Vorteil sehen sich diejenigen Produzenten, deren Marken kulturunabhängig und ortsunabhängig sind. Es wundert dann nicht mehr, daßso viel Geld in eine Werbung fließt, die ein Image in diesem Sinne aufbauen soll. [11]

In Benjamins Sinne mache ich den Begriff der `Säkularisierung' an der Loslösung aus dem konkreten Bedeutungszusammenhang mit dem Ziel und Resultat der Reproduzierbarkeit fest. Unter `Authentizität' verstehe ich hier die Zuordnungsbarkeit (Zuordnung) von Handlungen zu Handelnden unter weitgehender Vernachlässigung der Hintergründe und Konsequenzen der Handlung. Daraus folgt die Aufwertung einer Handlung, die reproduzierbar ist (gegenüber ihren Folgen und ggü. einer Handlung, die nicht reproduzierbar ist), denn eine solche kann beliebig oft vermarktet werden. Die Frage nach der Echtheit, die sich bei einem Kunstwerk noch stellt, tritt dagegen völlig in den Hintergrund.

> *``Mit der Emanzipation der einzelnen Kunstübungen aus dem Schoße des Rituals wachsen die Gelegenheiten zur Ausstellung ihrer Produkte."*

In Fußnote 12 zitiert Benjamin Brecht:

> *``Ist der Begriff Kunstwerk nicht mehr zu halten für das Ding, das entsteht, wenn ein Kunstwerk zur Ware verwandelt ist, dann müssen wir vorsichtig und behutsam, aber unerschrocken diesen Begriff weglassen, wenn wir nicht die Funktion dieses Dinges selber mitliquidieren wollen, ..."*

Gleiches gilt für jegliches Werk. Deutlich wird es jedoch insbesondere beim Kunstwerk und bei der alltäglichen Handlung, die jedem vertraut ist.

Die Frage, die im Raum stehen bleibt, ist die nach den Schlußfolgerungen und nach den Konsequenzen. Darüber haben sich schon viele Gedanken gemacht.

Walter Benjamin sah es so:

> ``*Die Menschheit, die einst bei Homer ein Schauobjekt für die Olympischen Götter war, ist es nun für sich selbst geworden.''*

Millionen privater Homepages im Internet scheinen ihm Recht zu geben. Dutzende Talkshows ebenfalls.

Fußnoten

[1] Walter Benjamin verwendet z.B. ein Wort, das in den letzten Jahren in der Sprache und im Denken einen herausgehobenen Platz gefunden hat: *virtuell*.

> ``*Wenn in der Lithographie virtuell die illustrierte Zeitung verborgen war, so in der Photographie der Tonfilm.''*,

so Walter Benjamin. Ohne explizit von *virtueller Realität* zu sprechen, meint er doch eine solche. Ist etwas *virtuell* verborgen, so ist es auch *virtuell* real. Heute kehrt sich das Verhältnis an vielen Stellen um: Es wird von virtueller Realität gesprochen, wo sie doch gar nicht gemeint ist.

Man kann an dieser Stelle auch auf den Unterschied zwischen *Realität*, das vom lateinischen res = Ding abstammt, und *Wirklichkeit* , in dem das Wirken steckt, hinweisen.

---

[2] Es gibt mindestens noch drei Personen, die ein ähnliches Gespür bewiesen haben: Bertolt Brecht mit seiner Radiotheorie, die vor Benjamins Arbeit entstanden ist, und Marshall McLuhan, dessen ``Understanding Media'' in den 60'er Jahren verfaßt wurde. Der Dritte war Andy Warhol, ebenfalls in den 60'er Jahren, der die Entwicklung der Kunst als eine hin zur *(Er)lebbarkeit* erfaßte.

> ``*Das ist der Sinn des Showbusiness - der Beweis, daß es völlig egal ist, wer du bist; wichtig ist nur, was sie denken, das du bist.''*
>
> [Warhol 1997]
>
> ``*Im gegenwärtigen Zeitalter der Elektrizität erleben wir, wie wir immer mehr in die Form der Information verwandelt werden und einer technischen Erweiterung des Bewußtseins entgegengehen.''*
>
> [McLuhan 1992]

---

[3] Abzugrenzen, was ein Medium ist und was nicht, gelingt nicht ohne weiteres. Geht man vom Wort aus -Medium-, so bedeutet dieses `Mittler'. Als solches vermittelt es etwas , auf eine bestimmte Art und Weise, zwischen Personen. Man könnte sagen, ein Medium setzt die Beteiligten (WER) in spezifischer Form (WIE) vermittels seines Inhaltes (WAS) zueinander in Beziehung. Das Medium kann dabei den Inhalt, die Form oder die Beziehung präferieren, nicht jedoch auf einen dieser Aspekte verzichten. Man sollte nicht versuchen, ein Medium an und für sich zu verstehen. Vielmehr kommt es darauf an, etwas als Medium zu verstehen.

Im konkreten Medium drückt sich eine Präferenz aus. [Man denke hier zum Beispiel an den Begriff *Massenmedium*.] Ein Medium kann seine Qualität ändern, indem es seine Präferenz ändert. Trotz aller möglichen Präferenz läßt es sich aber nur als Einheit verstehen. Man sollte nicht den Fehler machen, das eine mit dem anderen gleichzusetzen. Da ein Bild manchmal mehr sagt als

viele Worte, habe ich mich bemüht, dieses Modell anschaulich zu machen:

Zieht man jetzt noch in Betracht, daß ein Medium Phänomen der menschlichen Wirklichkeit ist, könnte man noch mit Kant das Verhältnis zu Raum und Zeit den Eigenschaften eines Mediums zurechnen. Dabei fällt auf, daß sich der Mensch (das Bewußtsein) von diesen beiden ``*Principien der Erkenntniß a priori*" [*] mittels Medium zu distanzieren (emanzipieren) sucht.

Bleiben wir beim Beispiel *Massenmedium*. Damit ein Medium *Massenmedium* sein kann, muß es in gewisser Weise Grenzen von Raum und Zeit überwinden. Hierbei ist nicht gemeint, die Naturgesetze außer Kraft zu setzen, sondern vielmehr Grenzen im Bewußtsein zu überwinden. Die Teilnehmer an einem *Massenmedium* suchen das Gefühl der Gleichzeitigkeit, das ihnen, die sie sich über große Entfernungen, vielleicht sogar die ganze Welt verteilt befinden, das Gefühl der Verbundenheit, des Miteinanders vermittelt. So wird die räumliche Grenze, die physisch praktisch unüberwindbar ist, medial überwunden:

Ein Medium ist *Massenmedium*, wenn eine genügend große Anzahl Beteiligter überall und gleichzeitig teilhaben können.

> *``Die Dinge sich räumlich und menschlich >>näherzubringen<< ist ein genau so leidenschaftliches Anliegen der gegenwärtigen Massen wie es ihre Tendenz einer Überwindung des Einmaligen jeder Gegebenheit durch die Aufnahme von deren Reproduktion ist."*
>
> *``Es verhält sich wohl so, daß die Sache erst richtig ins Rollen geriet, als die Fotografie aufkam. Dann der Film zu Beginn des zwanzigsten Jahrhunderts. Der Rundfunk. Das Fernsehen. Als die Dinge einen Zug ins Massenhafte bekamen."*
>
> [Bradbury 1981]

Sucht man nach Beispielen in der Gegenwartskultur, so stößt man sofort auf das Prinzessin-Diana-Phänomen und die Sportweltmeisterschaften. Bei diesen könnte man schon von *Globalisierung des Erlebens* sprechen. Offensichtlich werden die Beziehungen präferiert: Zuschauer, Akteur, Fan, Sieger, ...

Ein anderes Beispiel geben die Newsgroups des Internet ab. Dort wird der Inhalt präferiert. Dies drückt sich in der spartanischen Ausstattung der notwendigen Software und den Umgangsformen aus. Um wertvolle Bandbreite für inhaltliche und nicht für formale Zwecke einsetzen zu können, wurde z.T. eine eigene, komprimierte Sprache entwickelt. `CU' und `ROTFL' sind Ausdrücke derselben.

Akzeptiert man das vorgestellte -kurz angerissene- Modell für Medien, so könnte man zur Betrachtung *technischer Medien* übergehen. Haben diese besondere Qualitäten gegenüber nichttechnischen Medien aufzuweisen? Evident ist sicherlich, daß für sie

Raum und Zeit eine geringe Rolle spielen. [Anmerkung: WWW wird zwar oft sarkastisch mit World Wide Wait übersetzt. Das ändert aber nichts an der prinzipiellen Fähigkeit des WWW, Informationen unabhängig von Ort und Zeit zur Verfügung stellen zu können.] So gesehen sind sie besonders als Massenmedien geeignet. Radio und Fernsehen sind die bedeutsamsten Beispiele aus dem Alltag. An der Spitze der Hierarchie finden wir die elektronischen Medien, die sich durch ihre zunehmende Universalität auszeichnen. Das treffendste Beispiel dafür ist das Internet, das sich von China bis Argentinien, von Südafrika bis Island ausdehnt. In dieser Universalität begründet sein dürften auch die Schwierigkeiten, zu sagen, was aus dem Internet werden soll/wird.

Und noch etwas muß auffallen: Elektronische Medien haben keine `**Schwere**'. Die Inhalte technischer Medien sind nicht an konkrete Formen gebunden, noch sind es die Formen an konkrete Inhalte. Auch gibt es keinen spezifischen Teilnehmer-/ Teilhaberkreis. Von Orten gar nicht zu reden. Zwar gibt es eine -technologische- Hemmschwelle. Aber ist diese erst einmal überschritten, zerfließen fast alle Grenzen. Die zunehmende Verschmelzung der Massenmedien liefert Anschauungsobjekte: Fast jede Zeitung ist im Internet präsent. Radio kann man im Internet hören. Das Internet kann per Fernseher oder Mobiltelefon erreicht werden.

Die fehlende **Schwere** bringt viele Vorteile mit sich. Sie erleichtert viele Dinge. Allerdings erleichtert sie uns auch um viele Dinge. Oder sie erschwert diese. So ist es eine ungeheure Erleichterung, wenn man jemanden innerhalb von Sekunden oder Minuten weltweit per Email erreichen kann. Da aber eine elektronische Nachricht geschickt wurde, wird es schwer, deren Empfang zu beweisen. Eine elektronische Empfangsbestätigung ist nichts im Vergleich zu einer Papierquittung mit Unterschrift. [Anmerkung: Siehe dazu auch: [Zimmer 1997]]

Benjamin nennt dies den ``*Verlust der Aura*" .

Der Umgang mit elektronischen Medien erfordert mithin Substitute für gewohnte *Handlungsformen*, da gewohnte *Handlungen* durch neue ersetzt werden. Insofern bringt er sie hervor. Andere, gewohnte Handlungen, fallen weg, mit ihnen ihre Formen. Das gilt prinzipiell für jeden Umbruch, bei dem neue Medien in den Vordergrund rücken. Man denke an den Buchdruck und die Veränderung der Wissens*vermittlung*, die damit einherging. Allein, der räumliche und zeitliche Wirkungskreis dehnt sich bei elektronischen Medien unvergleichlich stärker aus.

[*] Immanuel Kant: Von dem Raume. In: Kritik der reinen Vernunft.

---

[4] Nicht selten entstehen dabei Kulte. Oder wie anders sollte man das weltweite Tamagotchi-Phänomen interpretieren. Alle Handlungen bestehen im Knöpfchendrücken. Interpretiert werden sie als Füttern, Streicheln, Spielen, Reinigen, ... Natürlich finden diese Aktionen nicht wirklich statt. Aber sie dienen der Verwirklichung einer Idee, einer Vorstellung, indem wirkliche Handlungen substituiert werden. Ein Vergleich mit kultischen Handlungen liegt da nahe. Der SPIEGEL spricht vom ``*globalisierten Gefühlshaushalt*'' .

Der SPIEGEL 43/1997, S.152

---

[5] Die TAZ schrieb neulich über einen Artikel über die Krise der Kirchen in Deutschland ``Das „Produkt`` Kirche auf der Suche nach einem neuen Profil. Kundenorientierung erwünscht".

[Jensen 1997]

---

[6] Auf der anderen Seite bilden sich Gruppen heraus, die spezifische Ideen kommunizieren, welche ihrem Inhalt nach mit dem gesellschaftlichen Wissen/Glauben nicht in Beziehung gesetzt werden können. Auch solche Ideen sind unproduktiv, weil nicht vermittelbar. Die Teilhaber an solchen Ideen bilden folglich relativ abgeschlossene Gruppen aus, da nur in solchen die

Kommunikation ohne Medium weitgehend realisierbar ist. Als Beispiele lassen sich Sekten und auch die Kreise von Wissenschaftlern anführen, die ihre Forschungen einem einzigen, sehr konkreten Thema widmen, zu dessen Verständnis hochspezialisierte Kenntnisse vonnöten sind.

> *``Kaum eine andere Wissenschaft hat sich so verästelt wie die Mathematik. Die offizielle Einteilung der American Mathematical Society unterscheidet 3400 Gebiete. Keiner kann da den Überblick behalten. Selbst die fleißigsten Mathematiker kennen sich gerade mal in zwei oder drei Sparten aus. Über ihre Forschung können sie sich nur mit einer Handvoll Spezialisten auf dem Globus austauschen. „Jeder arbeitet mit den Vorabdrucken seiner fünf besten Freunde``, lautet ein Bonmot der Szene."*

[Blum 1997]

---

[7] Zitat aus [Schulz 1997]

---

[8] Niklas Luhmann und Marshall McLuhan haben das z.B. Geld als Medium untersucht.

Geld ermöglicht es, Produktion und Konsumtion strikt zu trennen. Der Trennungsmechanismus ist einfach: Ein Produkt hat einen Wert. Der Produzent wird für das Produkt bezahlt. Der Konsument zahlt für das Produkt. Die Händler nutzen die Distanz und schlagen die Bezahlung ihrer Vermittlungsleistungen auf den Produktpreis auf.

Einige Konsequenzen:

> (1) Der Konsument weißin der Regel nichts mehr vom Produzenten, er hat bloßnoch eine Beziehung zum Händler. Eine direkte Beziehung zwischen Produzent und Konsument besteht nicht mehr.
>
> (2) Ort der Konsumtion und Ort der Produktion fallen auseinander. Zur Verbindung bedürfen sie eines Mediums, das von dem einen wie dem anderen unabhängig ist, dennoch eine Äquivalenz herstellen kann. Der Geldhandel ist ein solches Medium.
>
> (3) Nur, was sich mit Geld bezahlen läßt, wird gehandelt. Insofern gibt es eine Filterwirkung.

An anderer Stelle wird eine solche Filterwirkung durch z.B. den Begriff der `Aufmerksamkeitsschwelle der Medien' impliziert. [Holtz-Bacha 1997]

---

[9] In der Literatur finden sich z.B. Aussagen, wie diese:

> *``Mit der Erkenntnis, daß die Herstellung von Politik, also politisches Entscheidungshandeln, mehr und mehr ihre Darstellung, also ihre - in der Regel massenmediale - Vermittlung gleich mitbedenkt, geht üblicherweise die Feststellung einher, daß es die politischen Akteure immer besser verstehen, sich dabei die Medien zunutze zu machen. Damit verbindet sich aber zumeist die Klage, daß diese Politikvermittlung auf rhetorische oder eben symbolische Politik setzt, daß sie Worthülsen und Inszenierung vor Sachinformation und rationale Reflexion stellt."*

oder

> *``... Aufmerksamkeit heischende Verpackung ... statt Substanz."*

[Holtz-Bacha 1997]

---

[10] Anders ausgedrückt:

> *``In seinem Bestreben, das größtmögliche Publikum über die staatlichen Grenzen hinweg anzusprechen, muß das globalisierte Medienangebot universell sein und sich daher zwangsläufig von nationalen kulturellen und politischen Bezügen lösen. Was international also Homogenisierung bedeutet, wird in nationaler Perspektive als Verlust der spezifischen kulturellen Charakteristika des Medienangebots empfunden."*

[Holtz-Bacha 1997]

---

[11] Kulturunabhängigkeit soll in diesem Falle nicht bedeuten, daß die Kultur unbeeinflußt bleibt. Sie stellt nur nicht das Subjekt, sondern das Objekt der Veränderungen, nicht die Voraussetzungen, sondern den Gegenstand dar.

Mit dem Wissen darum läßt sich Politik machen:

> *``Die Eröffnung von Fast-food-Restaurants wäre beispielsweise eine wirksame ,,subversive`` Maßnahme, die gewiß auch auf Kuba ihre Wirkung im Sinne der Einführung westlichen [universalistischen, Anm. d. Autors] Lebensgefühls entfalten würde. Damit könnte Bill Clinton gelingen, was dem großen Perikles nicht glückte: einen lästigen Kleinstaat zermürben, die eigenen Interessen durchsetzen und doch mit den Partnern weiter in Frieden leben."*

[Hofmeister 1997]

[Anmerkung: Wilhelm Hofmeister arbeitet für die Konrad-Adenauer-Stiftung im Bereich Internationale Zusammenarbeit.]

Multimediagesetz (IuKDG*)

Inhaltsverzeichnis

Artikel 1: Gesetz über die Nutzung von Telediensten (Teledienstegesetz - TDG)

*[**Anmerkung:** Der Text befindet sich in einem gesonderten File.]*

Artikel 2: Gesetz über den Datenschutz bei Telediensten (Teledienstdatenschutzgesetz - TDDSG)

*[**Anmerkung:** Der Text befindet sich in einem gesonderten File.]*

Artikel 3: Gesetz zur digitalen Signatur (Signaturgesetz - SigG)

*[**Anmerkung:** Der Text befindet sich in einem gesonderten File.]*

Artikel 4: Änderung des Strafgesetzbuches

Das Strafgesetzbuch in der Fassung der Bekanntmachung vom 10. März 1987 (BGBl. I S. 945, 1160), zuletzt geändert durch ??? (BGBl. ???), wird wie folgt geändert:

1. §11 Abs. 3 StGB wird wie folgt gefaßt:

   ``*(3) Den Schriften stehen Ton- und Bildträger, Datenspeicher, Abbildungen und andere Darstellungen in denjenigen Vorschriften gleich, die auf diesen Absatz verweisen.*"

2. §74 d wird wie folgt geändert:

   a. In Absatz 3 wird nach dem Wort ``*Schriften*" die Angabe ``*(§11 Abs. 3)*" eingefügt.
   b. In Absatz 4 werden nach dem Wort ``*wenn*" die Wörter ``*die Schrift (§11 Abs. 3) oder*" eingefügt.

3. In §86 Abs. 1 werden nach dem Wort ``ausführt" die Wörter ``oder in Datenspeichern öffentlich zugänglich macht" eingefügt.

4. §184 wird wie folgt geändert:

   a. In Absatz 4 werden nach dem Wort ``*tatsächliches*" die Wörter ``*oder wirklichkeitsnahes*" eingefügt,
   b. In Absatz 5 Satz 1 werden nach dem Wort ``*tatsächliches*" die Wörter

``*oder wirklichkeitsnahes*" eingefügt.

Artikel 5: Änderung des Gesetzes über Ordnungswidrigkeiten

Das Gesetz über Ordnungswidrigkeiten in der Fassung der Bekanntmachung vom 19. Februar 1987 (BGBl. I S. 602), zuletzt geändert durch ??? (BGBl. ???), wird wie folgt geändert:

1. In §116 Abs. 1, §120 Abs. 1 Nr. 2 und §123 Abs. 2 Satz 1 werden jeweils nach dem Wort ``*Bildträgern*" ein Komma und das Wort ``*Datenspeichern*" eingefügt.

2. §119 wird wie folgt geändert:

   a. In Absatz 1 Nr. 2 werden nach dem Wort ``*Darstellungen*" die Wörter ``*oder durch das öffentliche Zugänglichmachen von Datenspeichern*" eingefügt.
   b. In Absatz 3 werden nach dem Wort ``*Bildträger*" ein Komma und das Wort ``*Datenspeicher*" eingefügt.

Artikel 6: Änderung des Gesetzes über die Verbreitung jugendgefährdender Schriften

Das Gesetz über die Verbreitung jugendgefährdender Schriften in der Fassung der Bekanntmachung vom 12. Juli 1985 (BGBl. I S. 1502), zuletzt geändert durch ??? (BGBl. ???), wird wie folgt geändert:

1. Die Überschrift wird wie folgt neu gefaßt:

   ``*Gesetz über die Verbreitung jugendgefährdender Schriften und Medieninhalte*"

2. §1 Abs. 3 wird wie folgt gefaßt:

   ``*(3) Den Schriften stehen Ton- und Bildträger, Datenspeicher, Abbildungen und andere Darstellungen gleich. Schriften im Sinne dieses Gesetzes sind nicht Rundfunksendungen nach §2 des Rundfunkstaatsvertrages sowie inhaltliche Angebote bei Verteildiensten und Abrufdiensten, soweit die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht, nach §2 des Mediendienste-Staatsvertrages in der Fassung vom 20. Januar bis 7. Februar 1997.*"

3. §3 wird wie folgt geändert:

    a. In Absatz 1 wird am Ende der Nummer 3 der Punkt durch ein Komma ersetzt und folgende Nummer 4 angefügt:

    ``*4. durch Informations- und Kommunikationsdienste verbreitet, bereitgehalten oder sonst zugänglich gemacht werden.*"

    b. Dem Absatz 2 wird folgender Satz angefügt:

    ``*Absatz 1 Nr. 4 gilt nicht, wenn durch technische Vorkehrungen Vorsorge getroffen ist, daß das Angebot oder die Verbreitung im Inland auf volljährige Nutzer beschränkt werden kann.*"

4. §5 Abs. 3 wird wie folgt gefaßt:

    ``*(3) Absatz 2 gilt nicht,*

    1. *wenn die Handlung im Geschäftsverkehr mit dem einschlägigen Handel erfolgt, oder*
    2. *wenn durch technische Vorkehrungen oder in sonstiger Weise eine Übermittlung an Kinder oder Jugendliche ausgeschlossen ist.*"

5. Nach §7 wird folgender §7a eingefügt:

    ``*§7a Jugendschutzbeauftragte*

    Wer gewerbsmäßig elektronische Informations- und Kommunikationsdienste, denen eine Übermittlung mittels Telekommunikation zugrunde liegt, zur Nutzung bereithält, hat einen Jugendschutzbeauftragten zu bestellen, wenn diese allgemein angeboten werden und jugendgefährdende Inhalte enthalten können. Er ist Ansprechpartner für Nutzer und berät den Diensteanbieter in Fragen des Jugendschutzes. Er ist von dem Diensteanbieter bei der Angebotsplanung und der Gestaltung der Allgemeinen Nutzungsbedingungen zu beteiligen. Er kann gegenüber dem Diensteanbieter eine Beschränkung von Angeboten vorschlagen. Die Verpflichtung des Diensteanbieters nach Satz 1 kann auch dadurch erfüllt werden, daß er eine Organisation der freiwilligen Selbstkontrolle zur Wahrnehmung der Aufgaben nach Satz 2 bis 4 verpflichtet."

6. Nach §21 Abs. 1 Nr. 3 wird folgende Nummer 3a eingefügt:

    ``*3a. entgegen §3 Abs. 1 Nr. 4 verbreitet, bereithält oder sonst zugänglich macht,*"

7. §18 wird wie folgt gefaßt:

``*(1) Eine Schrift unterliegt den Beschränkungen der §§3 bis 5, ohne daß es einer Aufnahme in die Liste und einer Bekanntmachung bedarf, wenn sie ganz oder im wesentlichen inhaltsgleich mit einer in die Liste aufgenommenen Schrift ist. Das gleiche gilt, wenn ein Gericht in einer rechtskräftigen Entscheidung festgestellt hat, daß eine Schrift pornographisch ist oder den in §130 Abs. 2 oder §131 des Strafgesetzbuches bezeichneten Inhalt hat.*

(2) Ist es zweifelhaft, ob die Voraussetzungen des Absatzes 1 erfüllt sind, so führt der Vorsitzende eine Entscheidung der Bundesprüfstelle herbei. Eines Antrages (§11 Abs. 2 Satz 1) bedarf es nicht. §12 gilt entsprechend.

(3) Wird die Schrift in die Liste aufgenommen, so gilt §19 entsprechend."

8. §18 a wird gestrichen.

9. §2 wird wie folgt geändert:

   a. Der bisherige Text wird Absatz 1.
   b. Es wird folgender Absatz 2 angefügt:

   ``*(2) Kommt eine Listenaufnahme offensichtlich nicht in Betracht, so kann der Vorsitzende das Verfahren einstellen.*".

10. §21 a Absatz 1 wird wie folgt gefaßt:

    ``*(1) Ordnungswidrig handelt, wer*

    1. *entgegen §4 Abs. 2 Satz 2 einen Abnehmer nicht auf die Vertriebsbeschränkungen hinweist, oder*
    2. *entgegen §7 a Abs. 1 Satz 1 einen Jugendschutzbeauftragten nicht bestellt oder eine Organisation der freiwilligen Selbstkontrolle zur Wahrnehmung dieser Aufgaben nicht verpflichtet.*"

Artikel 7: Änderung des Urheberrechtsgesetzes

Das Urheberrechtsgesetz vom 9. September 1965 (BGBl. I S. 1273), zuletzt geändert durch ??? (BGBl. ???), wird wie folgt geändert:

1. §4 wird wie folgt gefaßt:

``*§4 Sammelwerke und Datenbankwerke*

(1) Sammlungen von Werken, Daten oder anderen unabhängigen Elementen, die aufgrund der Auswahl oder Anordnung der Elemente eine persönliche geistige Schöpfung sind (Sammelwerke), werden, unbeschadet eines an den einzelnen Elementen gegebenenfalls bestehenden Urheberrechts oder verwandten Schutzrechts, wie selbständige Werke geschützt.

(2) Datenbankwerk im Sinne dieses Gesetzes ist ein Sammelwerk, dessen Elemente systematisch oder methodisch angeordnet und einzeln mit Hilfe elektronischer Mittel oder auf andere Weise zugänglich sind. Ein zur Schaffung des Datenbankwerkes oder zur Ermöglichung des Zugangs zu dessen Elementen verwendetes Computerprogramm (§69 a) ist nicht Bestandteil des Datenbankwerkes."

2. §23 Satz 2 wird wie folgt geändert:

    a. Nach dem Wort ``*Künste*" wird das Wort ``*oder*" durch ein Komma ersetzt.
    b. Nach dem Wort ``*Baukunst*" werden die Wörter ``*oder um die Bearbeitung oder Umgestaltung eines Datenbankwerkes*" eingefügt.

3. §53 wird wie folgt geändert:

    a. Nach Absatz 4 wird folgender Absatz 5 eingefügt:

        ``*Absatz 1 sowie Absatz 2 Nr. 2 bis 4 finden keine Anwendung auf Datenbankwerke, deren Elemente einzeln mit Hilfe elektronischer Mittel zugänglich sind. Absatz 2 Nr. 1 findet auf solche Datenbankwerke mit der Maßgabe Anwendung, daß der wissenschaftliche Gebrauch nicht zu gewerblichen Zwecken erfolgt.*"

    b. Die bisherigen Absätze 5 und 6 werden Absätze 6 und 7.

4. Nach §55 wird folgender §55 a eingefügt:

    ``*§55 a Benutzung eines Datenbankwerkes*

    Zulässig ist die Bearbeitung sowie die Vervielfältigung eines Datenbankwerkes durch den Eigentümer eines mit Zustimmung des Urhebers durch Veräußerung in Verkehr gebrachten Vervielfältigungsstücks des Datenbankwerkes, den in sonstiger Weise zu dessen Gebrauch Berechtigten oder denjenigen, dem ein Datenbankwerk aufgrund eines mit dem Urheber oder eines mit dessen Zustimmung mit einem Dritten geschlossenen Vertrags zugänglich gemacht wird, wenn und soweit die Bearbeitung oder Vervielfältigung für den Zugang zu den Elementen des Datenbankwerkes und für dessen

übliche Benutzung erforderlich ist. Wird aufgrund eines Vertrags nach Satz 1 nur ein Teil des Datenbankwerkes zugänglich gemacht, so ist nur die Bearbeitung sowie die Vervielfältigung dieses Teils zulässig. Entgegenstehende vertragliche Vereinbarungen sind nichtig."

5. In §63 Absatz 1 wird nach Satz 1 folgender Satz 2 eingefügt:

    a. ``*Das gleiche gilt in den Fällen des §53 Abs. 2 Nr. 1 und Abs. 3 Nr. 1 für die Vervielfältigung eines Datenbankwerkes.*"
    b. Die bisherigen Sätze 2 und 3 werden Sätze 3 und 4.

6. Nach §87 wird folgender Abschnitt eingefügt:

    ``*Sechster Abschnitt*
    Schutz des Datenbankherstellers

    §87a Begriffsbestimmungen

    (1) Datenbank im Sinne dieses Gesetzes ist eine Sammlung von Werken, Daten oder anderen unabhängigen Elementen, die systematisch oder methodisch angeordnet und einzeln mit Hilfe elektronischer Mittel oder auf andere Weise zugänglich sind und deren Beschaffung, Überprüfung oder Darstellung eine nach Art oder Umfang wesentliche Investition erfordert. Eine in ihrem Inhalt nach Art oder Umfang wesentlich geänderte Datenbank gilt als neue Datenbank, sofern die Änderung eine nach Art oder Umfang wesentliche Investition erfordert.

    (2) Datenbankhersteller im Sinne dieses Gesetzes ist derjenige, der die Investition im Sinne von Absatz 1 vorgenommen hat.

    §87b Rechte des Datenbankherstellers

    (1) Der Datenbankhersteller hat das ausschließliche Recht, die Datenbank insgesamt oder einen nach Art oder Umfang wesentlichen Teil der Datenbank zu vervielfältigen, zu verbreiten und öffentlich wiederzugeben. Der Vervielfältigung, Verbreitung oder öffentlichen Wiedergabe eines nach Art oder Umfang wesentlichen Teils der Datenbank steht die wiederholte und systematische Vervielfältigung, Verbreitung oder öffentliche Wiedergabe von nach Art und Umfang unwesentlichen Teilen der Datenbank gleich, sofern diese Handlungen einer normalen Auswertung der Datenbank zuwiderlaufen oder die berechtigten Interessen des Datenbankherstellers unzumutbar beeinträchtigen.

    (2) §17 Abs. 2 und §27 Abs. 2 und 3 sind entsprechend anzuwenden.

    §87c Schranken des Rechts des Datenbankherstellers

(1) Die Vervielfältigung eines nach Art oder Umfang wesentlichen Teils einer Datenbank ist zulässig

1. *zum privaten Gebrauch; dies gilt nicht für eine Datenbank, deren Elemente einzeln mit Hilfe elektronischer Mittel zugänglich sind,*
2. *zum eigenen wissenschaftlichen Gebrauch, wenn und soweit die Vervielfältigung zu diesem Zweck geboten ist und der wissenschaftliche Gebrauch nicht zu gewerblichen Zwecken erfolgt,*
3. *zum eigenen Gebrauch im Schulunterricht, in nichtgewerblichen Einrichtungen der Aus- und Weiterbildung sowie in der Berufsbildung in der für eine Schulklasse erforderlichen Anzahl.*

In den Fällen der Nummern 2 und 3 ist die Quelle deutlich anzugeben.

(2) Die Vervielfältigung, Verbreitung und öffentliche Wiedergabe eines nach Art oder Umfang wesentlichen Teils einer Datenbank ist zulässig zur Verwendung in Verfahren vor einem Gericht, einem Schiedsgericht oder einer Behörde sowie für Zwecke der öffentlichen Sicherheit.

§87d Dauer der Rechte

Die Rechte des Datenbankherstellers erlöschen fünfzehn Jahre nach der Veröffentlichung der Datenbank, jedoch bereits fünfzehn Jahre nach der Herstellung, wenn die Datenbank innerhalb dieser Frist nicht veröffentlicht worden ist. Die Frist ist nach §69 zu berechnen.

§87e Verträge über die Benutzung einer Datenbank

Eine vertragliche Vereinbarung, durch die sich der Eigentümer eines mit Zustimmung des Datenbankherstellers durch Veräußerung in Verkehr gebrachten Vervielfältigungsstücks der Datenbank, der in sonstiger Weise zu dessen Gebrauch Berechtigte oder derjenige, dem eine Datenbank aufgrund eines mit dem Datenbankhersteller oder eines mit dessen Zustimmung mit einem Dritten geschlossenen Vertrags zugänglich gemacht wird, gegenüber dem Datenbankhersteller verpflichtet, die Vervielfältigung, Verbreitung oder öffentliche Wiedergabe von nach Art und Umfang unwesentlichen Teilen der Datenbank zu unterlassen, ist insoweit unwirksam, als diese Handlungen weder einer normalen Auswertung der Datenbank zuwiderlaufen noch die berechtigten Interessen des Datenbankherstellers unzumutbar beeinträchtigen."

7. In §108 Abs. 1 wird nach Nr. 7 folgende Nummer angefügt:

``*8. eine Datenbank entgegen §87b Abs. 2 verwertet,*"

8. In §119 Abs. 3 werden nach dem Wort ``*Lichtbilder*" das Wort ``*und*" durch ein Komma ersetzt und nach dem Wort ``*Tonträger*" die Wörter ``*und die nach §87 b Abs. 2 geschützten Datenbanken*" eingefügt.

9. Nach §127 wird folgender §127 a eingefügt:

   ``*§127a Schutz des Datenbankherstellers*

   (1) Den nach §87b gewährten Schutz genießen deutsche Staatsangehörige sowie juristische Personen mit Sitz im Geltungsbereich dieses Gesetzes. §120 Abs. 2 ist anzuwenden.

   (2) Die nach deutschem Recht oder dem Recht eines der in §120 Abs. 2 Nr. 2 bezeichneten Staaten gegründeten juristischen Personen ohne Sitz im Geltungsbereich dieses Gesetzes genießen den nach §87 b gewährten Schutz, wenn

   1. *ihre Hauptverwaltung oder Hauptniederlassung sich im Gebiet eines der in §120 Abs. 2 Nr. 2 bezeichneten Staaten befindet oder*
   2. *ihr satzungsmäßiger Sitz sich im Gebiet eines dieser Staaten befindet und ihre Tätigkeit eine tatsächliche Verbindung zur deutschen Wirtschaft oder zur Wirtschaft eines dieser Staaten aufweist.*

   (3) Im übrigen genießen ausländische Staatsangehörige sowie juristische Personen den Schutz nach dem Inhalt von Staatsverträgen sowie von Vereinbarungen, die die Europäische Gemeinschaft mit dritten Staaten schließt; diese Vereinbarungen werden vom Bundesministerium der Justiz im Bundesgesetzblatt bekanntgemacht."

10. Nach §137 f wird folgender §137 g eingefügt:

    ``*§137 g Übergangsregelung bei Umsetzung der Richtlinie 96/9/EG*

    (1) Die §§23 Satz 2, 53 Abs. 5, 55 a und 63 Abs. 1 Satz 2 sind auch auf Datenbankwerke anzuwenden, die vor dem 1. Januar 1998 geschaffen wurden.

    (2) Die Vorschriften des Sechsten Abschnitts des Zweiten Teils sind auch auf Datenbanken anzuwenden, die zwischen dem 1. Januar 1983 und dem 31. Dezember 1997 hergestellt worden sind. Die Schutzfrist beginnt in diesen Fällen am 1. Januar 1998.

    (3) Die §§55 a und 87 e sind nicht auf Verträge anzuwenden, die vor dem 1. Januar 1998 abgeschlossen worden sind."

Artikel 8: Änderung des Preisangabengesetzes

Dem §1 des Preisangabengesetzes vom 3. Dezember 1984 (BGBl. I S. 1429) wird folgender Satz angefügt:

``*Bei Leistungen der Informations- und Kommunikationsdienste können auch Bestimmungen über die Angabe des Preisstandes fortlaufender Leistungen getroffen werden.*"

Artikel 9: Änderung der Preisangabenverordnung

Die Preisangabenverordnung vom 14. März 1985 (BGBl. I S. 580), zuletzt geändert durch ??? (BGBl. ???), wird wie folgt geändert:

1. Dem §3 Abs. 1 werden folgende Sätze angefügt:

   ``*Ort des Leistungsangebots ist auch die Bildschirmanzeige. Wird eine Leistung über Bildschirmanzeige erbracht und nach Einheiten berechnet, ist eine gesonderte Anzeige über den Preis der fortlaufenden Nutzung unentgeltlich anzubieten.*"

2. §8 Abs. 2 Nr. 2 wird wie folgt gefaßt:

   ``*2. des §3 Abs. 1 Satz 1, 2 oder 4 oder Abs. 2, jeweils auch in Verbindung mit §2 Abs. 5, über das Aufstellen, das Anbringen oder das Bereithalten von Preisverzeichnissen oder über das Anbieten einer Anzeige des Preises,*".

Artikel 10: Rückkehr zum einheitlichen Verordnungsrang

Die auf Artikel 8 beruhenden Teile der Preisangabenverordnung können auf Grund der Ermächtigung des §1 Preisangabengesetz durch Rechtsverordnung geändert werden.

Artikel 11: Inkrafttreten

Dieses Gesetz tritt mit Ausnahme des Artikels 7 , der am 1. Januar 1998 in Kraft tritt, am 1.

August 1997 in Kraft.

** Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienstegesetz - IuKDG); in der Fassung vom 13. Juni 1997*

Teledienstegesetz (TDG*)

Inhaltsverzeichnis

§1 Zweck des Gesetzes

Zweck des Gesetzes ist es, einheitliche wirtschaftliche Rahmenbedingungen für die verschiedenen Nutzungsmöglichkeiten der elektronischen Informations- und Kommunikationsdienste zu schaffen.

§2 Geltungsbereich

(1) Die nachfolgenden Vorschriften gelten für alle elektronischen Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Töne bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt (Teledienste).

(2) Teledienste im Sinne von Absatz 1 sind insbesondere:

1. Angebote im Bereich der Individualkommunikation (zum Beispiel Telebanking, Datenaustausch),
2. Angebote zur Information oder Kommunikation soweit nicht die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht (Datendienste, zum Beispiel Verkehrs-, Wetter-, Umwelt- und Börsendaten, Verbreitung von Informationen über Waren und Dienstleistungsangebote),
3. Angebote zur Nutzung des Internets oder weiterer Netze,
4. Angebote zur Nutzung von Telespielen,
5. Angebote von Waren und Dienstleistungen in elektronisch abrufbaren Datenbanken mit interaktivem Zugriff und unmittelbarer Bestellmöglichkeit.

(3) Absatz 1 gilt unabhängig davon, ob die Nutzung der Teledienste ganz oder teilweise unentgeltlich oder gegen Entgelt möglich ist.

(4) Dieses Gesetz gilt nicht für

1. Telekommunikationsdienstleistungen und das geschäftsmäßige Erbringen von Telekommunikationsdiensten nach §3 des Telekommunikationsgesetzes vom 25. Juli 1996 (BGBl. I S. 1120),
2. Rundfunk im Sinne des §2 des Rundfunkstaatsvertrages ,
3. inhaltliche Angebote bei Verteildiensten und Abrufdiensten, soweit die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht, nach §2 des Mediendienste-Staatsvertrages in der Fassung vom 20. Januar bis 7. Februar 1997.

(5) Presserechtliche Vorschriften bleiben unberührt.

§3 Begriffsbestimmungen

Im Sinne dieses Gesetzes sind:

1. ``Diensteanbieter" natürliche oder juristische Personen oder Personenvereinigungen, die eigene oder fremde Teledienste zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln,
2. ``Nutzer" natürliche oder juristische Personen oder Personenvereinigungen, die Teledienste nachfragen.

§4 Zugangsfreiheit

Teledienste sind im Rahmen der Gesetze zulassungs- und anmeldefrei.

§5 Verantwortlichkeit

(1) Diensteanbieter sind für eigene Inhalte, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich.

(2) Diensteanbieter sind für fremde Inhalte, die sie zur Nutzung bereithalten, nur dann verantwortlich, wenn sie von diesen Inhalten Kenntnis haben und es ihnen technisch möglich und zumutbar ist, deren Nutzung zu verhindern.

(3) Diensteanbieter sind für fremde Inhalte, zu denen sie lediglich den Zugang zur Nutzung vermitteln, nicht verantwortlich. Eine automatische und kurzzeitige Vorhaltung fremder Inhalte aufgrund Nutzerabfrage gilt als Zugangsvermittlung.

(4) Verpflichtungen zur Sperrung der Nutzung rechtswidriger Inhalte nach den allgemeinen Gesetzen bleiben unberührt, wenn der Diensteanbieter unter Wahrung des Fernmeldegeheimnisses gemäß §85 des Telekommunikationsgesetzes von diesen Inhalten Kenntnis erlangt und eine Sperrung technisch möglich und zumutbar ist.

§6 Anbieterkennzeichnung

Diensteanbieter haben für ihre geschäftsmäßigen Angebote anzugeben:

1. Namen und Anschrift sowie
2. bei Personenvereinigungen und -gruppen auch Namen und Anschrift des Vertretungsberechtigten.

** Gesetz über die Nutzung von Telediensten; Artikel 1 des Multimediagesetzes (Informations- und Kommunikationsdienstegesetz, IuKDG) vom 13. Juni 1997*

Teledienstedatenschutzgesetz (TDDSG*)

Inhaltsverzeichnis

§1 Geltungsbereich

(1) Die nachfolgenden Vorschriften gelten für den Schutz personenbezogener Daten bei Telediensten im Sinne des Teledienstegesetzes .

(2) Soweit in diesem Gesetz nichts anderes bestimmt ist, sind die jeweils geltenden Vorschriften über den Schutz personenbezogener Daten anzuwenden, auch wenn die Daten nicht in Dateien verarbeitet oder genutzt werden.

§2 Begriffsbestimmungen

Im Sinne dieses Gesetzes sind:

1. ``Diensteanbieter'' natürliche oder juristische Personen oder Personenvereinigungen, die Teledienste zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln,
2. ``Nutzer'' natürliche oder juristische Personen oder Personenvereinigungen, die Teledienste nachfragen.

§3 Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten dürfen vom Diensteanbieter zur Durchführung von Telediensten nur erhoben, verarbeitet und genutzt werden, soweit dieses Gesetz oder eine andere Rechtsvorschrift es erlaubt oder der Nutzer eingewilligt hat.

(2) Der Diensteanbieter darf für die Durchführung von Telediensten erhobene Daten für andere Zwecke nur verwenden, soweit dieses Gesetz oder eine andere Rechtsvorschrift es erlaubt oder der Nutzer eingewilligt hat.

(3) Der Diensteanbieter darf die Erbringung von Telediensten nicht von einer Einwilligung des Nutzers in eine Verarbeitung oder Nutzung seiner Daten für andere Zwecke abhängig machen, wenn dem Nutzer ein anderer Zugang zu diesen Telediensten nicht oder in zumutbarer Weise nicht möglich ist.

(4) Die Gestaltung und Auswahl technischer Einrichtungen für Teledienste hat sich an dem Ziel, keine oder so wenige personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen, auszurichten.

(5) Der Nutzer ist vor der Erhebung über Art, Umfang, Ort und Zwecke der Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu unterrichten. Bei automatisierten Verfahren, die eine spätere Identifizierung des Nutzers ermöglichen und eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten vorbereiten, ist der Nutzer vor Beginn dieses Verfahrens zu unterrichten. Der Inhalt der Unterrichtung muß für den Nutzer jederzeit abrufbar sein. Der Nutzer kann auf die Unterrichtung verzichten. Die Unterrichtung und der Verzicht sind zu protokollieren. Der Verzicht gilt nicht als Einwilligung im Sinne von Absatz 1 und 2.

(6) Der Nutzer ist vor Erklärung seiner Einwilligung auf sein Recht auf jederzeitigen Widerruf mit Wirkung für die Zukunft hinzuweisen. Absatz 5 Satz 3 gilt entsprechend.

(7) Die Einwilligung kann auch elektronisch erklärt werden, wenn der Diensteanbieter sicherstellt, daß

1. sie nur durch eine eindeutige und bewußte Handlung des Nutzers erfolgen kann,
2. sie nicht unerkennbar verändert werden kann,
3. ihr Urheber erkannt werden kann,
4. die Einwilligung protokolliert wird und
5. der Inhalt der Einwilligung jederzeit vom Nutzer abgerufen werden kann.

§4 Datenschutzrechtliche Pflichten des Diensteanbieters

(1) Der Diensteanbieter hat dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeiten zu informieren.

(2) Der Diensteanbieter hat durch technische und organisatorische Vorkehrungen sicherzustellen, daß

1. der Nutzer seine Verbindung mit dem Diensteanbieter jederzeit abbrechen kann,
2. die anfallenden personenbezogenen Daten über den Ablauf des Abrufs oder Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht werden, soweit nicht eine längere Speicherung für Abrechnungszwecke erforderlich ist,
3. der Nutzer Teledienste gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann,
4. die personenbezogenen Daten über die Inanspruchnahme verschiedener Teledienste durch einen Nutzer getrennt verarbeitet werden; eine Zusammenführung dieser Daten ist unzulässig, soweit dies nicht für Abrechnungszwecke erforderlich ist.

(3) Die Weitervermittlung zu einem anderen Diensteanbieter ist dem Nutzer anzuzeigen.

(4) Nutzungsprofile sind nur bei Verwendung von Pseudonymen zulässig. Unter einem Pseudonym erfaßte Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.

§5 Bestandsdaten

(1) Der Diensteanbieter darf personenbezogene Daten eines Nutzers erheben, verarbeiten und nutzen, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines

Vertragsverhältnisses mit ihm über die Nutzung von Telediensten erforderlich sind (Bestandsdaten).

(2) Eine Verarbeitung und Nutzung der Bestandsdaten für Zwecke der Beratung, der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung technischer Einrichtungen des Diensteanbieters ist nur zulässig, soweit der Nutzer in diese ausdrücklich eingewilligt hat.

§6 Nutzungs- und Abrechnungsdaten

(1) Der Diensteanbieter darf personenbezogene Daten über die Inanspruchnahme von Telediensten nur erheben, verarbeiten und nutzen, soweit dies erforderlich ist,

1. um dem Nutzer die Inanspruchnahme von Telediensten zu ermöglichen (Nutzungsdaten) oder
2. um die Nutzung von Telediensten abzurechnen (Abrechnungsdaten).

(2) Zu löschen hat der Diensteanbieter

1. Nutzungsdaten frühestmöglich, spätestens unmittelbar nach Ende der jeweiligen Nutzung, soweit es sich nicht um Abrechnungsdaten handelt,
2. Abrechnungsdaten, sobald sie für Zwecke der Abrechnung nicht mehr erforderlich sind; nutzerbezogene Abrechnungsdaten, die für die Erstellung von Einzelnachweisen über die Inanspruchnahme bestimmter Angebote auf Verlangen des Nutzers gemäß Absatz 4 gespeichert werden, sind spätestens 80 Tage nach Versendung des Einzelnachweises zu löschen, es sei denn, die Entgeltforderung wird innerhalb dieser Frist bestritten oder trotz Zahlungsaufforderung nicht beglichen.

(3) Die Übermittlung von Nutzungs- oder Abrechnungsdaten an andere Diensteanbieter oder Dritte ist unzulässig. Die Befugnisse der Strafverfolgungsbehörden bleiben unberührt. Der Diensteanbieter, der den Zugang zur Nutzung von Telediensten vermittelt, darf anderen Diensteanbietern, deren Teledienste der Nutzer in Anspruch genommen hat, lediglich übermitteln

1. anonymisierte Nutzungsdaten zu Zwecken deren Marktforschung,
2. Abrechnungsdaten, soweit diese zum Zwecke der Einziehung einer Forderung erforderlich sind.

(4) Hat der Diensteanbieter mit einem Dritten einen Vertrag über die Abrechnung des Entgelts geschlossen, so darf er diesem Dritten Abrechnungsdaten übermitteln, soweit es für diesen Zweck erforderlich ist. Der Dritte ist zur Wahrung des Fernmeldegeheimnisses zu verpflichten.

(5) Die Abrechnung über die Inanspruchnahme von Telediensten darf Anbieter, Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter von einem Nutzer in Anspruch genommener Teledienste nicht erkennen lassen, es sei denn der Nutzer verlangt einen Einzelnachweis.

§7 Auskunftsrecht des Nutzers

Der Nutzer ist berechtigt, jederzeit die zu seiner Person oder zu seinem Pseudonym gespeicherten Daten unentgeltlich beim Diensteanbieter einzusehen. Die Auskunft ist auf Verlangen des Nutzers auch elektronisch zu erteilen. Das Auskunftsrecht ist im Falle einer kurzfristigen Speicherung im Sinne von §33 Abs. 2 Nr. 5 Bundesdatenschutzgesetz nicht nach §34 Abs. 4 Bundesdatenschutzgesetz ausgeschlossen.

§8 Datenschutzkontrolle

(1) §38 Bundesdatenschutzgesetz findet mit der Maßgabe Anwendung, daß die Überprüfung auch vorgenommen werden darf, wenn Anhaltspunkte für eine Verletzung von Datenschutzvorschriften nicht vorliegen.

(2) Der Bundesbeauftragte für den Datenschutz beobachtet die Entwicklung des Datenschutzes bei Telediensten und nimmt dazu im Rahmen seines Tätigkeitsberichtes nach § 26 Abs. 1 BDSG Stellung.

** Gesetz über den Datenschutz bei Telediensten; Artikel 2 des Multimediagesetzes (Informations- und Kommunikationsdienstegesetz, IuKDG) vom 13. Juni 1997*

Bundesdatenschutzgesetz (BDSG*)

Inhaltsverzeichnis

Zweiter Unterabschnitt: Rechte des Betroffenen

Dritter Unterabschnitt: Bundesbeauftragter für den Datenschutz

---

Dritter Abschnitt: Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen

Erster Unterabschnitt: Rechtsgrundlagen der Datenverarbeitung

Zweiter Unterabschnitt: Rechte des Betroffenen

Dritter Unterabschnitt: Beauftragter für den Datenschutz, Aufsichtsbehörde

---

Vierter Abschnitt: Sondervorschriften

Fünfter Abschnitt: Schlußvorschriften

Anhang

Erster Abschnitt: Allgemeine Bestimmungen

§1 Zweck und Anwendungsbereich des Gesetzes

(1) Zweck dieses Gesetzes ist es, den einzelnen davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

(2) Dieses Gesetz gilt für die *Erhebung*, *Verarbeitung* und *Nutzung* personenbezogener Daten durch

1. öffentliche Stellen des Bundes,
2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie
    a. Bundesrecht ausführen oder
    b. als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt,
3. nicht-öffentliche Stellen, soweit sie die Daten in oder aus Dateien geschäftsmäßig oder für berufliche oder gewerbliche Zwecke verarbeiten oder nutzen.

(3) Bei der Anwendung dieses Gesetzes gelten folgende Einschränkungen:

1. Für automatisierte Dateien, die ausschließlich aus verarbeitungstechnischen Gründen vorübergehend erstellt und nach ihrer verarbeitungstechnischen Nutzung automatisch gelöscht werden, gelten nur die §§5 und 9.
2. Für nicht-automatisierte Dateien, deren personenbezogene Daten nicht zur Übermittlung an Dritte bestimmt sind, gelten nur die §§5, 9, 39 und 40. Außerdem gelten für Dateien öffentlicher Stellen die Regelungen über die Verarbeitung und Nutzung personenbezogener Daten in Akten. Werden im Einzelfall personenbezogene Daten übermittelt, gelten für diesen Einzelfall die Vorschriften dieses Gesetzes uneingeschränkt.

(4) Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(5) Die Vorschriften dieses Gesetzes gehen denen des Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

§2 Öffentliche und nicht-öffentliche Stellen

(1) *Öffentliche Stellen des Bundes* sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform. Als öffentliche Stellen gelten die aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz oder dem Gesetz über Fernmeldeanlagen zusteht.

(2) *Öffentliche Stellen der Länder* sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes und sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie derer Vereinigungen ungeachtet ihrer Rechtsform.

(3) Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen, gelten ungeachtet der Beteiligung nicht-öffentlicher Stellen als *öffentliche Stellen des Bunde* s, wenn

1. sie über den Bereich eines Landes hinaus tätig werden oder
2. dem Bund die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht.

Andernfalls gelten sie als öffentliche Stellen der Länder.

(4) *Nicht-öffentliche Stellen* sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 fallen. Nimmt eine nicht-öffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

§3 Weitere Begriffsbestimmungen

(1) *Personenbezogene Daten* sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

(2) Eine *Datei* ist

1. eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann (automatisierte Datei), oder
2. jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden kann (nicht-automatisierte Datei).

Nicht hierzu gehören Akten und Aktensammlungen, es sei denn, daß sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können.

(3) Eine *Akte* ist jede sonstige amtlichen oder dienstlichen Zwecken dienende Unterlage; dazu zählen auch Bild- und Tonträger. Nicht hierunter fallen Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.

(4) *Erheben* ist das Beschaffen von Daten über den Betroffenen.

(5) *Verarbeiten* ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im einzelnen ist, ungeachtet der dabei angewendeten Verfahren:

1. *Speichern* das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung,
2. *Verändern* das inhaltliche Umgestalten gespeicherter personenbezogener Daten,
3. *Übermitteln* das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten (Empfänger) in der Weise, daß
    a. die Daten durch die speichernde Stelle an den Empfänger weitergegeben werden oder
    b. der Empfänger von der speichernden Stelle zur Einsicht oder zum Abruf

bereitgehaltene Daten einsieht oder abruft,

4. *Sperren* das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,
5. *Löschen* das Unkenntlichmachen gespeicherter personenbezogener Daten.

(6) *Nutzen* ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

(7) *Anonymisieren* ist das Verändern personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

(8) *Speichernde Stelle* ist jede Person oder Stelle, die personenbezogene Daten für sich selbst speichert oder durch andere im Auftrag speichern läßt.

(9) *Dritter* ist jede Person oder Stelle außerhalb der speichernden Stelle. Dritte sind nicht der Betroffene sowie diejenigen Personen und Stellen, die im Geltungsbereich dieses Gesetzes personenbezogene Daten im Auftrag verarbeiten oder nutzen.

§4 Zulässigkeit der Datenverarbeitung und -nutzung

(1) Die Verarbeitung personenbezogener Daten und deren Nutzung sind nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat.

(2) Wird die Einwilligung bei dem Betroffenen eingeholt, ist er auf den Zweck der Speicherung und einer vorgesehenen Übermittlung sowie auf Verlangen auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben.

(3) Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand im Sinne von Absatz 2 Satz 2 auch dann vor, wenn durch die Schriftform der bestimmte Forschungszweck erheblich beeinträchtigt würde. In diesem Fall sind der Hinweis nach Absatz 2 Satz 1 und die Gründe, aus denen sich die erhebliche Beeinträchtigung des bestimmten Forschungszweckes ergibt, schriftlich festzuhalten.

§5 Datengeheimnis

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§6 Unabdingbare Rechte des Betroffenen

(1) Die Rechte des Betroffenen auf Auskunft (§§19, 34) und auf Berichtigung, Löschung oder Sperrung (§§ 20, 35) können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

(2) Sind die Daten des Betroffenen in einer Datei gespeichert, bei der mehrere Stellen speicherungsberechtigt sind, und ist der Betroffene nicht in der Lage, die speichernde Stelle festzustellen, so kann er sich an jede dieser Stellen wenden. Diese ist verpflichtet, das Vorbringen des Betroffenen an die speichernde Stelle weiterzuleiten. Der Betroffene ist über die Weiterleitung und die speichernde Stelle zu unterrichten. Die in §19 Absatz 3 genannten Stellen, die Behörden der Staatsanwaltschaft und der Polizei sowie öffentliche Stellen der Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, können statt des Betroffenen den Bundesbeauftragten für den Datenschutz unterrichten. In diesem Fall richtet sich das weitere Verfahren nach §19 Absatz 6.

§7 Schadensersatz durch öffentliche Stellen

(1) Fügt eine öffentliche Stelle dem Betroffenen durch eine nach den Vorschriften dieses Gesetzes oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige automatisierte Verarbeitung seiner personenbezogenen Daten einen Schaden zu, ist sie dem Betroffenen unabhängig von einem Verschulden zum Ersatz des daraus entstehenden Schadens verpflichtet.

(2) Bei einer schweren Verletzung des Persönlichkeitsrechts ist dem Betroffenen der Schaden, der nicht Vermögensschaden ist, angemessen in Geld zu ersetzen.

(3) Die Ansprüche nach den Absätzen 1 und 2 sind insgesamt bis zu einem Betrag in Höhe von zweihundertfünfzigtausend Deutsche Mark begrenzt. Ist aufgrund desselben Ereignisses an mehrere Personen Schadensersatz zu leisten, der insgesamt den Höchstbetrag von zweihundertfünfzigtausend Deutsche Mark übersteigt, so verringern sich die einzelnen Schadensersatzleistungen in dem Verhältnis, in dem ihr Gesamtbetrag zu dem Höchstbetrag steht.

(4) Sind bei einer Datei mehrere Stellen speicherungsberechtigt und ist der Geschädigte nicht in der Lage, die speichernde Stelle festzustellen, so haftet jede dieser Stellen.

(5) Mehrere Ersatzpflichtige haften als Gesamtschuldner.

(6) Auf das Mitverschulden des Betroffenen und die Verjährung sind die §§254 und 852 des Bürgerlichen Gesetzbuches entsprechend anzuwenden.

(7) Vorschriften, nach denen ein Ersatzpflichtiger in weiterem Umfang als nach dieser Vorschrift haftet oder nach denen ein anderer für den Schaden verantwortlich ist, bleiben unberührt.

(8) Der Rechtsweg vor den ordentlichen Gerichten steht offen.

§8 Schadensersatz durch nicht-öffentliche Stellen

Macht ein Betroffener gegenüber einer nicht-öffentlichen Stelle einen Anspruch auf Schadensersatz wegen einer nach diesem Gesetz oder anderen Vorschriften über den Datenschutz unzulässigen oder unrichtigen automatisierten Datenverarbeitung geltend und ist streitig, ob der Schaden die Folge eines von der speichernden Stelle zu vertretenden Umstandes ist, so trifft die Beweislast die speichernde Stelle.

§9 Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

§10 Einrichtung automatisierter Abrufverfahren

(1) Die Einrichtung eines automatisierten Verfahrens, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, ist zulässig, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben oder Geschäftszwecke der beteiligten Stellen angemessen ist. Die Vorschriften über die Zulässigkeit des einzelnen Abrufs bleiben unberührt.

(2) Die beteiligten Stellen haben zu gewährleisten, daß die Zulässigkeit des Abrufverfahrens kontrolliert werden kann. Hierzu haben sie schriftlich festzulegen:

1. Anlaß und Zweck des Abrufverfahrens,
2. Datenempfänger,
3. Art der zu übermittelnden Daten,
4. nach §9 erforderliche technische und organisatorische Maßnahmen.

Im öffentlichen Bereich können die erforderlichen Festlegungen auch durch die Fachaufsichtsbehörden getroffen werden.

(3) Über die Einrichtung von Abrufverfahren ist in Fällen, in denen die in §12 Abs. 1 genannten Stellen beteiligt sind, der Bundesbeauftragte für den Datenschutz unter Mitteilung der Festlegungen nach Absatz 2 zu unterrichten. Die Einrichtung von Abrufverfahren, bei denen die in §6 Abs. 2 und in §19 Abs. 3 genannten Stellen beteiligt sind, ist nur zulässig, wenn der für die speichernde und die abrufende Stelle jeweils zuständige Bundes- oder Landesminister oder deren Vertreter zugestimmt haben.

(4) Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Empfänger. Die speichernde Stelle prüft die Zulässigkeit der Abrufe nur, wenn dazu Anlaß besteht. Die speichernde Stelle hat zu gewährleisten, daß die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann. Wird ein Gesamtbestand personenbezogener Daten abgerufen oder übermittelt (*Stapelverarbeitung*), so bezieht sich die Gewährleistung der Feststellung und Überprüfung nur auf die Zulässigkeit des Abrufes oder der Übermittlung des Gesamtbestandes.

(5) Die Absätze 1 bis 4 gelten nicht für den Abruf aus Datenbeständen, die jedermann, sei es ohne oder nach besonderer Zulassung, zur Benutzung offenstehen.

§11 Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

(1) Werden personenbezogene Daten im Auftrag durch andere Stellen verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in den §§6 bis 8 genannten Rechte sind ihm gegenüber geltend zu machen.

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei die Datenverarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind. Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden.

(3) Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten oder nutzen. Ist er der Ansicht, daß eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(4) Für den Auftragnehmer gelten neben den §§ 5, 9, 43 Abs. 1, Abs. 3 und 4 sowie §44 Abs. 1 Nr. 2, 5, 6 und 7 und Abs. 2 nur die Vorschriften über die Datenschutzkontrolle oder die Aufsicht, und zwar für

1. (a) öffentliche Stellen,
   (b) nicht-öffentliche Stellen, bei denen der öffentlichen Hand die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht und der Auftraggeber eine öffentliche Stelle ist, die §§18, 24 bis 26 oder die entsprechenden Vorschriften der Datenschutzgesetze der Länder,
2. die übrigen nicht-öffentlichen Stellen, soweit sie personenbezogene Daten im Auftrag als Dienstleistungsunternehmen geschäftsmäßig verarbeiten oder nutzen, die §§32, 36 bis 38.

Zweiter Abschnitt: Datenverarbeitung der öffentlichen Stellen

Erster Unterabschnitt: Rechtsgrundlagen der Datenverarbeitung

§12 Anwendungsbereich

(1) Die Vorschriften dieses Abschnittes gelten für öffentliche Stellen des Bundes, soweit sie nicht

als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen.

(2) Soweit der Datenschutz nicht durch Landesgesetz geregelt ist, gelten die §§12 bis 17, 19 und 20 auch für die öffentlichen Stellen der Länder, soweit sie

1. Bundesrecht ausführen und nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen oder
2. als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt.

(3) Für Landesbeauftragte für den Datenschutz gilt §23 Abs. 4 entsprechend.

(4) Werden personenbezogene Daten für frühere, bestehende oder zukünftige dienst- oder arbeitsrechtliche Rechtsverhältnisse verarbeitet oder genutzt, gelten anstelle der §§14 bis 17, 19 und 20 der §28 Abs. 1 und 2 Nr. 1 sowie die §§33 bis 35.

§13 Datenerhebung

(1) Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stellen erforderlich ist.

(2) personenbezogene Daten sind beim Betroffenen zu erheben.

Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder
2. (a) die zu erfüllende Verwaltungsaufgabe ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder
   (b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde

und keine Anhaltspunkte dafür bestehen, daß überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

(3) Werden personenbezogene Daten beim Betroffenen mit seiner Kenntnis erhoben, so ist der Erhebungszweck ihm gegenüber anzugeben. Werden sie beim Betroffenen aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Auf Verlangen ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.

(4) Werden personenbezogene Daten statt beim Betroffenen bei einer nicht-öffentlichen Stelle erhoben, so ist die Stelle auf die Rechtsvorschrift, die zur Auskunft verpflichtet, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.

§14 Datenspeicherung, -veränderung und -nutzung

(1) Das Speichern, Verändern oder Nutzen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind. Ist keine Erhebung vorausgegangen, dürfen die Daten nur für die Zwecke geändert oder genutzt werden, für die sie gespeichert worden sind.

(2) Das Speichern, Verändern oder Nutzen für andere Zwecke ist nur zulässig, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,
2. der Betroffene eingewilligt hat,
3. offensichtlich ist, daß es im Interesse des Betroffenen liegt, und kein Grund zu der Annahme besteht, daß er in Kenntnis des anderen Zwecks seine Einwilligung verweigern würde,
4. Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
5. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die speichernde Stelle sie veröffentlichen dürfte, es sei denn, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Zweckänderung offensichtlich überwiegt,
6. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit erforderlich ist,
7. es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des §11 Abs. 1 Nr. 8 des Strafgesetzbuches oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist,
8. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder
9. es zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluß der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(3) Eine Verarbeitung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie der

Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen für die speichernde Stelle dient. Das gilt auch für die Verarbeitung oder Nutzung zu Ausbildungs- und Prüfungszwecken durch die speichernde Stelle, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

(4) personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

§15 Datenübermittlung an öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an öffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Empfängers liegenden Aufgaben erforderlich ist und
2. die Voraussetzungen vorliegen, die eine Nutzung nach §14 zulassen würden.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen des Empfängers, trägt dieser die Verantwortung. In diesem Falle prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegt, es sei denn, daß besonderer Anlaß zur Prüfung der Zulässigkeit der Übermittlung besteht. §10 Abs. 4 bleibt unberührt.

(3) Der Empfänger darf die übermittelten Daten für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nur unter den Voraussetzungen des §14 Abs. 2 zulässig.

(4) Für die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften gelten die Absätze 1 bis 3 entsprechend, sofern sichergestellt ist, daß bei dem Empfänger ausreichende Datenschutzmaßnahmen getroffen werden.

(5) Sind mit personenbezogenen Daten, die nach Absatz 1 übermittelt werden dürfen, weitere personenbezogene Daten des Betroffenen oder eines Dritten in Akten so verbunden, daß eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechtigte Interessen des Betroffenen oder eines Dritten an deren Geheimhaltung offensichtlich überwiegen; eine Nutzung dieser Daten ist unzulässig.

(6) Absatz 5 gilt entsprechend, wenn personenbezogene Daten innerhalb einer öffentlichen Stelle weitergegeben werden.

§16 Datenübermittlung an nicht-öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach §14 zulassen würden, oder
2. der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.

(3) In den Fällen der Übermittlung nach Absatz 1 Nr. 2 unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung seiner Daten. Dies gilt nicht, wenn damit zu rechnen ist, daß er davon auf andere Weise Kenntnis erlangt, oder wenn die Unterrichtung die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde.

(4) Der Empfänger darf die übermittelten Daten nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Die übermittelnde Stelle hat den Empfänger darauf hinzuweisen. Eine Verarbeitung oder Nutzung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Absatz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.

§17 Datenübermittlung an Stellen außerhalb des Geltungsbereiches dieses Gesetzes

(1) Für die Übermittlung personenbezogener Daten an Stellen außerhalb des Geltungsbereichs dieses Gesetzes sowie an über- und zwischenstaatliche Stellen gilt §16 Abs. 1 nach Maßgabe der für diese Übermittlung geltenden Gesetze und Vereinbarungen, sowie §16 Abs. 3.

(2) Eine Übermittlung unterbleibt, soweit Grund zu der Annahme besteht, daß durch sie gegen den Zweck eines deutschen Gesetzes verstoßen würde.

(3) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.

(4) Der Empfänger ist darauf hinzuweisen, daß die übermittelten Daten nur zu dem Zweck

verarbeitet oder genutzt werden dürfen, zu dessen Erfüllung sie ihm übermittelt werden.

§18 Durchführung des Datenschutzes in der Bundesverwaltung

(1) Die obersten Bundesbehörden, der Präsident des Bundeseisenbahnvermögens sowie die bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, über die von der Bundesregierung oder einer obersten Bundesbehörde lediglich die Rechtsaufsicht ausgeübt wird, haben für ihren Geschäftsbereich die Ausführung dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen. Das gleiche gilt für die Vorstände der aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange diesen ein ausschließliches Recht nach dem Postgesetz oder dem Gesetz über Fernmeldeanlagen zusteht.

(2) Die öffentlichen Stellen führen ein Verzeichnis der eingesetzten Datenverarbeitungsanlagen. Für ihre Dateien haben sie schriftlich festzulegen:

1. Bezeichnung und Art der Dateien,
2. Zweckbestimmung,
3. Art der gespeicherten Daten,
4. betroffenen Personenkreis,
5. Art der regelmäßig zu übermittelnden Daten und deren Empfänger,
6. Regelfristen für die Löschung der Daten,
7. zugriffsberechtigte Personengruppen oder Personen, die allein zugriffsberechtigt sind.

Sie haben ferner dafür zu sorgen, daß die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, überwacht wird.

(3) Absatz 2 Satz 2 gilt nicht für Dateien, die nur vorübergehend vorgehalten und innerhalb von drei Monaten nach ihrer Erstellung gelöscht werden.

Zweiter Unterabschnitt: Rechte des Betroffenen

§19 Auskunft an den Betroffenen

(1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf Herkunft oder Empfänger dieser Daten beziehen, und
2. den Zweck der Speicherung.

In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Sind die personenbezogenen Daten in Akten gespeichert, wird die Auskunft nur erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht. Die speichernde Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.

(2) Absatz 1 gilt nicht für personenbezogene Daten, die nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen.

(3) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministers der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

(4) Die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben gefährden würde,
2. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder
3. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheimgehalten werden müssen und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muß.

(5) Die Ablehnung der Auskunftserteilung bedarf einer Begründung nicht, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Falle ist der Betroffene darauf hinzuweisen, daß er sich an den Bundesbeauftragten für den Datenschutz wenden kann.

(6) Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen dem Bundesbeauftragten für den Datenschutz zu erteilen, soweit nicht die jeweils zuständige oberste Bundesbehörde im Einzelfall feststellt, daß dadurch die Sicherheit des Bundes oder eines Landes

gefährdet würde. Die Mitteilung des Bundesbeauftragten an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der speichernden Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

(7) Die Auskunft ist unentgeltlich.

§20 Berichtigung, Löschung und Sperrung von Daten

(1) personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Wird festgestellt, daß personenbezogene Daten in Akten unrichtig sind, oder wird ihre Richtigkeit von dem Betroffenen bestritten, so ist dies in der Akte zu vermerken oder auf sonstige Weise festzuhalten.

(2) personenbezogene Daten in Dateien sind zu löschen, wenn

1. ihre Speicherung unzulässig ist oder
2. ihre Kenntnis für die speichernde Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.

(3) An die Stelle einer Löschung tritt eine Sperrung, soweit

1. einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,
2. Grund zu der Annahme besteht, daß durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder
3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

(4) personenbezogene Daten in Dateien sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt.

(5) personenbezogene Daten in Akten sind zu sperren, wenn die Behörde im Einzelfall feststellt, daß ohne die Sperrung schutzwürdige Interessen des Betroffenen beeinträchtigt würden und die Daten für die Aufgabenerfüllung der Behörde nicht mehr erforderlich sind.

(6) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn

1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder eines Dritten

liegenden Gründen unerläßlich ist und
2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

(7) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen im Rahmen einer regelmäßigen Datenübermittlung diese Daten zur Speicherung weitergegeben werden, wenn dies zur Wahrung schutzwürdiger Interessen des Betroffenen erforderlich ist.

(8) §2 Abs. 1 bis 6, 8 und 9 des Bundesarchivgesetzes ist anzuwenden.

§21 Anrufung des Bundesbeauftragten für den Datenschutz

Jedermann kann sich an den Bundesbeauftragten für den Datenschutz wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen des Bundes in seinen Rechten verletzt worden zu sein. Für die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch Gerichte des Bundes gilt dies nur, soweit diese in Verwaltungsangelegenheiten tätig werden.

Dritter Unterabschnitt: Bundesbeauftragter für den Datenschutz

§22 Wahl des Bundesbeauftragten für den Datenschutz

(1) Der Deutsche Bundestag wählt auf Vorschlag der Bundesregierung den Bundesbeauftragten für den Datenschutz mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder. Der Bundesbeauftragte muß bei seiner Wahl das 35. Lebensjahr vollendet haben. Der Gewählte ist vom Bundespräsidenten zu ernennen.

(2) Der Beauftragte leistet vor dem Bundesminister des Innern folgenden Eid:

> "Ich schwöre, daß ich meine Kraft dem Wohle des deutschen Volkes widmen, seinen Nutzen mehren, Schaden von ihm wenden, das Grundgesetz und die Gesetze des Bundes wahren und verteidigen, meine Pflichten gewissenhaft erfüllen und Gerechtigkeit gegen jedermann üben werde. So wahr mir Gott helfe."

Der Eid kann auch ohne religiöse Beteuerung geleistet werden.

(3) Die Amtszeit des Bundesbeauftragten beträgt fünf Jahre. Einmalige Wiederwahl ist zulässig.

(4) Der Bundesbeauftragte steht nach Maßgabe dieses Gesetzes zum Bund in einem öffentlich-rechtlichen Amtsverhältnis. Er ist in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Er untersteht der Rechtsaufsicht der Bundesregierung.

(5) Der Bundesbeauftragte wird beim Bundesminister des Innern eingerichtet. Er untersteht der Dienstaufsicht des Bundesministers des Innern. Dem Bundesbeauftragten ist die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen; sie ist im Einzelplan des Bundesministers des Innern in einem eigenen Kapitel auszuweisen. Die Stellen sind im Einvernehmen mit dem Bundesbeauftragten zu besetzen. Die Mitarbeiter können, falls sie mit der beabsichtigten Maßnahme nicht einverstanden sind, nur im Einvernehmen mit ihm versetzt, abgeordnet oder umgesetzt werden.

(6) Ist der Bundesbeauftragte vorübergehend an der Ausübung seines Amtes verhindert, kann der Bundesminister des Innern einen Vertreter mit der Wahrnehmung der Geschäfte beauftragen. Der Bundesbeauftragte soll dazu gehört werden.

§23 Rechtsstellung des Bundesbeauftragten für den Datenschutz

(1) Das Amtsverhältnis des Bundesbeauftragten für den Datenschutz beginnt mit der Aushändigung der Ernennungsurkunde. Es endet

1. mit Ablauf der Amtszeit,
2. mit der Entlassung.

Der Bundespräsident entläßt den Bundesbeauftragten, wenn dieser es verlangt oder auf Vorschlag der Bundesregierung, wenn Gründe vorliegen, die bei einem Richter auf Lebenszeit die Entlassung aus dem Dienst rechtfertigen. Im Falle der Beendigung des Amtsverhältnisses erhält der Bundesbeauftragte eine vom Bundespräsidenten vollzogene Urkunde. Eine Entlassung wird mit der Aushändigung der Urkunde wirksam. Auf Ersuchen des Bundesministers des Innern ist der Bundesbeauftragte verpflichtet, die Geschäfte bis zur Ernennung seines Nachfolgers weiterzuführen.

(2) Der Bundesbeauftragte darf neben seinem Amt kein anderes besoldetes Amt, kein Gewerbe und keinen Beruf ausüben und weder der Leitung oder dem Aufsichtsrat oder Verwaltungsrat eines auf Erwerb gerichteten Unternehmens noch einer Regierung oder einer gesetzgebenden Körperschaft des Bundes oder eines Landes angehören. Er darf nicht gegen Entgelt außergerichtliche Gutachten abgeben.

(3) Der Bundesbeauftragte hat dem Bundesminister des Innern Mitteilung über Geschenke zu

machen, die er in bezug auf sein Amt erhält. Der Bundesminister des Innern entscheidet über die Verwendung der Geschenke.

(4) Der Bundesbeauftragte ist berechtigt, über Personen, die ihm in seiner Eigenschaft als Bundesbeauftragter Tatsachen anvertraut haben, sowie über diese Tatsachen selbst das Zeugnis zu verweigern. Dies gilt auch für die Mitarbeiter des Bundesbeauftragten mit der Maßgabe, daß über die Ausübung dieses Rechts der Bundesbeauftragte entscheidet. Soweit das Zeugnisverweigerungsrecht des Bundesbeauftragten reicht, darf die Vorlegung oder Auslieferung von Akten oder anderen Schriftstücken von ihm nicht gefordert werden.

(5) Der Bundesbeauftragte ist, auch nach Beendigung seines Amtsverhältnisses, verpflichtet, über die ihm amtlich bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Der Bundesbeauftragte darf, auch wenn er nicht mehr im Amt ist, über solche Angelegenheiten ohne Genehmigung des Bundesministers des Innern weder vor Gericht noch außergerichtlich aussagen oder Erklärungen abgeben. Unberührt bleibt die gesetzlich begründete Pflicht, Straftaten anzuzeigen und bei Gefährdung der freiheitlichen demokratischen Grundordnung für deren Erhaltung einzutreten.

(6) Die Genehmigung, als Zeuge auszusagen, soll nur versagt werden, wenn die Aussage dem Wohle des Bundes oder eines deutschen Landes Nachteile bereiten oder die Erfüllung öffentlicher Aufgaben ernstlich gefährden oder erheblich erschweren würde. Die Genehmigung, ein Gutachten zu erstatten, kann versagt werden, wenn die Erstattung den dienstlichen Interessen Nachteile bereiten würde. § 28 des Gesetzes über das Bundesverfassungsgericht in der Fassung der Bekanntmachung vom 12. Dezember 1985 (BGBl. I S. 2229) bleibt unberührt.

(7) Der Bundesbeauftragte erhält vom Beginn des Kalendermonats an, in dem das Amtsverhältnis beginnt, bis zum Schluß des Kalendermonats, in dem das Amtsverhältnis endet, im Falle des Absatzes 1 Satz 6 bis zum Ende des Monats, in dem die Geschäftsführung endet, Amtsbezüge in Höhe der einem Bundesbeamten der Besoldungsgruppe B9 zustehenden Besoldung. Das Bundesreisekostengesetz und das Bundesumzugskostengesetz sind entsprechend anzuwenden. Im übrigen sind die §§13 bis 20 des Bundesministergesetzes in der Fassung der Bekanntmachung vom 27. Juli 1971 (BGBl. I S. 1166), zuletzt geändert durch das Gesetz zur Kürzung des Amtsgehalts der Mitglieder der Bundesregierung und der Parlamentarischen Staatssekretäre vom 22. Dezember 1982 (BGBl. I S. 2007), mit der Maßgabe anzuwenden, daß an die Stelle der zweijährigen Amtszeit in §15 Abs. 1 des Bundesministergesetzes eine Amtszeit von fünf Jahren tritt. Abweichend von Satz 3 in Verbindung mit den §§15 bis 17 des Bundesministergesetzes berechnet sich das Ruhegehalt des Bundesbeauftragten unter Hinzurechnung der Amtszeit als ruhegehaltsfähige Dienstzeit in entsprechender Anwendung des Beamtenversorgungsgesetzes, wenn dies günstiger ist und der Bundesbeauftragte sich unmittelbar vor seiner Wahl zum Bundesbeauftragten als Beamter oder Richter mindestens in dem letzten gewöhnlich vor Erreichen der Besoldungsgruppe B9 zu durchlaufenden Amt befunden hat.

§24 Kontrolle durch den Bundesbeauftragten für den Datenschutz

(1) Der Bundesbeauftragte für den Datenschutz kontrolliert bei den öffentlichen Stellen des Bundes die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz. Werden personenbezogene Daten in Akten verarbeitet oder genutzt, kontrolliert der Bundesbeauftragte die Erhebung, Verarbeitung oder Nutzung, wenn der Betroffene ihm hinreichende Anhaltspunkte dafür darlegt, daß er dabei in seinen Rechten verletzt worden ist, oder dem Bundesbeauftragten hinreichende Anhaltspunkte für eine derartige Verletzung vorliegen.

(2) Die Kontrolle des Bundesbeauftragten erstreckt sich auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach §30 der Abgabenordnung, unterliegen. Bei den Stellen des Bundes im Sinne des §2 Abs. 1 Satz 2 wird das Post- und Fernmeldegeheimnis (Artikel 10 des Grundgesetzes) eingeschränkt, soweit dies zur Ausübung der Kontrolle bei den speichernden Stellen erforderlich ist. Das Kontrollrecht erstreckt sich mit Ausnahme von Nummer 1 nicht auf den Inhalt des Post- und Fernmeldeverkehrs. Der Kontrolle durch den Bundesbeauftragten unterliegen nicht:

1. personenbezogene Daten, die der Kontrolle durch die Kommission nach §9 des Gesetzes zu Artikel 10 Grundgesetz unterliegen, es sei denn, die Kommission ersucht den Bundesbeauftragten, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten, und
2. (a) personenbezogene Daten, die dem Post- und Fernmeldegeheimnis nach Artikel 10 des Grundgesetzes unterliegen,
   (b) personenbezogene Daten, die dem Arztgeheimnis unterliegen und
   (c) personenbezogene Daten in Personalakten oder in den Akten über die Sicherheitsüberprüfung, wenn der Betroffene der Kontrolle der auf ihn bezogenen Daten im Einzelfall gegenüber dem Bundesbeauftragten für den Datenschutz widerspricht. Unbeschadet des Kontrollrechts des Bundesbeauftragten unterrichtet die öffentliche Stelle die Betroffenen in allgemeiner Form über das ihnen zustehende Widerspruchsrecht.

(3) Die Bundesgerichte unterliegen der Kontrolle des Bundesbeauftragten nur, soweit sie in Verwaltungsangelegenheiten tätig werden.

(4) Die öffentlichen Stellen des Bundes sind verpflichtet, den Bundesbeauftragten und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist dabei insbesondere

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen und Akten, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im

Zusammenhang mit der Kontrolle nach Absatz 1 stehen,
2. jederzeit Zutritt in alle Diensträume zu gewähren.

Die in §6 Abs. 2 und §19 Abs. 3 genannten Behörden gewähren die Unterstützung nur dem Bundesbeauftragten selbst und den von ihm schriftlich besonders Beauftragten. Satz 2 gilt für diese Behörden nicht, soweit die oberste Bundesbehörde im Einzelfall feststellt, daß die Auskunft oder Einsicht die Sicherheit des Bundes oder eines Landes gefährden würde.

(5) Der Bundesbeauftragte teilt das Ergebnis seiner Kontrolle der öffentlichen Stelle mit. Damit kann er Vorschläge zur Verbesserung des Datenschutzes, insbesondere zur Beseitigung von festgestellten Mängeln bei der Verarbeitung oder Nutzung personenbezogener Daten, verbinden. §25 bleibt unberührt.

(6) Absatz 2 gilt entsprechend für die öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind.

§25 Beanstandungen durch den Bundesbeauftragten für den Datenschutz

(1) Stellt der Bundesbeauftragte für den Datenschutz Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten fest, so beanstandet er dies

1. bei der Bundesverwaltung gegenüber der zuständigen obersten Bundesbehörde,
2. beim Bundeseisenbahnvermögen gegenüber dem Präsidenten,
3. bei den aus dem Sondervermögen Deutschen Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz oder dem Gesetz über Fernmeldeanlagen zusteht, gegenüber deren Vorständen,
4. bei den bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem Vorstand oder dem sonst vertretungsberechtigten Organ und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf. In den Fällen von Satz 1 Nr. 4 unterrichtet der Bundesbeauftragte gleichzeitig die zuständige Aufsichtsbehörde.

(2) Der Bundesbeauftragte kann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt.

(3) Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die auf Grund der Beanstandung des Bundesbeauftragten getroffen worden sind. Die in Absatz 1 Satz 1 Nr. 4

genannten Stellen leiten der zuständigen Aufsichtsbehörde gleichzeitig eine Abschrift ihrer Stellungnahme an den Bundesbeauftragten zu.

§26 Weitere Aufgaben des Bundesbeauftragten für den Datenschutz, Dateienregister

(1) Der Bundesbeauftragte für den Datenschutz erstattet dem Deutschen Bundestag alle zwei Jahre einen Tätigkeitsbericht. Der Tätigkeitsbericht soll auch eine Darstellung der wesentlichen Entwicklung des Datenschutzes im nicht-öffentlichen Bereich enthalten.

(2) Auf Anforderung des Deutschen Bundestages oder der Bundesregierung hat der Bundesbeauftragte Gutachten zu erstellen und Berichte zu erstatten. Auf Ersuchen des Deutschen Bundestages, des Petitionsausschusses, des Innenausschusses oder der Bundesregierung geht der Bundesbeauftragte ferner Hinweisen auf Angelegenheiten und Vorgänge des Datenschutzes bei den öffentlichen Stellen des Bundes nach. Der Bundesbeauftragte kann sich jederzeit an den Deutschen Bundestag wenden.

(3) Der Bundesbeauftragte kann der Bundesregierung und den in §12 Abs. 1 genannten Stellen des Bundes Empfehlungen zur Verbesserung des Datenschutzes geben und sie in Fragen des Datenschutzes beraten. Die in §25 Abs. 1 Nr. 1 bis 4 genannten Stellen sind durch den Bundesbeauftragten zu unterrichten, wenn die Empfehlung oder Beratung sie nicht unmittelbar betrifft.

(4) Der Bundesbeauftragte wirkt auf die Zusammenarbeit mit den öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind, sowie mit den Aufsichtsbehörden nach §38 hin.

(5) Der Bundesbeauftragte führt ein Register der automatisiert geführten Dateien, in denen personenbezogene Daten gespeichert werden. Das gilt nicht für die Dateien der in §19 Abs. 3 genannten Behörden sowie für Dateien nach §18 Abs. 3. Die öffentlichen Stellen, deren Dateien in das Register aufgenommen werden, sind verpflichtet, dem Bundesbeauftragten eine Übersicht gemäß §18 Abs. 2 Satz 2 Nr. 1 bis 6 zuzuleiten. Das Register kann von jedermann eingesehen werden. Die Angaben nach §18 Abs. 2 Satz 2 Nr. 3 und 5 über Dateien der in §6 Abs. 2 genannten Behörden unterliegen nicht der Einsichtnahme. Der Bundesbeauftragte kann im Einzelfall für andere öffentliche Stellen mit deren Einverständnis festlegen, daß einzelne Angaben nicht der Einsichtnahme unterliegen.

Dritter Abschnitt: Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen

Erster Unterabschnitt: Rechtsgrundlagen der Datenverarbeitung

§27 Anwendungsbereich

(1) Die Vorschriften dieses Abschnittes finden Anwendung, soweit personenbezogene Daten in oder aus Dateien geschäftsmäßig oder für berufliche oder gewerbliche Zwecke verarbeitet oder genutzt werden durch

1. nicht-öffentliche Stellen,
2. (a) öffentliche Stellen des Bundes, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen,
   (b) öffentliche Stellen der Länder, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, Bundesrecht ausführen und der Datenschutz nicht durch Landesgesetz geregelt ist.

In den Fällen der Nummer 2 Buchstabe a gelten anstelle des §38 die §§18, 21 und 24 bis 26.

(2) Die Vorschriften dieses Abschnittes gelten nicht für die Verarbeitung und Nutzung personenbezogener Daten in Akten, soweit es sich nicht um personenbezogene Daten handelt, die offensichtlich aus einer Datei entnommen worden sind.

§28 Datenspeicherung, -übermittlung und -nutzung für eigene Zwecke

(1) Das Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig

1. im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen,
2. soweit es zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zu der Annahme besteht, daß das schutzwürdige Interesse des Betroffenen an

dem Ausschluß der Verarbeitung oder Nutzung überwiegt,

3. wenn die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die speichernde Stelle sie veröffentlichen dürfte, es sei denn, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Verarbeitung oder Nutzung offensichtlich überwiegt,
4. wenn es im Interesse der speichernden Stelle zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluß der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

Die Daten müssen nach Treu und Glauben und auf rechtmäßige Weise erhoben werden.

(2) Die Übermittlung oder Nutzung ist auch zulässig

1. (a) soweit es zur Wahrung berechtigter Interessen eines Dritten oder öffentlicher Interessen erforderlich ist oder
   (b) wenn es sich um listenmäßig oder sonst zusammengefaßte Daten über Angehörige einer Personengruppe handelt, die sich auf
   - eine Angabe über die Zugehörigkeit des Betroffenen zu dieser Personengruppe,
   - Berufs-, Branchen- oder Geschäftsbezeichnung, - Namen,
   - Titel,
   - akademische Grade,
   - Anschrift,
   - Geburtsjahr

   beschränken und kein Grund zu der Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat. In den Fällen des Buchstabens b kann im allgemeinen davon ausgegangen werden, daß dieses Interesse besteht, wenn im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses gespeicherte Daten übermittelt werden sollen, die sich

   - auf gesundheitliche Verhältnisse,
   - auf strafbare Handlungen,
   - auf Ordnungswidrigkeiten,
   - auf religiöse oder politische Anschauungen sowie
   - bei Übermittlung durch den Arbeitgeber auf arbeitsrechtliche Rechtsverhältnisse beziehen, oder

2. wenn es im Interesse einer Forschungseinrichtung zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluß der

Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(3) Widerspricht der Betroffene bei der speichernden Stelle der Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung, ist eine Nutzung oder Übermittlung für diese Zwecke unzulässig. Widerspricht der Betroffene beim Empfänger der nach Absatz 2 übermittelten Daten der Verarbeitung oder Nutzung für Zwecke der Werbung oder der Markt- oder Meinungsforschung, hat dieser die Daten für diese Zwecke zu sperren.

(4) Der Empfänger darf die übermittelten Daten für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nur unter den Voraussetzungen der Absätze 1 und 2 zulässig. Die übermittelnde Stelle hat den Empfänger darauf hinzuweisen.

§29 Geschäftsmäßige Datenspeicherung zum Zwecke der Übermittlung

(1) Das geschäftsmäßige Speichern oder Verändern personenbezogener Daten zum Zwecke der Übermittlung ist zulässig, wenn

1. kein Grund zu der Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Speicherung oder Veränderung hat, oder
2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die speichernde Stelle sie veröffentlichen dürfte, es sei denn, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Speicherung oder Veränderung offensichtlich überwiegt.

§28 Abs. 1 Satz 2 ist anzuwenden.

(2) Die Übermittlung ist zulässig, wenn

1. (a) der Empfänger ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat oder
   (b) es sich um listenmäßig oder sonst zusammengefaßte Daten nach §28 Abs. 2 Nr. 1 Buchstabe b handelt, die für Zwecke der Werbung oder der Markt- oder Meinungsforschung übermittelt werden sollen, und
2. kein Grund zu der Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat.

§28 Abs. 2 Nr. 1 Satz 2 gilt entsprechend. Bei der Übermittlung nach Nummer 1 Buchstabe a sind die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung von der übermittelnden Stelle aufzuzeichnen. Bei der Übermittlung im automatisierten Abrufverfahren obliegt die Aufzeichnungspflicht dem Empfänger.

(3) Für die Verarbeitung oder Nutzung der übermittelten Daten gilt §28 Abs. 3 und 4.

§30 Geschäftsmäßige Datenspeicherung zum Zwecke der Übermittlung in anonymisierter Form

(1) Werden personenbezogene Daten geschäftsmäßig gespeichert, um sie in anonymisierter Form zu übermitteln, sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Diese Merkmale dürfen mit den Einzelangaben nur zusammengeführt werden, soweit dies für die Erfüllung des Zweckes der Speicherung oder zu wissenschaftlichen Zwecken erforderlich ist.

(2) Die Veränderung personenbezogener Daten ist zulässig, wenn

1. kein Grund zu der Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Veränderung hat, oder
2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die speichernde Stelle sie veröffentlichen dürfte, es sei denn, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Veränderung offensichtlich überwiegt.

(3) Die personenbezogenen Daten sind zu löschen, wenn ihre Speicherung unzulässig ist.

(4) Die §§29, 33 bis 35 gelten nicht.

§31 Besondere Zweckbindung

Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

§32 Meldepflichten

(1) Die Stellen, die personenbezogene Daten geschäftsmäßig

1. zum Zwecke der Übermittlung speichern,
2. zum Zwecke der anonymisierten Übermittlung speichern oder
3. im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen,

sowie ihre Zweigniederlassungen und unselbständigen Zweigstellen haben die Aufnahme und Beendigung ihrer Tätigkeit der zuständigen Aufsichtsbehörde innerhalb eines Monats mitzuteilen.

(2) Bei der Anmeldung sind folgende Angaben für das bei der Aufsichtsbehörde geführt Register mitzuteilen:

1. Name oder Firma der Stelle,
2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzlich oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
3. Anschrift,
4. Geschäftszwecke der Stelle und der Datenverarbeitung,
5. Name des Beauftragten für den Datenschutz,
6. allgemeine Beschreibung der Art der gespeicherten personenbezogenen Daten.

Im Falle des Absatzes 1 Nr. 3 ist diese Angabe nicht erforderlich.

(3) Bei der Anmeldung sind außerdem folgende Angaben mitzuteilen, die nicht in das Register aufgenommen werden:

1. Art der eingesetzten Datenverarbeitungsanlagen,
2. bei regelmäßiger Übermittlung personenbezogener Daten Empfänger und Art der übermittelten Daten.

(4) Absatz 1 gilt für die Änderung der nach Absätzen 2 und 3 mitgeteilten Angaben entsprechend.

(5) Die Aufsichtsbehörde kann im Einzelfall festlegen, welche Angaben nach Absatz 2 Nr. 4 und 6, Absatz 3 und Absatz 4 mitgeteilt werden müssen. Der mit den Mitteilungen verbundene Aufwand muß in einem angemessenen Verhältnis zu ihrer Bedeutung für die Überwachung durch die Aufsichtsbehörde stehen.

Zweiter Unterabschnitt: Rechte des Betroffenen

§33 Benachrichtigung des Betroffenen

(1) Werden erstmals personenbezogene Daten für eigene Zwecke gespeichert, ist der Betroffene von der Speicherung und der Art der Daten zu benachrichtigen. Werden personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert, ist der Betroffene von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen.

(2) Eine Pflicht zur Benachrichtigung besteht nicht, wenn

1. der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat,
2. die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich der Datensicherung oder der Datenschutzkontrolle dienen,
3. die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheimgehalten werden müssen,
4. die zuständige öffentliche Stelle gegenüber der speichernden Stelle festgestellt hat, daß das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
5. die Daten in einer Datei gespeichert werden, die nur vorübergehend vorgehalten und innerhalb von drei Monaten nach ihrer Erstellung gelöscht wird,
6. die Daten für eigene Zwecke gespeichert sind und
    a. aus allgemein zugänglichen Quellen entnommen sind oder
    b. die Benachrichtigung die Geschäftszwecke der speichernden Stelle erheblich gefährden würde, es sei denn, daß das Interesse an der Benachrichtigung die Gefährdung überwiegt, oder
7. die Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert sind und
    a. aus allgemein zugänglichen Quellen entnommen sind, soweit sie sich auf diejenigen Personen beziehen, die diese Daten veröffentlicht haben, oder
    b. es sich um listenmäßig oder sonst zusammengefaßte Daten handelt (§29 Abs. 2 Nr. 1 Buchstabe b).

§34 Auskunft an den Betroffenen

(1) Der Betroffene kann Auskunft verlangen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf Herkunft und Empfänger beziehen,
2. den Zweck der Speicherung und
3. Personen und Stellen, an die seine Daten regelmäßig übermittelt werden, wenn seine Daten automatisiert verarbeitet werden.

Er soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnen. Werden die personenbezogenen Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert, kann der Betroffene über Herkunft und Empfänger nur Auskunft verlangen, wenn er begründete Zweifel an der Richtigkeit der Daten geltend macht. In diesem Falle ist Auskunft über Herkunft und Empfänger auch dann zu erteilen, wenn diese Angaben nicht gespeichert sind.

(2) Der Betroffene kann von Stellen, die geschäftsmäßig personenbezogene Daten zum Zwecke der Auskunftserteilung speichern, Auskunft über seine personenbezogenen Daten verlangen, auch wenn sie nicht in einer Datei gespeichert sind. Auskunft über Herkunft und Empfänger kann der Betroffene nur verlangen, wenn er begründete Zweifel an der Richtigkeit der Daten geltend macht. §38 Abs. 1 ist mit der Maßgabe anzuwenden, daß die Aufsichtsbehörde im Einzelfall die Einhaltung von Satz 1 überprüft, wenn der Betroffene begründet darlegt, daß die Auskunft nicht oder nicht richtig erteilt worden ist.

(3) Die Auskunft wird schriftlich erteilt, soweit nicht wegen der besonderen Umstände eine andere Form der Auskunftserteilung angemessen ist.

(4) Eine Pflicht zur Auskunftserteilung besteht nicht, wenn der Betroffene nach §33 Abs. 2 Nr. 2 bis 6 nicht zu benachrichtigen ist.

(5) Die Auskunft ist unentgeltlich. Werden die personenbezogenen Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert, kann jedoch ein Entgelt verlangt werden, wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann. Das Entgelt darf über die durch die Auskunftserteilung entstandenen direkt zurechenbaren Kosten nicht hinausgehen. Ein Entgelt kann in den Fällen nicht verlangt werden, in denen besondere Umstände die Annahme rechtfertigen, daß Daten unrichtig oder unzulässig gespeichert werden, oder in denen die Auskunft ergibt, daß die Daten zu berichtigen oder unter der Voraussetzung des §35 Abs. 2 Satz 2 Nr. 1 zu löschen sind.

(6) Ist die Auskunftserteilung nicht unentgeltlich, ist dem Betroffenen die Möglichkeit zu geben, sich im Rahmen seines Auskunftsanspruchs persönlich Kenntnis über die ihn betreffenden Daten und Angaben zu verschaffen. Er ist hierauf in geeigneter Weise hinzuweisen.

§35 Berichtigung, Löschung und Sperrung von Daten

(1) personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.

(2) personenbezogene Daten können außer in den Fällen des Absatzes 3 Nr. 1 und 2 jederzeit gelöscht werden. personenbezogene Daten sind zu löschen, wenn

1. ihre Speicherung unzulässig ist,
2. es sich um Daten über gesundheitliche Verhältnisse, strafbare Handlungen, Ordnungswidrigkeiten sowie religiöse oder politische Anschauungen handelt und ihre Richtigkeit von der speichernden Stelle nicht bewiesen werden kann,
3. sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich ist, oder
4. sie geschäftsmäßig zum Zwecke der Übermittlung verarbeitet werden und eine Prüfung am Ende des fünften Kalenderjahres nach ihrer erstmaligen Speicherung ergibt, daß eine längerwährende Speicherung nicht erforderlich ist.

(3) An die Stelle einer Löschung tritt eine Sperrung, soweit

1. im Falle des Absatzes 2 Nr. 3 oder 4 einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,
2. Grund zu der Annahme besteht, daß durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder
3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

(4) personenbezogene Daten sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt.

(5) personenbezogene Daten, die unrichtig sind oder deren Richtigkeit bestritten wird, müssen bei der geschäftsmäßigen Datenspeicherung zum Zwecke der Übermittlung außer in den Fällen des Absatzes 2 Nr. 2 nicht berichtigt, gesperrt oder gelöscht werden, wenn sie aus allgemein zugänglichen Quellen entnommen und zu Dokumentationszwecken gespeichert sind. Auf Verlangen des Betroffenen ist diesen Daten für die Dauer der Speicherung seine Gegendarstellung beizufügen. Die Daten dürfen nicht ohne diese Gegendarstellung übermittelt werden.

(6) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen im Rahmen einer regelmäßigen Datenübermittlung diese Daten zur Speicherung weitergegeben werden, wenn dies zur Wahrung der schutzwürdigen Interessen des Betroffenen erforderlich ist.

(7) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn

1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerläßlich ist und
2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

Dritter Unterabschnitt: Beauftragter für den Datenschutz, Aufsichtsbehörde

§36 Bestellung eines Beauftragten für den Datenschutz

(1) Die nicht-öffentlichen Stellen, die personenbezogene Daten automatisiert verarbeiten und damit in der Regel mindestens fünf Arbeitnehmer ständig beschäftigen, haben spätestens innerhalb eines Monats nach Aufnahme ihrer Tätigkeit einen Beauftragten für den Datenschutz schriftlich zu bestellen. Das gleiche gilt, wenn personenbezogene Daten auf andere Weise verarbeitet werden und damit in der Regel mindestens zwanzig Arbeitnehmer ständig beschäftigt sind.

(2) Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt.

(3) Der Beauftragte für den Datenschutz ist dem Inhaber, dem Vorstand, dem Geschäftsführer oder dem sonstigen gesetzlich oder nach der Verfassung des Unternehmens berufenen Leiter unmittelbar zu unterstellen. Er ist bei Anwendung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Die Bestellung zum Beauftragten für den Datenschutz kann nur auf Verlangen der Aufsichtsbehörde oder in entsprechender Anwendung von §626 des Bürgerlichen Gesetzbuchs widerrufen werden.

(4) Der Beauftragte für den Datenschutz ist zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit er nicht davon durch den Betroffenen befreit wird.

(5) Die nicht-öffentliche Stelle hat den Beauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen und ihm insbesondere, soweit dies zur Erfüllung seiner Aufgaben

erforderlich ist, Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen.

§37 Aufgaben des Beauftragten für den Datenschutz

(1) Der Beauftragte für den Datenschutz hat die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz sicherzustellen. Zu diesem Zweck kann er sich in Zweifelsfällen an die Aufsichtsbehörde wenden. Er hat insbesondere

1. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen; zu diesem Zweck ist er über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten,
2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderen Vorschriften über den Datenschutz, bezogen auf die besonderen Verhältnisse in diesem Geschäftsbereich und die sich daraus ergebenden besonderen Erfordernisse für den Datenschutz, vertraut zu machen,
3. bei der Auswahl der bei der Verarbeitung personenbezogener Daten tätigen Personen beratend mitzuwirken.

(2) Dem Beauftragten ist von der nicht-öffentlichen Stelle eine Übersicht zur Verfügung zu stellen über

1. eingesetzte Datenverarbeitungsanlagen,
2. Bezeichnung und Art der Dateien,
3. Art der gespeicherten Daten,
4. Geschäftszwecke, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist,
5. deren regelmäßige Empfänger,
6. zugriffsberechtigte Personengruppen oder Personen, die allein zugriffsberechtigt sind.

(3) Absatz 2 Nr. 2 bis 6 gilt nicht für Dateien, die nur vorübergehend vorgehalten und innerhalb von drei Monaten nach ihrer Erstellung gelöscht werden.

§38 Aufsichtsbehörde

(1) Die Aufsichtsbehörde überprüft im Einzelfall die Ausführung dieses Gesetzes sowie anderer

Vorschriften über den Datenschutz, soweit diese die Verarbeitung oder Nutzung personenbezogener Daten in oder aus Dateien regeln, wenn ihr hinreichende Anhaltspunkte dafür vorliegen, daß eine dieser Vorschriften durch nicht-öffentliche Stellen verletzt ist, insbesondere wenn es der Betroffene selbst begründet darlegt.

(2) Werden personenbezogene Daten geschäftsmäßig

1. zum Zwecke der Übermittlung gespeichert,
2. zum Zwecke der anonymisierten Übermittlung gespeichert oder
3. im Auftrag durch Dienstleistungsunternehmen verarbeitet,

überwacht die Aufsichtsbehörde die Ausführung dieses Gesetzes oder anderer Vorschriften über den Datenschutz, soweit diese die Verarbeitung oder Nutzung personenbezogener Daten in oder aus Dateien regeln. Die Aufsichtsbehörde führt das Register nach §32 Abs. 2. Das Register kann von jedem eingesehen werden.

(3) Die der Prüfung unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen haben der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen. Der Auskunftspflichtige kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in §383 Abs. 1 Nr. 1 bis 3 der Zivilprozeßordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Der Auskunftspflichtige ist darauf hinzuweisen.

(4) Die von der Aufsichtsbehörde mit der Überprüfung oder Überwachung beauftragten Personen sind befugt, soweit es zur Erfüllung der der Aufsichtsbehörde übertragenen Aufgaben erforderlich ist, während der Betriebs- und Geschäftszeiten Grundstücke und Geschäftsräume der Stelle zu betreten und dort Prüfungen und Besichtigungen vorzunehmen. Sie können geschäftliche Unterlagen, insbesondere die Übersicht nach §37 Abs. 2 sowie die gespeicherten personenbezogenen Daten und die Datenverarbeitungsprogramme, einsehen. §24 Abs. 6 gilt entsprechend. Der Auskunftspflichtige hat diese Maßnahmen zu dulden.

(5) Zur Gewährleistung des Datenschutzes nach diesem Gesetz und anderen Vorschriften über den Datenschutz, soweit diese die Verarbeitung oder Nutzung personenbezogener Daten in oder aus Dateien regeln, kann die Aufsichtsbehörde anordnen, daß im Rahmen der Anforderungen nach §9 Maßnahmen zur Beseitigung festgestellter technischer oder organisatorischer Mängel getroffen werden. Bei schwerwiegenden Mängeln dieser Art, insbesondere, wenn sie mit besonderer Gefährdung des Persönlichkeitsrechts verbunden sind, kann sie den Einsatz einzelner Verfahren untersagen, wenn die Mängel entgegen der Anordnung nach Satz 1 und trotz der Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden. Sie kann die Abberufung des Beauftragten für den Datenschutz verlangen, wenn er die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit nicht besitzt.

(6) Die Landesregierungen oder die von ihnen ermächtigten Stellen bestimmen die für die Überwachung der Durchführung des Datenschutzes im Anwendungsbereich dieses Abschnittes zuständigen Aufsichtsbehörden.

(7) Die Anwendung der Gewerbeordnung auf die den Vorschriften dieses Abschnitts unterliegenden Gewerbebetriebe bleibt unberührt.

Vierter Abschnitt: Sondervorschriften

§39 Zweckbindung bei personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen

(1) personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und die von der zur Verschwiegenheit verpflichteten Stelle in Ausübung ihrer Berufs- oder Amtspflicht zur Verfügung gestellt worden sind, dürfen von der speichernden Stelle nur für den Zweck verarbeitet oder genutzt werden, für den sie sie erhalten hat. In die Übermittlung an eine nicht-öffentliche Stelle muß die zur Verschwiegenheit verpflichtete Stelle einwilligen.

(2) Für einen anderen Zweck dürfen die Daten nur verarbeitet oder genutzt werden, wenn die Änderung des Zwecks durch besonderes Gesetz zugelassen ist.

§40 Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen

(1) Für Zwecke der wissenschaftlichen Forschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für Zwecke der wissenschaftlichen Forschung verarbeitet oder genutzt werden.

(2) Die Übermittlung personenbezogener Daten an andere als öffentliche Stellen für Zwecke der wissenschaftlichen Forschung ist nur zulässig, wenn diese sich verpflichten, die übermittelten Daten nicht für andere Zwecke zu verarbeiten oder zu nutzen und die Vorschrift des Absatzes 3 einzuhalten.

(3) Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert.

(4) Die wissenschaftliche Forschung betreibenden Stellen dürfen personenbezogene Daten nur veröffentlichen, wenn

1. der Betroffene eingewilligt hat oder
2. dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerläßlich ist.

§41 Verarbeitung und Nutzung personenbezogener Daten durch die Medien

(1) Soweit personenbezogene Daten von Unternehmen oder Hilfsunternehmen der Presse oder des Films oder von Hilfsunternehmen des Rundfunks ausschließlich zu eigenen journalistisch-redaktionellen Zwecken verarbeitet oder genutzt werden, gelten von den Vorschriften dieses Gesetzes nur die §§5 und 9. Soweit Verlage personenbezogene Daten zur Herausgabe von Adressen-, Telefon-, Branchen- oder vergleichbaren Verzeichnissen verarbeiten oder nutzen, gilt Satz 1 nur, wenn mit der Herausgabe zugleich eine journalistisch-redaktionelle Tätigkeit verbunden ist.

(2) Führt die journalistisch-redaktionelle Verarbeitung oder Nutzung personenbezogener Daten durch die Rundfunkanstalten des Bundesrechts zur Veröffentlichung von Gegendarstellungen des Betroffenen, so sind diese Gegendarstellungen zu den gespeicherten Daten zu nehmen und für dieselbe Zeitdauer aufzubewahren wie die Daten selbst.

(3) Wird jemand durch eine Berichterstattung der Rundfunkanstalten des Bundesrechts in seinem Persönlichkeitsrecht beeinträchtigt, so kann er Auskunft über die der Berichterstattung zugrundeliegenden, zu seiner Person gespeicherten Daten verlangen. Die Auskunft kann verweigert werden, soweit aus den Daten auf die Person des Verfassers, Einsenders oder Gewährsmannes von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann. Der Betroffene kann die Berichtigung unrichtiger Daten verlangen.

(4) Im übrigen gelten für die Rundfunkanstalten des Bundesrechts von den Vorschriften dieses Gesetzes die §§5 und 9. Anstelle der §§24 bis 26 gilt §42, auch soweit es sich um Verwaltungsangelegenheiten handelt.

§42 Datenschutzbeauftragte der Rundfunkanstalten des Bundesrechts

(1) Die Rundfunkanstalten des Bundesrechts bestellen jeweils einen Beauftragten für den Datenschutz, der an die Stelle des Bundesbeauftragten für den Datenschutz tritt. Die Bestellung erfolgt auf Vorschlag des Intendanten durch den Verwaltungsrat für die Dauer von vier Jahren, wobei Wiederbestellungen zulässig sind. Das Amt eines Beauftragten für den Datenschutz kann neben anderen Aufgaben innerhalb der Rundfunkanstalt wahrgenommen werden.

(2) Der Beauftragte für den Datenschutz kontrolliert die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz. Er ist in Ausübung dieses Amtes unabhängig und nur dem Gesetz unterworfen. Im übrigen untersteht er der Dienst- und Rechtsaufsicht des Verwaltungsrates.

(3) Jedermann kann sich entsprechend §21 Satz 1 an den Beauftragten für den Datenschutz wenden.

(4) Der Beauftragte für den Datenschutz erstattet den Organen der jeweiligen Rundfunkanstalt des Bundesrechts alle zwei Jahre, erstmals zum 1. Januar 1994 einen Tätigkeitsbericht. Er erstattet darüber hinaus besondere Berichte auf Beschluß eines Organes der jeweiligen Rundfunkanstalt. Die Tätigkeitsberichte übermittelt der Beauftragte auch an den Bundesbeauftragten für den Datenschutz.

(5) Weitere Regelungen entsprechend den §§23 bis 26 treffen die Rundfunkanstalten des Bundesrechts jeweils für ihren Bereich. §18 bleibt unberührt.

Fünfter Abschnitt: Schlußvorschriften

§43 Strafvorschriften

(1) Wer unbefugt von diesem Gesetz geschützte personenbezogene Daten, die nicht offenkundig sind,

1. speichert, verändert oder übermittelt,

2. zum Abruf mittels automatisierten Verfahrens bereithält oder
3. abruft oder sich oder einem anderen aus Dateien verschafft,

wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer

1. die Übermittlung von durch dieses Gesetz geschützten personenbezogenen Daten, die nicht offenkundig sind, durch unrichtige Angaben erschleicht,
2. entgegen §16 Abs. 4 Satz 1, §28 Abs. 4 Satz 1, auch in Verbindung mit §29 Abs. 3, §39 Abs. 1 Satz 1 oder §40 Abs. 1 die übermittelten Daten für andere Zwecke nutzt, indem er sie an Dritte weitergibt, oder
3. entgegen §30 Abs. 1 Satz 2 die in §30 Abs. 1 Satz 1 bezeichneten Merkmale oder entgegen §40 Abs. 3 Satz 3 die in §40 Abs. 3 Satz 2 bezeichneten Merkmale mit den Einzelangaben zusammenführt.

(3) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

(4) Die Tat wird nur auf Antrag verfolgt.

§44 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen §29 Abs. 2 Satz 3oder 4 die dort bezeichneten Gründe oder die Art und Weise ihrer glaubhaften Darlegung nicht aufzeichnet,
2. entgegen §32 Abs. 1 , auch in Verbindung mit Absatz 4 , eine Meldung nicht oder nicht rechtzeitig erstattet oder entgegen §32 Abs. 2, auch in Verbindung mitAbsatz 4, bei einer solchen Meldung die erforderlichen Angaben nicht, nicht richtig oder nicht vollständig mitteilt,
3. entgegen §33 Abs. 1 den Betroffenen nicht, nicht richtig oder nicht vollständig benachrichtigt,
4. entgegen §35 Abs. 5 Satz 3 Daten ohne Gegendarstellung übermittelt,
5. entgegen §36 Abs. 1 einen Beauftragten für den Datenschutz nicht oder nicht rechtzeitig bestellt,
6. entgegen §38 Abs. 3 Satz 1eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht

rechtzeitig erteilt oder entgegen §38 Abs. 4 Satz 4 den Zutritt zu den Grundstücken oder Geschäftsräumen oder die Vornahme von Prüfungen oder Besichtigungen oder die Einsicht in geschäftliche Unterlagen nicht duldet, oder

7. einer vollziehbaren Anordnung nach §38 Abs. 5 Satz 1zuwiderhandelt.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Deutsche Mark geahndet werden.

Anlage

Werden personenbezogene Daten automatisiert verarbeitet, sind Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind,

1. Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (*Zugangskontrolle*),
2. zu verhindern, daß Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (*Datenträgerkontrolle*),
3. die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern (*Speicherkontrolle*),
4. zu verhindern, daß Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (*Benutzerkontrolle*),
5. zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (*Zugriffskontrolle*),
6. zu gewährleisten, daß überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können (*Übermittlungskontrolle*),
7. zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (*Eingabekontrolle*),
8. zu gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (*Auftragskontrolle*),
9. zu verhindern, daß bei der Übertragung personenbezogener Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (*Transportkontrolle*),
10. die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (*Organisationskontrolle*)

** Artikel 1 des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes vom 20. Dezember 1990, BGBl. I S. 2954, 2955, zuletzt geändert durch das Gesetz zur Neuordnung des Postwesens und der Telekommunikation vom 14. September 1994, BGBl. I S. 2325*

Stand: 11.11.1997

Signaturgesetz (SigG*)

Inhaltsverzeichnis

---

§1 Zweck und Anwendungsbereich

(1) Zweck des Gesetzes ist es, Rahmenbedingungen für digitale Signaturen zu schaffen, unter denen diese als sicher gelten und Fälschungen digitaler Signaturen oder Verfälschungen von signierten Daten zuverlässig festgestellt werden können.

(2) Die Anwendung anderer Verfahren für digitale Signaturen ist freigestellt, soweit nicht digitale Signaturen nach diesem Gesetz durch Rechtsvorschrift vorgeschrieben sind.

§2 Begriffsbestimmungen

(1) Eine digitale Signatur im Sinne dieses Gesetzes ist ein mit einem privaten Signaturschlüssel erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Schlüssels, der mit einem Signaturschlüssel-Zertifikat einer Zertifizierungsstelle oder der Behörde nach §3 versehen ist, den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen läßt.

(2) Eine Zertifizierungsstelle im Sinne dieses Gesetzes ist eine natürliche oder juristische Person, die die Zuordnung von öffentlichen Signaturschlüsseln zu natürlichen Personen bescheinigt und dafür eine Genehmigung gemäß §4 besitzt.

(3) Ein Zertifikat im Sinne dieses Gesetzes ist eine mit einer digitalen Signatur versehene digitale Bescheinigung über die Zuordnung eines öffentlichen Signaturschlüssels zu einer natürlichen Person (Signaturschlüssel-Zertifikat) oder eine gesonderte digitale Bescheinigung, die unter eindeutiger Bezugnahme auf ein Signaturschlüssel-Zertifikat weitere Angaben enthält (Attribut-Zertifikat).

(4) Ein Zeitstempel im Sinne dieses Gesetzes ist eine mit einer digitalen Signatur versehene digitale Bescheinigung einer Zertifizierungsstelle, daß ihr bestimmte digitale Daten zu einem bestimmten Zeitpunkt vorgelegen haben.

§3 Zuständige Behörde

Die Erteilung von Lizenzen und die Ausstellung von Zertifikaten, die zum Signieren von Zertifikaten eingesetzt werden, sowie die Überwachung der Einhaltung dieses Gesetzes und der Rechtsverordnung nach §16 obliegen der Behörde nach §66 des Telekommunikationsgesetzes .

§4 Genehmigung von Zertifizierungsstellen

(1) Der Betrieb einer Zertifizierungsstelle bedarf einer Genehmigung der zuständigen Behörde. Diese ist auf Antrag zu erteilen.

(2) Die Genehmigung ist zu versagen, wenn Tatsachen die Annahme rechtfertigen, daß der Antragsteller nicht die für den Betrieb einer Zertifizierungsstelle erforderliche Zuverlässigkeit besitzt, wenn der Antragsteller nicht nachweist, daß die für den Betrieb einer Zertifizierungsstelle erforderliche Fachkunde vorliegt, oder wenn zu erwarten ist, daß bei Aufnahme des Betriebes die übrigen Voraussetzungen für den Betrieb der Zertifizierungsstelle nach diesem Gesetz und der Rechtsverordnung nach §16 nicht vorliegen werden.

(3) Die erforderliche Zuverlässigkeit besitzt, wer die Gewähr dafür bietet, als Lizenzinhaber die für den Betrieb der Zertifizierungsstelle maßgeblichen Rechtsvorschriften einzuhalten. Die erforderliche Fachkunde liegt vor, wenn die im Betrieb der Zertifizierungsstelle tätigen Personen über die dafür erforderlichen Kenntnisse, Erfahrungen und Fertigkeiten verfügen. Die übrigen Voraussetzungen für den Betrieb der Zertifizierungsstelle liegen vor, wenn die Maßnahmen zur Erfüllung der Sicherheitsanforderungen dieses Gesetzes und der Rechtsverordnung nach §16 der zuständigen Behörde rechtzeitig in einem Sicherheitskonzept aufgezeigt und die Umsetzung durch eine von der zuständigen Behörde anerkannten Stelle geprüft und bestätigt worden ist.

(4) Die Lizenz kann mit Nebenbestimmungen versehen werden, soweit dies erforderlich ist um sicherzustellen, daß die Zertifizierungsstelle bei Aufnahme des Betriebes und im Betrieb die Voraussetzungen dieses Gesetzes und der Rechtsverordnung nach §16 erfüllt.

(5) Die zuständige Behörde stellt für Signaturschlüssel, die zum Signieren von Zertifikaten eingesetzt werden, die Zertifikate aus. Die Vorschriften für die Vergabe von Zertifikaten durch Zertifizierungsstellen gelten für die zuständige Behörde entsprechend. Diese hat die von ihr ausgestellten Zertifikate jederzeit für jeden über öffentlich erreichbare Telekommunikationsverbindungen nachprüfbar und abrufbar zu halten. Dies gilt auch für Informationen über Anschriften und Rufnummern der Zertifizierungsstellen, die Sperrung von von ihr ausgestellten Zertifikaten, die Einstellung und die Untersagung des Betriebs einer

Zertifizierungsstelle sowie die Rücknahme oder den Widerruf von Genehmigungen.

(6) Für öffentliche Leistungen nach diesem Gesetz und der Rechtsverordnung nach §16 werden Kosten (Gebühren und Auslagen) erhoben.

§5 Vergabe von Zertifikaten

(1) Die Zertifizierungsstelle hat Personen, die ein Zertifikat beantragen, zuverlässig zu identifizieren. Sie hat die Zuordnung eines öffentlichen Signaturschlüssels zu einer identifizierten Person durch ein Signaturschlüssel-Zertifikat zu bestätigen und dieses sowie Attribut-Zertifikate jederzeit für jedermann über öffentlich erreichbare Telekommunikationsverbindungen nachprüfbar und mit Zustimmung des Signaturschlüssel-Inhabers abrufbar zu halten.

(2) Die Zertifizierungsstelle hat auf Verlangen eines Antragstellers Angaben über seine Vertretungsmacht für eine dritte Person sowie zur berufsrechtlichen oder sonstigen Zulassung in das Signaturschlüssel-Zertifikat oder ein Attribut-Zertifikat aufzunehmen, soweit ihr die Einwilligung des Dritten zur Aufnahme dieser Vertretungsmacht oder die Zulassung zuverlässig nachgewiesen wird.

(3) Die Zertifizierungsstelle hat auf Verlangen eines Antragstellers im Zertifikat anstelle seines Namens ein Pseudonym aufzuführen.

(4) Die Zertifizierungsstelle hat Vorkehrungen zu treffen, damit Daten für Zertifikate nicht unbemerkt gefälscht oder verfälscht werden können. Sie hat weiter Vorkehrungen zu treffen, um die Geheimhaltung der privaten Signaturschlüssel zu gewährleisten. Eine Speicherung privater Signaturschlüssel bei der Zertifizierungsstelle ist unzulässig.

(5) Die Zertifizierungsstelle hat für die Ausübung der Zertifizierungstätigkeit zuverlässiges Personal einzusetzen. Für das Bereitstellen von Signaturschlüsseln sowie das Erstellen von Zertifikaten hat sie technische Komponenten gemäß §14 einzusetzen. Dies gilt auch für technische Komponenten, die ein Nachprüfen von Zertifikaten nach Absatz 1 Satz 2 ermöglichen.

§6 Unterrichtungspflicht

Die Zertifizierungsstelle hat die Antragsteller nach §5 Abs. 1 über die Maßnahmen zu unterrichten, die erforderlich sind, um zu sicheren digitalen Signaturen und deren zuverlässiger Prüfung beizutragen. Sie hat die Antragsteller darüber zu unterrichten, welche technischen

Komponenten die Anforderungen nach §14 Abs. 1 und 2 erfüllen, sowie über die Zuordnung der mit einem privaten Signaturschlüssel erzeugten digitalen Signaturen. Sie hat die Antragsteller darauf hinzuweisen, daß Daten mit digitaler Signatur bei Bedarf neu zu signieren sind, bevor der Sicherheitswert der vorhandenen Signatur durch Zeitablauf geringer wird.

§7 Inhalt von Zertifikaten

(1) Das Signaturschlüssel-Zertifikat muß mindestens folgende Angaben enthalten:

1. Den Namen des Signaturschlüssel-Inhabers, der im Falle einer Verwechslungsmöglichkeit mit einem Zusatz zu versehen ist, oder ein dem Signaturschlüssel-Inhaber zugeordnetes unverwechselbares Pseudonym, das als solches kenntlich sein muß,
2. den zugeordneten öffentlichen Signaturschlüssel,
3. die Bezeichnung der Algorithmen, mit denen der öffentliche Schlüssel des Signaturschlüssel-Inhabers sowie der öffentliche Schlüssel der Zertifizierungsstelle benutzt werden kann,
4. die laufende Nummer des Zertifikates,
5. Beginn und Ende der Gültigkeit des Zertifikates,
6. den Namen der Zertifizierungsstelle und
7. Angaben, ob die Nutzung des Signaturschlüssels auf bestimmte Anwendungen nach Art und Umfang beschränkt ist.

(2) Angaben zur Vertretungsmacht für eine dritte Person sowie zur berufsrechtlichen oder sonstigen Zulassung können sowohl in das Signaturschlüssel-Zertifikat als auch in ein Attribut-Zertifikat aufgenommen werden.

§8 Sperrung von Zertifikaten

(1) Die Zertifizierungsstelle hat ein Zertifikat zu sperren, wenn ein Signaturschlüssel-Inhaber oder sein Vertreter es verlangt, das Zertifikat auf Grund falscher Angaben zu §7 erwirkt wurde, sie ihre Tätigkeit beendet und diese nicht von einer anderen Zertifizierungsstelle fortgeführt wird oder die zuständige Behörde gemäß §13 Abs. 5 Satz 2 eine Sperrung anordnet. Die Sperrung muß den Zeitpunkt enthalten, von dem an sie gilt. Eine rückwirkende Sperrung ist unzulässig.

(2) Enthält ein Zertifikat Angaben einer dritten Person, so kann auch diese eine Sperrung dieses Zertifikates verlangen.

(3) Die zuständige Behörde sperrt von ihr nach §4 Abs. 5 ausgestellte Zertifikate, wenn eine Zertifizierungsstelle ihre Tätigkeit einstellt oder wenn die Genehmigung zurückgenommen oder widerrufen wird.

§9 Zeitstempel

Die Zertifizierungsstelle hat digitale Daten auf Verlangen mit einem Zeitstempel zu versehen. §5 Abs. 5 Satz 1 und 2 gilt entsprechend.

§10 Dokumentation

Die Zertifizierungsstelle hat die Sicherheitsmaßnahmen zur Einhaltung dieses Gesetzes und der Rechtsverordnung nach §16 sowie die ausgestellten Zertifikate so zu dokumentieren, daß die Daten und ihre Unverfälschtheit jederzeit nachprüfbar sind.

§11 Einstellung der Tätigkeit

(1) Die Zertifizierungsstelle hat, wenn sie ihre Tätigkeit einstellt, dies zum frühestmöglichen Zeitpunkt der zuständigen Behörde anzuzeigen und dafür zu sorgen, daß die bei Einstellung der Tätigkeit gültigen Zertifikate durch eine andere Zertifizierungsstelle übernommen werden, oder diese zu sperren.

(2) Sie hat die Dokumentation nach §10 an die Zertifizierungsstelle, welche die Zertifikate übernimmt, oder andernfalls an die zuständige Behörde zu übergeben.

(3) Sie hat einen Antrag auf Eröffnung eines Konkurs- oder Vergleichsverfahrens der zuständigen Behörde unverzüglich anzuzeigen.

§12 Datenschutz

(1) Die Zertifizierungsstelle darf personenbezogene Daten nur unmittelbar beim Betroffenen selbst und nur insoweit erheben, als dies für Zwecke eines Zertifikates erforderlich ist. Eine

Datenerhebung bei Dritten ist nur mit Einwilligung des Betroffenen zulässig. Für andere als die in Satz 1 genannten Zwecke dürfen die Daten nur verwendet werden, wenn dieses Gesetz oder eine andere Rechtsvorschrift es erlaubt oder der Betroffene eingewilligt hat.

(2) Bei einem Signaturschlüssel-Inhaber mit Pseudonym hat die Zertifizierungsstelle die Daten über dessen Identität auf Ersuchen an die zuständigen Stellen zu übermitteln, soweit dies für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes oder des Zollkriminalamtes erforderlich ist. Die Auskünfte sind zu dokumentieren.

(3) §38 des Bundesdatenschutzgesetzes findet mit der Maßgabe Anwendung, daß die Überprüfung auch vorgenommen werden darf, wenn Anhaltspunkte für eine Verletzung von Datenschutzvorschriften nicht vorliegen.

§13 Kontrolle und Durchsetzung von Verpflichtungen

(1) Die zuständige Behörde kann gegenüber Zertifizierungsstellen Maßnahmen zur Sicherstellung der Einhaltung dieses Gesetzes und der Rechtsverordnung treffen. Dazu kann sie insbesondere die Benutzung ungeeigneter technischer Komponenten untersagen und den Betrieb der Zertifizierungsstelle vorübergehend ganz oder teilweise untersagen. Personen, die den Anschein erwecken, über eine Genehmigung nach §4 zu verfügen, ohne daß dies der Fall ist, kann die Tätigkeit der Zertifizierung untersagt werden.

(2) Zum Zwecke der Überwachung nach Absatz 1 Satz 1 haben Zertifizierungsstellen der zuständigen Behörde das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu gestatten, auf Verlangen die in Betracht kommenden Bücher, Aufzeichnungen, Belege, Schriftstücke und sonstigen Unterlagen zur Einsicht vorzulegen, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren. Der zur Erteilung einer Auskunft Verpflichtete kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in §383 Absatz 1 Nr. 1 bis 3 der Zivilprozeßordnung bezeichneten Angehörigen der Gefahr der Verfolgung wegen einer Straftat oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Der zur Auskunft Verpflichtete ist auf dieses Recht hinzuweisen.

(3) Bei Nichterfüllung der Pflichten aus diesem Gesetz oder der Rechtsverordnung oder bei Entstehen eines Versagungsgrundes für eine Genehmigung hat die zuständige Behörde die erteilte Genehmigung zu widerrufen, wenn Maßnahmen nach Absatz 1 Satz 2 keinen Erfolg versprechen.

(4) Im Falle der Rücknahme oder des Widerrufs einer Lizenz oder der Einstellung der Tätigkeit einer Zertifizierungsstelle hat die zuständige Behörde eine Übernahme der Tätigkeit durch eine andere Zertifizierungsstelle oder die Abwicklung der Verträge mit den Signaturschlüssel-Inhabern sicherzustellen. Dies gilt auch bei Antrag auf Eröffnung eines Konkurs- oder Vergleichsverfahrens, wenn die genehmigte Tätigkeit nicht fortgesetzt wird.

(5) Die Gültigkeit der von einer Zertifizierungsstelle ausgestellten Zertifikate bleibt vom Widerruf einer Lizenz unberührt. Die zuständige Behörde kann eine Sperrung von Zertifikaten anordnen, wenn Tatsachen die Annahme rechtfertigen, daß Zertifikate gefälscht oder nicht hinreichend fälschungssicher sind oder daß zur Anwendung der Signaturschlüssel eingesetzte technische Komponenten Sicherheitsmängel aufweisen, die eine unbemerkte Fälschung digitaler Signaturen oder eine unbemerkte Verfälschung signierter Daten zulassen.

§14 Technische Komponenten

(1) Für die Erzeugung und Speicherung von Signaturschlüsseln sowie die Erzeugung und Prüfung digitaler Signaturen sind technische Komponenten mit Sicherheitsvorkehrungen erforderlich, die Fälschungen digitaler Signaturen und Verfälschungen signierter Daten zuverlässig erkennbar machen und gegen unberechtigte Nutzung privater Signaturschlüssel schützen.

(2) Für die Darstellung zu signierender Daten sind technische Komponenten mit Sicherheitsvorkehrungen erforderlich, die die Erzeugung einer digitalen Signatur vorher eindeutig anzeigen und feststellen lassen, auf welche Daten die digitale Signatur sich bezieht. Für die Überprüfung signierter Daten sind technische Komponenten mit Sicherheitsvorkehrungen erforderlich, die feststellen lassen, ob die signierten Daten unverändert sind, auf welche Daten die digitale Signatur sich bezieht und welchem Signaturschlüssel-Inhaber die digitale Signatur zuzuordnen ist.

(3) Bei technischen Komponenten, mit denen Signaturschlüssel-Zertifikate gemäß §5 Abs. 1 Satz 2 nachprüfbar oder abrufbar gehalten werden, sind Vorkehrungen erforderlich, um die Zertifikatverzeichnisse vor unbefugter Veränderung und unbefugtem Abruf zu schützen.

(4) Bei technischen Komponenten nach Absatz 1 bis 3 ist es erforderlich, daß sie nach dem Stand der Technik hinreichend geprüft sind und die Erfüllung der Anforderungen durch eine von der zuständigen Behörde anerkannten Stelle bestätigt ist.

(5) Bei technischen Komponenten, die nach den in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen

Wirtschaftsraum geltenden Regelungen oder Anforderungen rechtmäßig hergestellt oder in den Verkehr gebracht werden und die gleiche Sicherheit gewährleisten, ist davon auszugehen, daß die die sicherheitstechnische Beschaffenheit betreffenden Anforderungen nach Absatz 1 bis 3 erfüllt sind. In begründeten Einzelfällen ist auf Verlangen der zuständigen Behörde nachzuweisen, daß die Anforderungen nach Satz 1 erfüllt sind. Soweit zum Nachweis der die sicherheitstechnische Beschaffenheit betreffenden Anforderungen im Sinne der Absätze 1 bis 3 die Vorlage einer Bestätigung einer von der zuständigen Behörde anerkannten Stelle vorgesehen ist, werden auch Bestätigungen von in anderen Mitgliedstaaten der Europäischen Union oder in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum zugelassenen Stellen berücksichtigt, wenn die den Prüfberichten dieser Stellen zugrundeliegenden technischen Anforderungen, Prüfungen und Prüfverfahren denen der durch die zuständige Behörde anerkannten Stellen gleichwertig sind.

§15 Ausländische Zertifikate

(1) Digitale Signaturen, die mit einem öffentlichen Signaturschlüssel überprüft werden können, für den ein ausländisches Zertifikat aus einem anderen Mitgliedstaat der Europäischen Union oder aus einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum vorliegt, sind, soweit sie gleichwertige Sicherheit aufweisen, digitalen Signaturen nach diesem Gesetz gleichgestellt.

(2) Absatz 1 gilt auch für andere Staaten, soweit überstaatliche oder zwischenstaatliche Vereinbarungen über die Anerkennung der Zertifikate getroffen sind.

§16 Rechtsverordnung

Die Bundesregierung wird ermächtigt**,** durch Rechtsverordnung die zur Durchführung der §§3 bis 15 erforderlichen Rechtsvorschriften zu erlassen über

1. die näheren Einzelheiten des Verfahrens der Erteilung, Rücknahme und des Widerrufs einer Lizenz sowie des Verfahrens bei Einstellung lizenzierter Tätigkeit,
2. die gebührenpflichtigen Tatbestände nach §4 Abs. 6 und die Höhe der Gebühr,
3. die nähere Ausgestaltung der Pflichten der Zertifizierungsstellen,
4. die Gültigkeitsdauer von Signaturschlüssel-Zertifikaten,
5. die nähere Ausgestaltung der Kontrolle der Zertifizierungsstellen,
6. die näheren Anforderungen an die technischen Komponenten sowie die Prüfung technischer Komponenten und die Bestätigung, daß die Anforderungen erfüllt sind,

7. den Zeitraum sowie das Verfahren, nach dem eine neue digitale Signatur angebracht werden sollte.

** Gesetz zur Digitalen Signatur; Artikel 3 des Multimediagesetzes (Informations- und Kommunikationsdienstegesetzes, IuKDG) vom 13. Juni 1997*

Literatur Digitale Signaturen

Digitale Signaturen

- **Allgemeine Überlegungen**
- **Technische Grundlagen digitaler Signaturen**
- **Gesetzliche Regelungen und Rahmenbedingungen für digitale Signaturen (Deutschland)**
  - Allgemeiner gesetzlicher Rahmen
  - Das Signaturgesetz (*SigG)*
  - Das Telekommunikationsgesetz (*TKG*)
  - Das Informations- und Kommunikationsdienstegesetz (*IuKDG*)
  - Das Bundesdatenschutzgesetz (*BDSG*)
- **Gesetzliche Regelungen und Rahmenbedingungen in den USA**
  - Der "*Utah Digital Signature Act*"
  - Der "*Georgia Digital Signature Act*"
- **Anwendungen digitaler Signaturen**
  - Voraussetzungen für den (praktischen) Einsatz digitaler Signaturen
  - Elektronische Dokumente
  - PGP - `Pretty Good Privacy'
  - Chipkarten

Verschlüsselung

- **Einführungen und allgemeine Ausführungen**
- **Rechtliche Situation**
  - Nationale Situation
  - Internationale Situation
- **Verfahren, Standards, Zertifizierung**
  - Symmetrische Verfahren
  - Asymmetrische Verfahren
  - Steganographie
  - Hashing, Einwegfunktionen
  - Schlüsselverwaltung, Authentifizierung und Zertifizierung
- **(Un-)Sicherheit der Verschlüsselungsverfahren**

(Un-)Sicherheit elektronischer Systeme

- **(Un-)Sicherheit der Telekommunkation**
- **(Un-)Sicherheit der Verschlüsselung im digitalen Telefonnetz**
- **(Un-)Sicherheit der Verschlüsselung beim digitalen Fernsehen**
- **(Un-)Sicherheit der Geheimzahlen im Bankenwesen**
- **(Un-)Sicherheit von Chipkarten**

Sonstige Literatur

[Funk & Wagnalls]

Funk & Wagnalls New Encyclopedia.
In: Infopedia 2.0, 1993, auf CD-ROM (CD-ROM Basispaket), tewi-Verlag München

[Webster's]

Merriam Webster's Dictionary.
In: Infopedia 2.0, 1993, auf CD-ROM (CD-ROM Basispaket), tewi-Verlag München

[Microsoft LexiRom]

Microsoft: **LexiRom.**
Deutsche Ausgabe, auf CD-ROM.

[Bertelsmann Universallexikon]

Bertelsmann Universallexikon 1997.
CD-ROM.

[Holt/Morgan 1994]

Holt, William H./Morgan, Rockie J.: **UNIX. An Open Systems Dictionary.**
Resolution Business Press, Inc., Bellevue, WA, USA, 1994

[Creifelds]

Creifelds Rechtswörterbuch.
13. Auflage, C.H. Beck'sche Verlagsbuchhandlung, München, 1996

[Antike 1982]

Lexikon der Antike.
Bibliographisches Institut Leipzig, 5. Aufl., Leipzig, 1982

[Neuburger 1919]

Neuburger, Albrecht: **Die Technik des Altertums.**
R. Voigtländers Verlag in Leipzig, 1919
(Reprint erschienen im Reprint-Verlag Leipzig)

[Benjamin 1996]

Benjamin, Walter: **Das Kunstwerk im Zeitalter seiner technischen Reproduzierbarkeit.**
Suhrkamp Verlag, Frankfurt am Main, 1996

[Zimmer 1997]

Zimmer, Dieter E.: **Die Macht des Papiers.**Warum Wissenschaftler nur mit Vorbehalt elektronisch publizieren.
In: DIE ZEIT 41, 3.10.1997

[Jensen 1997]

Jensen, Anette: **Kundenorientierung erwünscht.** Das Produkt „Kirche`` auf der Suche nach einem neuen Profil.
In: die tageszeitung, 14.11.1997

[Hofmeister 1997]

Hofmeister, Wilhelm: **Schon Perikles lag falsch.**Amerikas Handelsembargo gegen Kuba ist zum Scheitern verurteilt.
In: DIE ZEIT 47, 14.11.1997

[Schulz 1997]

Winfried Schulz: **Neue Medien - Chancen und Risiken.**
In: Aus Politik und Zeitgeschichte. Beilage zur Wochenzeitung Das Parlament. 42/97, 10. Oktober 1997; S.5

[Holtz-Bacha 1997]

Christina Holtz-Bacha: **Das fragmentierte Medien-Publikum. Folgen für das politische System**.
In: Aus Politik und Zeitgeschichte. Beilage zur Wochenzeitung Das Parlament. 42/97, 10. Oktober 1997

[Warhol 1997]

Warhol, Andy zitiert nach W. Janusczak: **Andys unbekannte Seiten.**
In: ZEITmagazin Nr. 8, 14. Februar 1997

[McLuhan 1992]

McLuhan, Herbert Marshall: **Die magischen Kanäle.**
ECON Verlag 1992; Originalausgabe: Understanding Media, McGraw-Hill, 1964

[Blum 1997]

Blum, Wolfgang: **Formeln, Chips und Sonderlinge.**
In: DIE ZEIT Nr. 50 vom 5. Dezember 1997

[Bradbury 1981]

Bradbury, Ray: **Fahrenheit 451.**
Diogenes Verlag AG Zürich, 1981; Originalausgabe: Fahrenheit 451, Ballantine Books, Inc., New York 1953

[Conrad/Mertens 1990]

Conrad, Dietrich/Mertens, Klaus: **Kirchenbau im Mittelalter.**
Edition Leipzig, Leipzig, 1990; S. 167, 168

[Binding 1993]

Binding, Günther: **Baubetrieb im Mittelalter.**
Wissenschaftliche Buchgesellschaft, Darmstadt, 1993; S. 269 ff

[Electronic Telegraph 16.12.1997]

Spies like US.
In: Electronic Telegraph vom 16. Dezember 1997, Ausgabe 936. Im Internet: http://www.telegraph.com

[Hammer 1995]

Hammer, Volker: **Vertrauensinstanz**.
S.614 in: Datenschutz und Datensicherheit (DuD) 10/1995

Digitale Signaturen

Allgemeine Überlegungen

[Hartmann/Ulrich 1997]

Hartmann, Anja/Ulrich, Otto: **Digitale Signaturen im Diskurs.**
S.13-22 in: BSI, Kulturelle Beherrschbarkeit digitaler Signaturen.
SecuMedia Verlag, Ingelheim, 1997

[Heuser 1997]

Heuser, Ansgar: **Die Digitale Signatur - eine mögliche Antwort?**
S.31-35 in: BSI, Kulturelle Beherrschbarkeit digitaler Signaturen.
SecuMedia Verlag, Ingelheim, 1997

[Kumbruck 1997]

Kumbruck, Christel: **Welche Kultur braucht die digitale Signatur?** Erster Erfahrungsbericht aus der Zukunft.
S.37-52 in: BSI, Kulturelle Beherrschbarkeit digitaler Signaturen.
SecuMedia Verlag, Ingelheim, 1997

[Keese 1997]

Keese, Christoph: **Deutschland reguliert das Internet.**
In: Berliner Zeitung vom 14./15.6.1997

[Tenhaef 1997]

Tenhaef, Rainer: **Nachbesserungswünsche liegen schon auf dem Tisch.**
In: Das Parlament 35/1997

Technische Grundlagen digitaler Signaturen

[Diffie/Hellman 1976]

Diffie, Whitfield/Hellman, Martin: **New Directions in Cryptography.**
IEEE Transactions on Information Theory, 22/6, 1976.

[Damm 1995]

Damm, Frank: **Konstruktion und Analyse beweisbar sicherer elektronischer Unterschriftenverfahren**.
Dissertation an der Universität Köln; Verlag Shaker, Aachen 1995

[Wobst 1997 (II)]

Wobst, Reinhardt: **Fälschern auf der Spur.**Sicherheit digitaler Signaturen.
UNIXopen 2/97, S.46-49, AWi Aktuelles Wissen Verlagsgesellschaft mbH, Trostberg

[Fox 1996 (I)]

Fox, Dirk: **Digitale Signaturen 96.**Arbeitstagung der GI-Fachgruppe 2.5.3 "Verläßliche IT-Systeme" und TeleTrusT e.V.
Tagungsbericht.
Tagung vom 18.-19. September 1996, GMD Darmstadt

[Fox 1993]

Fox, Dirk: **Der "Digital Signature Standard": Aufwand, Implementierung und Sicherheit.**
S.333-352 in: Verläßliche Informationssysteme. Proceedings der GI-Fachtagung VIS'93, Friedrich Vieweg & Sohn Verlagsgesellschaft mbH, Braunschweig/Wiesbaden

[Pfitzmann 1991]

Pfitzmann, Birgit: **Sicherheit von herkömmlichen und Fail-Stop-Signaturen.**
KES - Zeitschrif für Kommunikations- und EDV-Sicherheit 7/5 (1991), S. 321-326

[Pfitzmann 1996]

Pfitzmann, Birgit: **Digital Signature Schemes.**General Framework and Fail-Stop Signatures.
Lecture Notes in Computer Science, Vol. 1100, Springer-Verlag, Berlin Heidelberg New York, 1996

[Greenfield 1994]

Greenfield, Jonathan S.: **Distributed Programming Paradigms with Cryptography Applications.**
Lecture Notes in Computer Science, Vol. 870, Springer-Verlag, Berlin Heidelberg New York, 1994

Gesetzliche Regelungen und Rahmenbedingungen für digitale Signaturen (Deutschland)

Allgemeiner gesetzlicher Rahmen

[Bizer 1995]

Bizer, Johann: **Der gesetzliche Regelungsbedarf digitaler Signaturverfahren.**
Datenschutz und Datensicherung (DuD) 8/1995, S.459-463, Friedrich Vieweg & Sohn Verlagsgesellschaft mbH, Braunschweig/Wiesbaden

[Bizer 1997]

Bizer, Johann: **Funktion und Voraussetzungen digitaler Signaturen aus rechtlicher Sicht.**
S.111-123 in: BSI, Kulturelle Beherrschbarkeit digitaler Signaturen.
SecuMedia Verlag, Ingelheim, 1997

Das Signaturgesetz (SigG)

[SigGB]

Amtliche Begründung zum Regierungsentwurf des Signaturgesetzes.
in: Müller, Günter/Pfitzmann, Andreas (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik, S. 411-434, Addison Wesley Longman Verlag GmbH, Bonn u.a., 1997

[Bieser 1996]

Bieser, Wendelin: **Bundesregierung plant Gesetz zur digitalen Signatur.**
Computer und Recht (CR) 9/1996, S. 564-567,...

[Ehmann 1996]

Ehmann, Eugen: Computer und Recht aktuell. **Signaturgesetz.**
Computer und Recht (CR) 9/1996, S. 578-50,...

[Schmitz 1996 (I)]

Schmitz, Ulrich: **Netznotar soll künftig elektronischen Rechtsverkehr "wasserdicht" machen.**
Computer Zeitung (CZ) 43/1996, Konradin-Verlag

[Schmitz 1996 (II)]

Schmitz, Ulrich: **Schlüssel für die elektronische Signatur sind noch lange nicht geschmiedet.**
Computer Zeitung (CZ) 48/1996, Konradin-Verlag

[Fox 1996 (II)]

Fox, Dirk: **Schriftprobe.**Verbindliche Kommunikation im Multimediagesetz.
iX 11/96, S.18, 19, Verlag Heinz Heise GmbH &Co KG, Hannover

[Schmeh 1997]

Schmeh, Klaus: **Digitale Signaturen.** Fälschungssichere Bits.
Global Online 3/97, S.66-68

[Mertes 1996]

Mertes, Paul: **Gesetz und Verordnung zur digitalen Signatur - Bewegung auf der Datenautobahn?**
Computer und Recht (CR) 12/1996, S. 769-775,...

[SigG]

Das `**Signaturgesetz**' im Wortlaut.

[SigV]

Die **Verordnung zum Signaturgesetz**im Wortlaut.

[SigB]

Bieser, Wendelin: **Begründung und Überlegungen zum Signaturgesetz.**
S. 399-434 in Müller, Günther/Pfitzmann, Andreas (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik. Band I, Addison Wesley Longman Verlag GmbH, 1997

Das Telekommunikationsgesetz (*TKG*)

[Wuermeling/Felixberger 1997]

Wuermeling, Ulrich/Felixberger, Stefan: F**ernmeldegeheimnis und Datenschutz im Telekommunikationsgesetz.**
Computer und Recht (CR) 4/1997, S. 230-238,...

[Köhntopp 1996 (I)]

Köhntopp, Marit: **Telewahn.**Bonner Regelwerke zum Thema Telekommunikation.
iX 5/1996, S.124-126, Verlag Heinz Heise GmbH &Co KG, Hannover

[TKG]

Das `**Telekommunikationsgesetz**' (TKG)im Wortlaut.

Das Informations- und Kommunikationsdienstegesetz (*IuKDG*)

[IuKDG]

Das `**Multimediagesetz**' (IuKDG) im Wortlaut.

[Bröhl 1997]

Bröhl, Georg M.: **Rechtliche Rahmenbedingungen für neue Informations- und Kommunikationsdienste.**
Computer und Recht (CR) 2/1997, S.73-79,...

[Schulzki-Haddouti 1997 (I)]

Schulzki-Haddouti, Christiane: **Das Informations- und Kommunikationsdienste-Gesetz - IuKDG.**Rechtsunsicherheit als Programm!
telepolis am 3.2.1997, http://www.heise.de/tp

Das Bundesdatenschutzgesetz

[BDSG]

Das `**Bundesdatenschutzgesetz**' (BDSG) im Wortlaut.

Anwendungen digitaler Signaturen

Voraussetzungen für den (praktischen) Einsatz digitaler Signaturen

[Schröder 1997]

Schröder, Klaus-Werner: **Digitale Signaturen - wer beherrscht wen?**
S.68-78 in: BSI, Kulturelle Beherrschbarkeit digitaler Signaturen.
SecuMedia Verlag, Ingelheim, 1997

[Flinn/Jordan 1997]

Flinn, Patrick J./Jordan, James M. III: **Using the RSA Algorithm for Encryption and Digital Signatures: Can You Encrypt, Decrypt, Sign and Verify without Infringing the RSA Patent?**
http://www.cyberlaw.com, 9. Juli 1997

[Hammer 1993]

Hammer, Volker: **Beweiswert elektronischer Signaturen.**
S.269-291 in: Verläßliche Informationssysteme. Proceedings der GI-Fachtagung VIS'93, Friedrich Vieweg & Sohn Verlagsgesellschaft mbH, Braunschweig/Wiesbaden.

[Rüßmann 199?]

Rüßmann, Helmut: **Das Beweisrecht elektronischer Dokumente.**
http://ri.jura.uni-sb.de/IfRI/jur-pc/elekdok.htm (???)

[Rosenoer 1997]

Rosenoer, Jonathan: **CyberLaw. The Law of the Internet.**
Springer-Verlag New York Berlin Heidelberg, 1997

Elektronische Dokumente und digitale Signaturen

[Kruse 1997]

Kruse, Dietrich: **Praxisfeld Gesundheitswesen.**
S.97-107 in: BSI, Kulturelle Beherrschbarkeit digitaler Signaturen.
SecuMedia Verlag, Ingelheim, 1997

[Glade 1997]

Glade, Alex: **Praxisfeld Kreditwirtschaft.**
S.94-96 in: BSI, Kulturelle Beherrschbarkeit digitaler Signaturen.
SecuMedia Verlag, Ingelheim, 1997

[Göttlinger 1997]

Göttlinger, Franz: **Elektronisches Grundbuch bei den sächsischen Grundbuchämtern.**
S.87-93 in: BSI, Kulturelle Beherrschbarkeit digitaler Signaturen.
SecuMedia Verlag, Ingelheim, 1997

[Kempf 1998]

Kempf, Dieter: ``**Ämter-Equipment hemmt die digitale Steuererklärung**''.
Interview. S.9 in Computer Zeitung (CZ) 13/1998, Konradin-Verlag

PGP - `Pretty Good Privacy'

[Shecter 1997]

Shecter, Robb: **Security and Authentication with Digital Signatures.** How one university uses PGP and digital Signatures to make its network secure.
Linux Journal, August 1997, S. 12ff, Specialized Systems Consultants, Inc. (SSC), Seattle, WA, USA.

[Luckhardt 1997]

Luckhardt, Norbert: **Prettier Good Privacy.** PGP 5.0 - jetzt als Komplettpaket.
c't 8/1997, S. 58, Verlag Heinz Heise GmbH & Co KG, Hannover

[Moreau 1996]

Moreau, Thierry: **A Probabilistic Flaw in PGP Design?**
Computers & Security Vol. 15 Num. 1, S.39-43, Elsevier Science Ltd.

[Klemm u.a. 1996]

Klemm, Andreas; Köhntopp, Marit; Schmitz, Ulrich; Simons, Peter; Wollert, Hagen: **Sicherheitsfenster.** PGP-Anwendungen unter Unix und Windows.
iX 9/1996, S. 44-52, Verlag Heinz Heise GmbH &Co KG, Hannover

[Luckhardt/Bögeholz 1996]

Luckhardt, Norbert/Bögeholz, Harald: **Schlüsselerlebnisse.**PGP-Frontends im Überblick.
c't 1/1996, S.132 ff, Verlag Heinz Heise GmbH &Co KG, Hannover

Chipkarten

[Eisele 1995]

Eisele, Raymund: **Sicherheit und Elektronische Unterschriften - SmartDisk.**
Datenschutz und Datensicherung (DuD) 7/1995, S.401-406, Friedrich Vieweg & Sohn Verlagsgesellschaft mbH, Braunschweig/Wiesbaden

---

Verschlüsselung

Einführung und allgemeine Ausführungen

[Schneier 1996]

Schneier, Bruce: **Angewandte Kryptographie.** Protokolle, Algorithmen und Sourcecode in C.
Addison-Wesley Publishing Company, Bonn u.a., 1996

[Menezes/Oorschot/Vanstone 1997]

Menezes, Alfred J.; Oorschot, Paul C. van; Vanstone, S. A.: **Handbook of Applied Cryptography.**
CRC Press, Boca Raton u.a., 1997

[Kahn 1967]

Kahn, David: **The Codebreakers: The Story of Secret Writing.**
Macmillan Publishing Corp., 1967

[Wobst 1997 (I)]

Wobst, Reinhardt: **Abenteuer Kryptologie.** Methoden, Risiken und Nutzen der Datenverschlüsselung.
Addison-Wesley Longman Verlag GmbH, Bonn u.a., 1997

[Bauer 1994]

Bauer, Friedrich L.: **Kryptologie.** Methoden und Maximen.
2. Auflage, Springer-Verlag, Berlin Heidelberg New York, 1994

[Beth/Frisch/Simmons 1991]

Beth, Thomas; Frisch, Markus; Simmons, Gustavus J.: **Public-Key Cryptography: State of the Art and Future Directions.**
Lecture Notes in Computer Science, Vol. 578, Springer-Verlag Berlin u.a., 1991

[Kippenhahn 1997]

Kippenhahn, Rudolf: **Verschlüsselte Botschaften.** Geheimschrift, Enigma und Chipkarte.
Rowohlt Verlag GmbH, Reinbek bei Hamburg, 1997

[Zimmermann 1997]

Zimmermann, Phil: **Wir alle haben etwas zu verbergen.**
Global Online 3/97, S.72, 73

[Bizer 1996]

Bizer, Johann: Kryptokontroverse - **Der Schutz der Vertraulichkeit in der Telekommunikation.**
Datenschutz und Datensicherung (DuD) 1/1996, S.5-14, Friedrich Vieweg & Sohn Verlagsgesellschaft mbH, Braunschweig/Wiesbaden

[Huhn/Pfitzmann 1996 (I)]

Huhn, Michaela/Pfitzmann, Andreas: **Technische Randbedingungen jeder Kryptoregulierung.**
Datenschutz und Datensicherung (DuD) 1/1996, S.3-26, Friedrich Vieweg & Sohn Verlagsgesellschaft mbH, Braunschweig/Wiesbaden

[Huhn/Pfitzmann 1996 (II)]

Huhn, Michaela/Pfitzmann, Andreas: **Krypto(de)regulierung.**
Datenschutznachrichten (DANA) 6/1996, S. 4 ff, Deutsche Vereinigung für Datenschutz e.V. (DVD), Bonn

[CRISIS 1996]

Cryptography's Role In Securing The Information Society.
Committee to Study National Cryptography Policy; Computer Science and Telecommunications Board; Commission on Physical Sciences, Mathematics, and Applications; National Research Council, National Academy Press, Washington, D.C. ,USA 1996

[Hagemann/Rieke 1994]

Hagemann, Hagen/Rieke, Andres: **Datenschlösser.** Grundlagen der Kryptologie.
c't 8/1994, S.230-238, Verlag Heinz Heise GmbH &Co KG, Hannover

[Luckhardt 1996]

Luckhardt, Norbert: **Qnf jne rvasnpu, tryy?**Kryptologische Begriffe und Verfahren.
c't 12/96, S.110-113, Verlag Heinz Heise GmbH &Co KG, Hannover

[Holz 1996]

Holz, Thomas: **Elektronisches Geld.**Seminararbeit.

http:/www. ???

[Kanther 1997]

Kanther, Manfred: **"Mit Sicherheit in die Informationsgesellschaft".**
Rede von Bundesinnenminister Manfred Kanther anläßlich der Eröffnung des 5. IT-Sicherheitskongresses am 28. April 1997 in Bonn; hrsg. vom Pressereferat im Bundesministerium des Innern, Graurheindorfer Straße 198, 53117 Bonn

[Tedrick 1985]

Tedrick, Tom: **On the history of cryptography during WW2, and possible new directions for cryptographic research.**
in: Advances in Cryptology - EUROCRYPT '85. Proceedings. S. 18-28. Lecture Notes in Computer Science, Vol. 219, Springer Verlag Berlin Heidelberg New York Tokyo, 1986.

Rechtliche Situation

Nationale Situation

[Koch 1997]

Koch, Alexander: **Grundrecht auf Verschlüsselung.**
Computer und Recht (CR) 2/1997, S.106-110, ...

[Dix 1997]

Dix, Alexander: **Gesetzliche Verschlüsselungsstandards - Möglichkeiten und Grenzen der Gesetzgebung.**
Computer und Recht (CR) 1/1997, S.38-43, ...

[Schulzki-Haddouti 1997 (II)]

Schulzki-Haddouti, Christiane: **Kanthers Kurs auf das Kryptoverbot. Regierungsvarianten zur Kryptoregulierung.**
telepolis 21.3.1997, http://www.heise.de/tp

[GMD-TKT 1997]

GMD Darmstadt, Institut für Telekooperationstechnik: **Kryptoverbot in Deutschland?** Kommentar von TKT zu einem möglichen Verbot von Kryptographie auf offenen Kommunikationsnetzen in Deutschland.
http://www. ???

[provet 1997]

Projektgruppe verfassungsverträgliche Technikgestaltung e.V.: **Beschränkungen kryptografischer Verfahren sind verfassungswidrig.**
http://www. ???

[ftz 199?]

Freies Telekommunikations-Zentrum Hamburg e.V.: **Rechtsfragen** ???
http://www. ???

Internationale Situation

[Günther 1997]

Günther, Andreas: **Ausfuhrkontrollen für IT-Produkte in den USA.** Aktuelle Entwicklungen im Exportkontrollrecht und in der Kryptopolitik.
Computer und Recht (CR) 4/1997, S.245-252, ...

[Rihaczek 1996]

Rihaczek, Karl: **Die Kryptokontroverse: Das Normungsverbot.**
Datenschutz und Datensicherung (DuD) 1/1996, S.15-22, Friedrich Vieweg & Sohn Verlagsgesellschaft mbH, Braunschweig/Wiesbaden

[Highland 1996]

Highland, Joseph: Random Bits & Bytes. **US Cryptographic Policy.**
Computers & Security Vol. 15 Num. 6, S.458ff, Elsevier Science Ltd.

[Koops 1996]

Koops, B. J.: **Crypto Law Survey.** (dt.) Kryptographie: Rechtliche Situation. Überblick über Kryptographie-Regulierungen weltweit.
http://www. ???

[Wright 1997]

Wright, Steven: **Assessing the Technologies of Political Control.**
Bericht an das Europäische Parlament (Nr.: PE 166 499), 1997
Internet: http://www.heise.de/tp

Verfahren, Standards, Zertifizierung

Symmetrische Verfahren

bei **[Schneier 1996]**

bei **[Menezes/Oorschot/Vanstone 1997]**

Asymmetrische Verfahren

bei **[Schneier 1996]**

bei **[Menezes/Oorschot/Vanstone 1997]**

[Hess 1997]

Hess, Erwin: **Public-Key Cryptosystems Based on Elliptic Curves.**- An Evolutionary Approach -
S. 118 in: Lecture Notes in Computer Science, Vol. 1355, Springer-Verlag, Berlin Heidelberg New York, 1997

Steganographie

[Köhntopp 1996 (II)]

Köhntopp, Marit: **Sag's durch die Blume.** Steganographie als Verschlüsselungstechnik.
iX 4/1996, S.92-96, Verlag Heinz Heise GmbH &Co KG, Hannover

[Kahn 1996]

Kahn, David: **The History of Steganography.**
in: Information Hiding. Proceedings. Lecture Notes in Computer Science, Vol. 1174. Springer-Verlag, Berlin Heidelberg New York, 1996

[Westfeld 1997]

Westfeld, Andreas: **Steganographie am Beispiel einer Videokonferenz.**
in: Müller, Günter/Pfitzmann, Andreas (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik, S.507-525, Addison Wesley Longman Verlag GmbH, Bonn u.a., 1997

Hashing

[Pieprzyk/Sadeghiyan 1993]

Pieprzyk, Josef / Sadeghiyan, Babak: **Design of Hashing Algorithms.**
Lecture Notes in Computer Science, Vol. 756, Springer-Verlag, Berlin Heidelberg New York, 1993

[Preneel 1997]

Preneel, Bart: **Hash Functions and MAC Algorithms Based on Block Ciphers.**
S. 270-282 in: Lecture Notes in Computer Science, Vol. 1355, Springer-Verlag, Berlin Heidelberg New York, 1997

Einweg-Funktionen

[Kurtz/Mahaney/Royer 1988]

Kurtz, Stuart A. / Mahaney, Stephen R. / Royer, James S.: **On the Power of 1-way Functions.**
in: CRYPTO'88. Proceedings. Lecture Notes in Computer Science, Vol. 403, Springer-Verlag, Berlin Heidelberg New York, 1988

Schlüsselverwaltung, Authentifizierung und Zertifizierung

[Jablon 1996]

Jablon, David P.: **Strong Password-Only Authenticated Key Exchange.**
Computer Communication Review Vol. 26 Num. 5, Oct. 1996, S.5ff, ACM/SIGCOMM

[Grimm 1996]

Grimm, Rüdiger: **Kryptoverfahren und Zertifizierungsinstanzen.**
Datenschutz und Datensicherung (DuD) 1/1996, S.27-36, Friedrich Vieweg & Sohn Verlagsgesellschaft mbH, Braunschweig/Wiesbaden

[Fumy 1995]

Fumy, Walter: **Authentifizierung und Schlüsselmanagement.**
Datenschutz und Datensicherung (DuD) 10/1995, S.607-613, Friedrich Vieweg & Sohn Verlagsgesellschaft mbH, Braunschweig/Wiesbaden

[Borchers 1996]

Borchers, Detlef: **Der Kampf um die Schlüsselgewalt.**
In: DIE ZEIT Nr. 25, 14. Juni 1996

[Breilmann 1996]

Breilmann, Markus: **Schlüsselposition.** Authentifizierung in offenen Netzen.
iX 10/1996, S.102-104, Verlag Heinz Heise GmbH &Co KG, Hannover

[Klein/Damm 1993]

Klein, Birgit/Damm, Frank: **Komponenten informationstechnischer Authentifikationsdienste.**
S.293-305 in: Verläßliche Informationssysteme. Proceedings der GI-Fachtagung VIS'93, Friedrich Vieweg & Sohn Verlagsgesellschaft mbH, Braunschweig/Wiesbaden

[Tsuji 1996]

Tsuji, Shigeo: **Electronic Money and Key Management from Global and Regional Points of View.**
Advances in Cryptology - ASIACRYPT '96, S.173-183, Lecture Notes in Computer Science Vol. 1163, Springer Verlag, Berlin Heidelberg New York

[Blake-Wilson/Johnson/Menezes 1997]

Blake-Wilson, S./Johnson, D./Menezes, A.: **Key Agreement Protocols and Their Security Analysis.**
Lecture Notes in Computer Science, Vol. 1355, Springer-Verlag, Berlin Heidelberg New York, 1997

(Un-)Sicherheit der Verschlüsselungsverfahren

[CZ 18/94]

Verschlüsselungsverfahren geknackt. 129stellige Codes sind unsicher.
Computer Zeitung (CZ) 18/1994, Konradin-Verlag

[Nentwig 1997]

Nentwig, Dietmar:V**erschlüsselungsprogramme benutzen einen Mix aus verschiedenen Verfahren.**
Computer Zeitung (CZ) 9/1997, Konradin-Verlag

[c't 6/1998]

Sicherheits-Notizen. Kryptowettbewerb.
c't 6/1998, S. 94, Verlag Heinz Heise GmbH &Co KG, Hannover

[Mund 1993]

Mund, Sibylle: **Sicherheitsanforderungen - Sicherheitsmaßnahmen.**
S.225-237 in: Verläßliche Informationssysteme. Proceedings der GI-Fachtagung VIS'93, Friedrich Vieweg & Sohn Verlagsgesellschaft mbH, Braunschweig/Wiesbaden

[Biskup 1993]

Biskup, Joachim: **Sicherheit von IT-Systemen als ``sogar wenn - sonst nichts - Eigenschaft''.**
S.239-254 in: Verläßliche Informationssysteme. Proceedings der GI-Fachtagung VIS'93, Friedrich Vieweg & Sohn Verlagsgesellschaft mbH, Braunschweig/Wiesbaden

---

(Un-)Sicherheit elektronischer Systeme

(Un-)Sicherheit der Telekommunikation

[Helf 1997]

Helf, Karl-Heinz: **Sicherheit in der Telekommunikation als Regulierungsaufgabe.**
Computer und Recht (CR) 6/1997, S.331-335, ..

[Jennen u.a. 1996]

Jennen, Angelika; Kersten, Heinrich; Schröder, Klaus-Werner: **Sicherheitszertifizierung des BSI.**
Computer und Recht (CR) 11/1996, S.702-704,...

[Versteegen 1997]

Versteegen, Gerhard: **Knackpunkte.** Zertifizierung nach der ITSEC.
iX 2/1997, S.120-123, Verlag Heinz Heise GmbH &Co KG, Hannover

[Ruhmann/Schulzki-Haddouti 1998]

Ruhmann, Ingo/Schulzki-Haddouti, Christiane: **Abhör-Dschungel.**Geheimdienste lesen ungeniert mit - Grundrechte werden abgebaut.
c't 5/1998, S. 82-93, Verlag Heinz Heise GmbH &Co KG, Hannover

[Pordesch/Schneider 1997]

Pordesch, Ulrich/Schneider, Michael J.: **Sichere Kommunikation in der Gesundheitsversorgung.**
in: Müller, Günter/Pfitzmann, Andreas (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik, S. 61-80, Addison Wesley Longman Verlag GmbH, Bonn u.a., 1997

(Un-)Sicherheit der Verschlüsselung im digitalen Telefonnetz

[WW 37/1997]

Hacker: **Wir haben den Code des D1-Netzes geknackt.**
Wirtschaftswoche 37/1996

bei **[Ruhmann/Schulzki-Haddouti 1998]**

(Un-)Sicherheit der Verschlüsselung beim digitalen Fernsehen

[Krimm 1997]

Krimm, Markus: **Hack des Jahres.**
PC Magazin/DOS 9/1997, S.60ff, DMV-Verlag

(Un-)Sicherheit im Bankenwesen

[Damgard/Knudsen 1994]

Damgard, Ivan B./Knudsen, Lars R.: **The Breaking of the AR Hash Function.**
in: Advances in Cryptology - EUROCRYPT '93, S. 286 ff; Lecture Notes in Computer Science Vol. 765, Springer Verlag, Berlin Heidelberg New York, 1994

[OLG Hamm (31 U 72/96)]

OLG Hamm: **Mißbrauch von EC-Karten.**
Computer und Recht (CR) 6/1997, S.339-343, ...

[Rossa 1997(I)]

Rossa, Caroline Beatrix: **Mißbrauch beim electronic cash.** Eine zivilrechtliche Bewertung.
Computer und Recht (CR) 3/1997, S.138-146, ...

[Rossa 1997(II)]

Rossa, Caroline Beatrix: **Mißbrauch beim electronic cash.** Eine strafrechtliche Bewertung.
Computer und Recht (CR) 4/1997, S.219-229, ...

[Pausch 1997]

Pausch, Manfred: **Die Sicherheit von Magnetstreifenkarten im automatisierten Zahlungsverkehr.**
Computer und Recht (CR) /1997, S.174-180, ...

[Heine 1997]

Heine, Henning: **Experte bezweifelt Sicherheit neuer PIN-Nummern**
Berliner Zeitung, 30./31. August 1997, Verlag Gruner + Jahr

[SPIEGEL 36/1997]

Spätes Eingeständnis. Die gültigen Geheimzahlen der ec-Karten sind nicht mehr sicher. In aller Eile wird ein neuer Code eingeführt.
DER SPIEGEL 36/1997, S. 104

(Un-)Sicherheit von Chipkarten

[SPIEGEL 47/1996]

Einbruch ohne Spuren.
DER SPIEGEL 47/1996, S.216, 217

[Kruse/Peuckert 1995]

Kruse, Dietrich/Peuckert, Heribert: **Chipkarte und Sicherheit.**
Datenschutz und Datensicherung (DuD) 3/1995, Friedrich Vieweg & Sohn Verlagsgesellschaft mbH, Braunschweig/ Wiesbaden

[Kocar 1996]

Kocar, Osman: **Hardwaresicherheit von Mikrochips in Chipkarten.**
Datenschutz und Datensicherung (DuD) 7/1996, S.421-424, Friedrich Vieweg & Sohn Verlagsgesellschaft mbH, Braunschweig/Wiesbaden

[Kiranas 1997]

Kiranas, Argiris: **Technische Sicherheitsmechanismen in Point-Of-Sale (POS)-Systemen (Teil 1).**
Datenschutz und Datensicherung (DuD) 7/1996, S.413-420, Friedrich Vieweg & Sohn Verlagsgesellschaft mbH, Braunschweig/Wiesbaden

[Horster 1994]

Horster, Patrick: **"Nichtstandardisierte Verfahren lassen sich nicht verbieten."**
Interview in der Computer Zeitung (CZ) 15/1994, Konradin-Verlag

[CZ 44/96]

Heiße Chipkarten geben Code preis. Neue Methode greift schon beim Abhören verschlüsselter Text.

Computer Zeitung (CZ) 44/1996, Konradin-Verlag

[Anderson/Kuhn 1996]

Anderson, Ross/Kuhn, Markus: **Tamper Resistance - a Cautionary Note.**
in: The Second USENIX Workshop on Electronic Commerce. Proceedings, Oakland, California, November 18-21, 1996, pp 1-11, ISBN 1-880446-83-9.

Using the RSA Algorithm for Encryption and Digital Signatures:

Can You Encrypt, Decrypt, Sign and Verify without Infringing the RSA Patent?

(http://www.cyberlaw.com)

Patrick J. Flinn and James M. Jordan III

Zusammenfassung des Artikels

von Robert Gehring

In der Fachliteratur zu Kryptographie findet man im jeweiligen Abschnitt zu RSA üblicherweise den Hinweis, daß der RSA-Algorithmus patentiert sei (US Pat. 4.405.829), z.B. auch bei [Schneier 1996], S.541. Damit entsteht der Eindruck, daß zum legalen Einsatz des RSA-Verfahrens eine Lizenz des Lizenzinhabers, in diesem Falle RSADSI (RSA Data Security Inc.) notwendig sei. Die Autoren des Artikels untersuchen das RSA-Patent im Detail und zeigen auf, daß es gute Gründe dafür gibt, anzunehmen, daß

- einzelne Aktionen des RSA-Verfahrens ohne Patentverletzung vorgenommen werden können, auch wenn man nicht im Besitz einer gültigen RSA-Lizenz ist
- das RSA-Patent nicht den rechtlichen Anforderungen entspricht, die in den USA für eine Patenterteilung gestellt werden

Sie weisen daraufhin, daß es sich um theoretische Überlegungen und persönliche Auffassungen handelt, die nicht als juristischer Rat zu verstehen sind. Daß diese Überlegungen nichtsdestotrotz fundiert sind, läß sich aufgrund der beruflichen Qualifikation der Autoren annehmen: Flinn und Jordan sind praktizierende Anwälte, Jordan insbesondere Patentanwalt.

Hier folgt eine Zusammenfassung ihrer Schlußfolgerungen und Argumente.

RSA-Entschlüsselung stellt keine Patentverletzung dar

Die RSA-Patentanmeldung enthält 40 Patentansprüche (*claims*), von denen 10 unabhängige Ansprüche und die restlichen 30 abhängige Ansprüche darstellen. Die bloße Operation der Entschlüsselung einer RSA-verschlüsselten[1] Nachricht wird im Patent nicht als unabhängiger Anspruch aufgeführt[2] .

Der grundlegende Anspruch ist Nummer 23, der Patentschutz für folgende Verfahren beansprucht (im Wortlaut):

> "encoding a digital message word signal M to a ciphertext word signal C, where M corresponds to a number representative of a message and
>
> 0 <= M <= n-1
>
> where n is a composite number of the form
>
> n = p * q
>
> where p and q are prime numbers, and
>
> where C is a number representative of an encoded form of message word M,
>
> wherein said encoding step comprises the step of:
>
> transforming said message word signal M to said ciphertext word signal C wherby
>
> C [is congruent to] M^e (mod n)
>
> where e is a number relatively prime to (p-1) * (q-1)."

Die Autoren führen nun folgende Schritte an, die für eine mutmaßliche Patentverletzung (*alleged infringement*) vollzogen werden müßten (Rohübersetzung):

- ☐ Kryptographische Kommunikationen herbeiführen (*establish*);
- ☐ Sicherstellen, daß die Nachricht (M) die Länge null hat, oder länger ist, und daß sie kürzer als (n-1) ist;
- ☐ Den Modulus (n) durch Auswahl und Multiplikation der Primzahlen (p) und (q) erzeugen;
- ☐ Den Verschlüsselungsexponenten (e) derart definieren, daß er teilerfremd (relativ prim) zu (p-1)*(q-1) ist;
- ☐ Die Nachricht (M) in einen Geheimtext (C) verschlüsseln, indem (M) hoch (e) bestimmt wird;
- ☐ Den Geheimtext modulo (n) reduzieren.

Der Schritt der Entschlüsselung wird in Anspruch 23 nicht aufgeführt. Insbesondere stellt eine Entschlüsselung (*decoding*) keine Verschlüsselung (*encoding*) dar, die Begriffe sind klar unterschieden und haben eine je eigene Bedeutung. Die Entschlüsselung wird in Anspruch 24 aufgeführt:

> "decoding said ciphertext word signal C to said message word signal M,
>
> wherein said decoding step comprises the step of:
>
> transforming said ciphertext word signal C, whereby:

M [is congruent to] C^d (mod n)

where d is a multiplicative inverse of e (mod (lcm ((p-1), (q-1))))."

Nun ist aber Anspruch 24 ein abhängiger Anspruch, der eingeleitet wird mit

"24. The method according to claim 23 ..."

Eine Verletzung des abhängigen Anspruches 24 durch bloßes Entschlüsseln einer RSA-verschlüsselten Nachricht ist nach amerikanischem Patentrecht nicht möglich, da der referenzierte, unabhängige Anspruch 23 die Entschlüsselung nicht aufführt. Entschlüsselung kommt ohne die in Anspruch 23 aufgeführten Aktionen aus.

Die Autoren prüften dann noch die anderen unabhängigen Ansprüche des RSA-Patentes und kamen zu dem Schluß, daß die bloße Entschlüsselung einer RSA-verschlüsselten Nachricht keine Patentverletzung darstellen könne. Dies gilt dann auch für die Verifizierung einer digitalen Signatur, die unter Verwendung des RSA-Verfahrens erzeugt wurde.

Erzeugung einer digitalen Signatur mittels RSA muß keine Patentverletzung sein

---

An dieser Stelle formulieren die Autoren etwas vorsichtiger:

"It appears that the process of *generating* an RSA signature also may be done without infringing Claim 23."

Um eine Nachricht mit RSA zu verschlüsseln, muß man über die Zahlen verfügen, mit denen die Schlüssel zusammenhängen: p, q, n, e und d. Es genügt, darüber zu verfügen. *Man muß sie nicht selbst erzeugt haben.* Der Prozeß der Schlüsselerzeugung kann unabhängig von dem der Verschlüsselung erfolgen. Dieser Prozeß fällt sicherlich unter den Patentschutz. Man kann aber einmal erzeugte Schlüssel wiederverwenden, selbst in Software die ohne RSA-Lizenz daherkommt.

Die Autoren sind der Auffassung, daß es dem RSA-Patentinhaber schwer fallen würde, nachzuweisen, daß eine *Verschlüsselung, die ohne Schlüsselerzeugung auskommt*, unter das Patent fällt. Das Verschlüsselungsverfahren mit Exponenten und modularer Arithmetik wurde nämlich bereits von Stephen Pohlig und Martin Hellman in dem nach ihnen benannten Verschlüsselungssystem eingeführt - 1975. Pohlig und Hellman traten damit bereits zwei Jahre vor dem Trio Rivest/Shamir/Adleman auf den Plan. Der einzige Unterschied zwischen RSA und Pohlig-Hellman besteht darin, das erstere das Produkt zweier Primzahlen verwenden, wogegen letztere mit einer Primzahl auskamen.

In einem Vergleich stellen die Autoren das RSA-Verfahren und das Verfahren von Pohlig und Hellman gegenüber.

	RSA-Verfahren	**Verfahren von Pohlig und Hellman**
Verschlüsselungsoperation	$C = M^e \bmod n$	$C = M^e \bmod n$
Entschlüsselungsoperation	$M = C^d \bmod n$	$M = C^d \bmod n$
Modulus	p * q (p,q sind Primzahlen)	p (p ist Primzahl)
Verschlüsselungsexponent	e, e ist teilerfremd (relativ prim) zu (p-1)*(q-1)	e, e ist teilerfremd (relativ prim) zu (p-1)
Entschlüsselungsexponent	$d = e^{-1} \bmod ((p-1)*(q-1))$	$d = e^{-1} \bmod (p-1)$

Wie ersichtlich, unterscheiden sich die Verschlüsselungs- und die Entschlüsselungsoperationen nicht, *sie sind identisch.*

Vorausgesetzt, man verfügte über die beiden Exponenten d und e, könnte man mit einer Software, die das Pohlig-Hellman-Verfahren implementiert, genauso ver- und entschlüsseln, wie mit einer RSA-Software.

Daraus schlußfolgern die Autoren, daß die RSA-Patentanmeldung ohne die aufgeführte Schlüsselerzeugung ungültig gewesen wäre, da das Pohlig-Hellman-Patent dem entgegengestanden hätte.

Anschließend wenden sich die Autoren der Frage der Beihilfe zur Patentverletzung (*contributory infringement*) zu. Sie weisen auf den entscheidenden Punkt hin, daß es eine Beihilfe zur Patentverletzung per definitionem nur geben kann, wenn es eine direkte Patentverletzung gibt, zu der beigetragen werden kann. Dies muß willentlich und wissentlich geschehen.

Unterstellt, daß dies der Fall wäre, müßte im Detail untersucht werden, wie die Beihilfe ausgestaltet wäre. Würde sie z.B. mit Mitteln vollzogen, die nicht spezifisch dazu dienen, wäre der Nachweis schwer zu führen[3].

Secure Sockets Client

Als nächstes wenden sich die Autoren einem "*Real World Example*" zu und beschreiben das Beispiel SSL-Client. Sie untersuchen die Abläufe des Schlüsselaustausches und der Verschlüsselung und kommen zu dem Schluß, daß ein Nutzer eines SSL-Clients gutgläubig davon ausgehen kann, daß alles seine Richtigkeit hat und er nichts Ungesetzliches tut.

Die fragwürdige Gültigkeit des RSA-Patents

Der letzte wesentliche Punkt in den Betrachtungen der Autoren ist der Gültigkeit des RSA-Patents gewidmet. Bis zu diesem Punkt waren sie in ihren Überlegungen immer davon ausgegangen, daß das Patent gültig ist, d.h. daß der Antrag auf Patentschutz und das Procedere seiner Einbringung mit den Regeln für die Patenterteilung konform waren. Nun untersuchen sie, ob diese Unterstellung gerechtfertigt ist.

Patentierbarkeit von Algorithmen

1972 stellte der US Supreme Court fest, daß ein Algorithmus kein

> "process, machine, manufacture, or composition of matter"

sei, wie es in Abschnitt 101 des Patentgesetzes (*Patent Act*) gefordert wird. Ein Algorithmus war im Verständnis des US Supreme Court eine

> "procedure for solving a given type of mathematical problem".

Diese Definition schloß Algorithmen von der Patentierung aus.

1981 änderte sich die Situation schlagartig, ebenfalls durch eine Entscheidung des US Supreme Court. Im Fall *Diamond vs. Dehr* wurde um einen verbesserten Prozeß zur Gummiherstellung gestritten. Die Verbesserung wurde im wesentlichen durch einen Algorithmus zur Behandlung von Gummi bei spezifischen Temperaturen repräsentiert. Der Supreme Court entschied nun, daß dadurch, daß ein Algorithmus Bestandteil eines ansonsten patentierbaren Verfahrens sei -und die Herstellung von Gummi ist prinzipiell patentierbar- nicht begründet werden könne, daß das Verfahren keinen Patentschutz nach Abschnitt 101 des

Patentgesetzes zu erhalten habe. Dem Richterspruch des Supreme Court folgten weitere Urteile von Appellationsgerichten, die genauer eingrenzten, wann und wie Algorithmen Patentschutz erhalten können.

Zur Feststellung der Patentierbarkeit eines Algorithmus' wurde der sogenannte *Freeman-Walter-Abele*-Test[4] erarbeitet, der folgendermaßen vorgenommen wird:

> Zuerst wird untersucht, ob ein mathematischer Algorithmus direkt oder indirekt in den Patentansprüchen genannt wird.
>
> Ist das der Fall, wird festgestellt, ob die Erfindung, für die Patentschutz beantragt wird, nur den Algorithmus, oder mehr umfaßt.
>
> Geht es um Schutz einzig und allein für den Algorithmus, d.h. nicht um Schutz für physikalische Elemente oder Prozeßschritte, die auf dem Algorithmus aufbauen, ist der Anspruch ungesetzlich.
>
> Wenn dagegen der Algorithmus in einem Verfahren, daß ansonsten patentierbar wäre zum Einsatz kommt, oder in einer patentierbaren Apparatur, sind die Bedingungen von Abschnitt 101 des Patentgesetzes erfüllt.

Zusammengefaßt kann ein Algorithmus patentiert werden, wenn er eine der folgenden Bedingungen erfüllt:

- ☐ Der Algorithmus ist Element eines physikalischen Prozesses.
- ☐ Der Algorithmus ist Element eines physikalischen Gerätes.

Das RSA-Verfahren und der *Freeman-Walter-Abele*-Test

Die Autoren sind der Ansicht, daß die Formulierungen im RSA-Patentantrag den Forderungen der Gerichtsurteile, die im *Freeman-Walter-Abele*-Test zum Ausdruck kommen, wohl nicht genügen dürften. Als physikalische Geräte werden genannt:

> "a communication channel", "an encoding means", "a decoding means".

Dies sind die allgemeinsten Formulierungen, die diesbezüglich überhaupt möglich sind. Daß sie ein physikalisches Gerät beschreiben, kann man eigentlich nicht behaupten. Oder was hat man sich unter einem "encoding means" vorzustellen?

Ähnlich ist es mit den Beschreibungen des physikalischen Prozesses. Dieser wird mit

> "encode" a "message word signal"

geschildert. [*Frage: Was alles ist ein "message word signal"?*]

An dieser Stelle erwähnen die Autoren weitere Fälle, in denen des um die Patentierbarkeit von Algorithmen ging und in denen Computer eine Rolle spielten. Die Urteile in diesen Fällen waren von der Natur der Eingabedaten abhängig. Die Entscheidungen fielen zugunsten der Antragsteller aus, wenn es sich um Daten handelte, die Resultat von

> "physical activity or objects"

waren. In einem Fall scheiterte der Antragsteller. Bei seinen Daten handelte es sich um Gebote von Auktionären, d.h. um das Resultat menschlichen Denkens, oder zumindest Empfindens.

Die Frage nach der Gültigkeit des RSA-Patents läßt sich unter diesen Umständen nicht mehr eindeutig beantworten.

Formalien

Als sei dies noch nicht genug, haben die Autoren noch weitere Fragwürdigkeiten aufgedeckt.

In Abschnitt 112 des Patentgesetzes werden Anforderungen an die Formulierung eines Patentantrages gestellt. Eine davon besagt, der Erfinder möge

> "set forth the best mode contemplated by the inventor of carrying out his invention".

Der Grund für diese Forderung ist, daß einem Mißbrauch des Patentschutzes vorgebeugt werden soll. Es handelt sich um eine klare Forderung, die keine Spielräume kennt.

Zurück zum Fall RSA. Es stellte sich heraus, daß Dr. Rivest im Januar 1978, also vor dem Patentantrag, ein Papier veröffenlicht hatte, das mehr Details über die Ausführung des RSA-Verfahrens beschrieb, als später im Patentantrag aufgeführt wurden[5]. Im Patentantrag wurde also nicht der "best mode of carrying out" offengelegt. Dies ist ein klarer Verstoß gegen die Regeln des Abschnitt 112 des Patentgesetzes. Aus diesem Grunde könnte das Patent ungültig sein.

Die Autoren haben noch andere Merkwürdigkeiten aufgedeckt. So vermieden es die Antragsteller, die Verwandtschaft zum Pohlig-Hellman-Verfahren zu erwähnen. Unerwähnt blieb auch eine Arbeit aus dem 19. (!) Jahrhundert zum Thema Einweg-Funktionen und Kryptographie, die bereits das Faktorisierungsproblem, auf dem RSA aufbaut, diskutiert[6].

Fazit

Die Feststellung, daß RSA patentiert sei, ist richtig. Dabei sollte man es aber nicht belassen. Wie die Autoren gezeigt haben, ist das RSA-Patent zumindest äußerst fragwürdig. Da das Patent und die Lizenzierungspolitik der Lizenzinhaber ein großes Hindernis für die Verbreitung von Digitalen Signaturen darstellen, sollte dieser Punkt weiter untersucht werden.

Einige Aktionen des RSA-Verfahrens lassen sich ausführen, ohne das Patent zu verletzen. Gerade die für den Einsatz Digitaler Signaturen so wichtige Verifikation fällt in der Regeln nicht unter das Patent.

Fußnoten

[1] Unter einer RSA-verschlüsselten Nachricht wird an dieser Stelle eine Nachricht verstanden, die entsprechend dem RSA-Algorithmus verschlüsselt wurde.

[2] Das amerikanische Patentrecht kennt unterschiedliche Arten von Patentansprüchen: unabhängige Ansprüche (*independent claims*) und abhängige Ansprüche (*dependent claims*). Abhängige Ansprüche heißen so, weil sie einen Anspruch unter Bezugnahme auf einen unabhängigen Anspruch anmelden (*incorporate by reference*). Eine eventuelle Patentverletzung muß als Verletzung eines unabhängigen Anspruches nachgewiesen werden. Ein abhängiger Patentanspruch kann nicht verletzt werden, wenn der als Bezug dienende unabhängige Anspruch nicht verletzt wurde.

[3] Es ist eine andere Spezialität des amerikanischen Rechtssystems, daß zur Feststellung der Frage, ob ein Mittel (Gerät, Verfahren) als Tatwerkzeug für die Beihilfe zur Tat zu betrachten ist, das Mittel im Ganzen und in Bezug auf die Tat untersucht wird. Stellt sich dabei heraus, daß es genügend andere Zwecke gibt, zu denen das Mittel verwandt werden kann und verwandt wird (*substantial use*), so wird es nicht als Tatwerkzeug qualifiziert. Beihilfe zur Tat wird dann in der Regel nicht unterstellt. Zum Thema `*contributory infringement*' siehe auch: [Rosenoer 1997], S.5, 6, 12, 71, 72, 82-84

[4] Der Name leitet sich von den drei entscheidenden Fällen vor Appellationsgerichten ab: *In re Walter*, *In re Freeman* und *In re Abele*.

[5] Insbesondere machte Dr. Rivest detaillierte Ausführungen zur Auswahl der Primzahlen und des Exponenten (e), die in der Patentschrift nicht enthalten sind.

[6] 1870 befaßte sich William S. Jevons damit.

Quelle	Digitale Signaturen	Verschlüsselung	Abhören etc.
Oliver Müller, LINUX-Magazin 4/97	-	**Neuer Angriff auf den Wirtschaftsstandort Deutschland** **Droht das ``Aus'' der Kryptographie in Deutschland?** Nachdem die USA den Export von Verschlüsselungstechnologien weiter engeschränkt haben, will auch die deutsche Bundesregierung nachziehen. Der Vertrieb und der Einsatz von Kryptosystemen soll verschiedenen Quellen zufolge künftig eingeschränkt und genehmigungspflichtig werden. Wer demnach in Zukunft Software und Hardware zur Verschlüsselung von Daten vertreibt oder einsetzt, die keine Möglichkeiten zum Mitlesen der Sicherheitsbehörden bieten, macht sich nach dem Willen der Regierung straftbar. ... Laut Joerg Tauss (MdB, SPD) fand am 19.12.1996 ein vertrauliches Treffen der Referenten der Innenministerien aus Bund und Ländern statt, in dem sich die Teilnehmer für eine Beschränkung des Vertriebs und des Einsatzes von Kryptosystemen aussprachen.	-

		... *S.42 ff*	
Dirk Fox, iX 5/1997	-	*siehe Abhören*	**Schutzmechanismen für's Internet** **Uneinsehbar** ... Die Sicherheitsprobleme lokaler und globaler Rechnernetze sind lange bekannt, und schon vor vielen Jahren wurden Vorschläge und Konzepte entwickelt, die diese Lücken mit informationstechnischen Mitteln, insbesondere durch Verwendung kryptographischer Protokolle und Zugangskontrollmechanismen schließen sollen. ... In absehbarer Zeit könnten daher sichere Internet-Verbindungen selbstverständlich sein - sofern die Nachfrage groß genug ist und nationale Kryptoregulierungen oder Exportbeschränkungen dies nicht verhindern. Mithören kann fast jeder Das Mithören ist die älteste und einfachste Angriffsform, ein passiver Angriff, der praktisch nicht verhindert oder festgestellt werden kann. ... Da Routing-Rechner im Internet keinerlei Überprüfung auf

			Vertrauenswürdigkeit unterliegen und insbesondere große Internet-Provider ein kommerzielles Interesse an einer Auswertung der Kommunikationsdaten zu Werbezwecken haben, kann nicht grundsätzlich davon ausgegangen werden, daß das Fernmeldegeimnis (Art. 10 GG) im Internet eine besondere Beachtung genießt. ... --- **Schutz durch Kryptographie** Schutz vor Abhörangriffen kann man durch eine Verschlüsselung der Daten erreichen. Damit wird ein Angriff nicht verhindert, wohl aber der Erfolg für den Angreifer: Ist das Verschlüsselungsverfahren gut, dann wird dieser die abgehörten Daten ohne den passenden Schlüssel nicht entschlüsseln können. ... *S.148 ff*
iX 6/1997	-	**Internet-Unternehmen suchen Krypto-Auswege** **Lobbyarbeit am Big Ben** ... Die jüngst vorgestellten Cryptography Guidelines der OECD heizen die internationale Diskussion um den Einsatz der Kryptographie wieder an.	-

...

Denn mit der vagen Festschreibung von Key-Recovery -Verfahren als künftige Standardlösung sind die wenigsten GIP-Vertreter glücklich. Auch mit der vorsichtigen Bejahung der OECD, daß Strafverfolgungsbehörden einen Zugriff auf die Kryptoschlüssel haben müßten, ist man nicht einverstanden.

...

Strittig ist vor allem der in einem Anhang zu den Richtlinien (http://www.oecd.org/dsti/iccp/crypto_e.html) ausgeführte Punkt 6, der sich mit dem `Lawful Access' befaßt.

...

Mit Kanther in die Abhörgesellschaft

In der Bundesregierung entzünden sich offenbar Meinungsverschiedenheiten am Begriff der `Informationsgesellschaft'. Während sich Justizminister Edzard Schmidt-Jortzig (FDP) für freie Kommunikation stark macht - `Verschlüsselung schafft die technische Voraussetzung dafür, daß die Idee des

Postgeheimnisses in die Zukunft übertragen werden kann' -, hält Kabinettskollege Manfred Kanther (CDU) offenbar daran fest, digitale Kommunikation per Gesetz abhörbar machen zu wollen.

...

Mit der Behauptung, Abhöraktionen leisteten einen sinnvollen Beitrag zur Verhinderung von Kriminalität, untermauerte er seine Forderung nach der ausschließlichen Verwendung von Schlüsseln, die für die Staatsorgane zugänglich sein müssen.

...

Andy Müller-Maguhn vom Chaos Computer Club hatte einen treffenden Vergleich parat: `Dies käme dem Vorschlag gleich, daß alle Bürger einen Nachschlüssel zu ihrer Wohnung und die Geheimzahl ihrer EC-Karte beim örtlichen Polizeirevier abgeben sollten.'

...

Redner von IBM und Certco versuchten im Anschluß an diese Positionen, eine Trennung zwischen Key Recovery und Key Escrow zu ziehen und die Vorteile der eigenen Lösungen darzustellen. Kritik an der künstlichen Unterscheidung (`Begriffsklauberei') äußerte vor

		allem Whitfield Diffie. ... Auf kuriose Weise schlug sich hingegen Ulrich Sandl vom Bundeswirtschaftsministerium auf die Seite der Anwender. Sandl, der als Kryptographiebeauftragter an den OECD-Verhandlungen teilgenommen hatte, sah für Deutschland die Erlaubnis starker Kryptographie kommen. ... Sandl bejahte ausdrücklich, daß eine Zugriffsmöglichkeit für die Strafverfolgungsbehörden gegeben sein muß. ... *S.14 ff*	
Oliver Müller, LINUX-Magazin 7/1997	**Einführung in die Kryptographie - Teil 1** **Achtung, Geheimsache!** ... Durch ``digitale Unterschriften'' kann man ein elektronisches Dokument signieren, ähnlich wie beim handschriftlichen Unterzeichnen eines Dokuments aus	**Einführung in die Kryptographie - Teil 1** **Achtung, Geheimsache!** Der Online-Markt boomt. Wer heute - gerade als Unternehmer - etwas auf sich hält, ist im Internet vertreten und nutzt die schnellen Kommunikationsmöglichkeiten dieses Mediums. Doch diese Präsenz bringt es mit sich, daß auch vertrauliche Daten, die nicht gerade für die Augen der Konkurrenz vorgesehen sind, über die öffentlichen Weiten und Tiefen des Internet übertragen	-

	Papier. Somit wären in Zukunft Verträge, behördliche Dokumente und ähnliches in digitaler Form denkbar. Möglich wäre es dann beispielsweise, seine Steuererklärung elektronisch zu verfassen oder Verträge online unter Dach und Fach zu bringen. ... *S.15 ff*	werden müssen. Es ist also zwingend nötig, diese Daten vor fremden Augen zu verschließen. Wen wundert es dann noch, daß Verschlüsselungstechnologien Hochkonjunktur haben. In dieser und den folgenden Ausgaben werden wir die zugrundeliegenden kryptographischen Techniken näher beleuchten und einen spannenden Einblick in das Gebiet der Verschlüsselung geben. ... *S.15 ff*	
Oliver Müller, LINUX-MAGAZIN 8/1997	-	**Einführung in die Kryptographie - Teil 2** **Steganographie** Im Zuge der Diskussion um ein Kryptokontrollgesetz taucht immer wieder der Begriff der Steganographie auf. Wenn man Informationen schon nicht ``offen'' verschlüsseln darf, versteckt man sie eben in scheinbar harmlosen Daten. Wie diese steganographischen Daten arbeiten, zeigt dieser Beitrag. ... S.21 ff	-

iX 8/1997	-	-	**Multimediagesetz passiert Bundesrat - Lauschangriff durch die Hintertür befürchtet** Das umstrittene Informations- und Kommunikationsdienstegesetz (IuKDG), auch Multimediagesetzt genannt, kann wie geplant am 1. August in Kraft treten. Der Bundesrat hat ihm am 4. Juli zugestimmt, ..., daß durch eine Änderung der Strafprozeßordnung Mobiltelefone als Peilsende für die Erstellung von Bewegungsmustern herangezogen werden könnten. Überdies sollen Sicherheitsbehörden Mobiltelefone mit Spezialgeräten direkt abhören können - egal, wieviele Unbeteiligte dabei in derselben Funkzelle dabei mitbelauscht werden. Ganz nebenbei soll auch eine Regelung zugunsten des Verfassungsschutzes erweitert werden, nach der bisher nur das Zollkriminalamt in besonders schweren Fällen (etwa Handel mit Kriegswaffen) Telefone präventiv abhören darf. *S.30*
Florian Rötzer, telepolis 8.9.1997	*siehe Verschlüsselung*	**Europäische Kommission: Freier Markt für Verschlüsselungstechniken** ... Indirekt, aber deutlich hat die europäische Kommission in einer während der European Internet Forum veröffentlichten Mitteilung über Europäische Richtlinien für digitale	-

		Unterschriften und Verschlüsselung die Versuche der amerikanischen Behörden kritisiert, auch auf globaler Ebene die Verschlüsselung zu begrenzen und Sicherheitsbehörden durch key escrow oder key recovery die Möglichkeit zu eröffnen, verschlüsselte Mitteilungen zu lesen. ...	
Wolfgang Hoffmann, DIE ZEIT, Nr. 38 vom 12.9.1997	**Was bei der Verabschiedung des sogenannten Signaturgesetzes vor Monaten befürchtet wurde, tritt nun ein.** ... Bisher ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) zuständig, das Informationssysteme sowie deren Komponenten prüft und die Datensicherheit mit dem Siegel des Bundesadlers amtlich beglaubigt. ... Jetzt schafft Innenminister **Manfred Kanther** Fakten: Zwei	-	-

	Firmen, darunter die Daimler-Benz-Tochter Debis, haben sich bereits um die private Zertifizierung unter dem Hoheitszeichen beworben. Wie aus dem Innenministerium zu erfahren ist, stehen die Verhandlungen kurz vor dem Abschluß. ...		
Hajo Passon, iX 10/1997	-	**Cryptix - ein kryptographischer Werkzeugkasten** **Auf Nummer sicher** Bei kryptographischen Anwendungen ist es nicht nur überflüssig, sondern auch gefährlich, ungenügend getestete eigene kryptografische Software einzusetzen. Die Kommerzialisierung des Internet, Intranet-Strukturen, die firmeninterne Nutzung öffentlicher Netze oder der Wunsch nach Vertraulichkeit der privaten Kommunikation - es gibt viele Faktoren, die den Bedarf nach gesichertem Datenaustausch steigen lassen. Cryptix ist ein Projekt, das kryptographische Routinen als Perl5- und als Java-Objektbibliothek - oder, wie es in korrekter Java-Terminiologie heißt - als Package zur Verfügung zu stellen. Die frei verfügbare Software entstand in	-

		Irland und unterliegt so nicht den US-Exportbeschränkungen, die dem PGP -Erfinder Philip Zimmerman das Leben schwer machten. ... *S.160 ff*	
c't 11/1997	-	**Kryptoregulierung: Gefahr für Bürgerrechte oder Chance für Europa?** Mitte September trafen sich auf Einladung von Privacy International (siehe http://www.privacy.org/pi/) namhafte Kryptologen sowie Vertreter von Regulierungsbehörden und Regierungen in den Räumen des Europäischen Parlaments in Brüssel. Die für eine nationale Schlüsselhinterlegungspflicht erforderliche Infrastruktur sei unmöglich bereitzustellen, betonten Matt Blaze (AT&T) und Carl Ellison (Cybercash). Ebenso sei es ausgeschlossen, hinterlegte Schlüssel gleichermaßen gegen den Zugriff Unbefugter zu schützen, ihre Zuordnung zu einer Person zu gewährleisten und sie dennoch ohne Zeitverzug berechtigten Einrichtungen zur Verfügung zu stellen. Ein Verzicht auf die nötige Sicherheit der Schlüssel, um die Effizienz des Verfahrens für Strafverfolgungs- und andere Behörden zu erhalten, hätte jedoch bei wachsender Bedeutung sicherer	**Ohr des Gesetzes** **Regierung will Abhörbefugnisse drastisch erweitern** ... Nun will ein Gesetzentwurf der Bundesregierung die Überweachungsvorschriften auch auf Telekommuniukation in `privaten' Netzen ausdehnen. Bisher blieben sie verschont, weil die dort benutzten Systeme keine für die Öffentlichkeit bestimmte Fernmeldeanlage darstellen. Entsprechende Änderungen an StPO , AWG und G-10-Gesetz finden sich jetzt im Entwurf eines Begleitgesetzes zum Telekommunikationsgesetz. ... Die Überwachungsvorschriften sollen sich künftig auf jeden erstrecken, der geschäftsmäßig Telekommunikationsdienstleistungen erbringt oder daran auch nur mitwirkt. Diese Formulierung deckt sich mit der Begriffsbestimmung von §3 Nr. 5 TKG und wird dort definiert als `nachhaltiges Angebot von Telekommunikation einschließlich des Angebots von

		Kommunikation für lebensnotwendige Vorgänge katastrophale Folgen. ... *S.54*	Übertragungswegen für Dritte mit und ohne Gewinnerzielungsabsicht'. ... Zum `geschäftsmäßigen Erbringen von Telekommunikationsdienstleistungen' gehören nach der Begründung des TKG-Entwurfs auch Nebenstellenanlagen in Hotels und Krankenhäusern, ... *S.136 ff*
Thomas Weihrich, GATEWAY 11/1997	-	**Internet-Sicherheit, Teil 5: Schlüsselverwaltung** **Schlüsseldienst** ... Eine Schlüsselverwaltung für das Internet sollte gut >>skalieren<<. Das heißt, der Aufwand darf bei steigender Zahl von Kommunikationspartnern nicht überproportional anwachsen. Gegenwärtig ist nur eine Methode verfügbar: Die Schlüsselverwaltung wird auf einer authentisierten Public-Key-Infrastruktur aufgebaut. Eine Alternative sind X.509-Zertifikate, die eine Institution herausgibt, die durch die öffentliche Hand dazu ermächtigt wurde. ... Eine zweite Möglichkeit ist das >>Domain Name System<< (RFC2065). Das dritte	-

		Verfahren ist das >> Web of Trust<<, ein Netz von Personen, die sich kennen. ... *S.118 ff*	

Routing-Rechner

Routing-Rechner ist ein Synonym für Router.

Router

Router - (engl.) router

Router sind Computer in Netzwerken mit paketvermittelter Kommunikation (packet switch network), wie es z.B. das Internet ist, die eine besondere Aufgabe -das Routen- übernehmen.

Sie sind dafür zuständig, die ankommenden Nachrichtenpakete auf den schnellsten Weg zum Empfänger weiterzuleiten. Dazu analysieren sie die Adresse des Empfängers und ermitteln aus internen Tabellen die nächste Station -oft wieder ein Router- auf dem Wege zum Empfänger. Fällt ein Router aus, stehen in den Tabellen der anderen alternative Router, zu denen die Pakete geleitet werden können.

Router können ganz normale Computer sein, die für diese Aufgabe eingerichtet werden. Es gibt aber auch spezielle Computer, die nur für diesen Zweck entwickelt werden. Diese erhalten ein Betriebssystem, das im Hinblick auf Netzwerk-Funktionalität optimiert ist.

Siehe auch: Routing-Rechner

packet switch network

packet switch network (engl.) - Netzwerk mit paketvermittelter Kommunikation

Netzwerk mit paketvermittelter Kommunikation

Netzwerk mit paketvermittelter Kommunikation - (engl.) packet switch network

Es gibt prinzipiell zwei Möglichkeiten, über ein Netzwerk zu kommunizieren:

1. Man kann eine direkte, ununterbrochende Verbindung zwischen Sender und Empfänger herstellen, über die kontinuierlich Nachrichten fließen können. Solche Netzwerke heißen z.B. *verbindungsorientierte Netzwerke*. Sie sind relativ teuer, da die Leitung auch dann Kosten verursacht, wenn keine Daten darüber fließen.

2. Man kann eine indirekte, unterbrechbare Verbindung zwischen Sender und Empfänger herstellen. Über eine solche Verbindung können die Nachrichten nicht kontinuierlich fließen. Zum Nachrichtenaustausch werden die Nachrichten -vom Sender unbemerkt- in kleine Teile, Pakete, zerlegt. Diese werden vom Sender nacheinander auf die Reise zum Empfänger geschickt. Bevor der Empfänger sie präsentiert bekommt, werden die Einzelteile wieder zusammengefügt. Netzwerke, die nach diesem Prinzip arbeiten, nennt man Netzwerke mit paketvermittelter Kommunikation.

Deutsch

Nachricht

Netzwerk mit paketvermittelter Kommunikation

Nutzerprofil

English

NBS - National Bureau of Standards

NDA - Non-Disclosure Agreement

NFS - Number Field Sieve

NIST - National Institute of Standards and Technology

NSA - National Security Agency

number theory

Nachricht

Nachricht - (engl.) message

Unter einer Nachrichtverstehen die Kryptologendie vom Senderverschlüsselte und an den Empfängerverschickte Information. Oft wird nicht zwischen der Information in unverschlüsselter und in ihrer verschlüsselten Form unterschieden. Beide werden dann Nachricht genannt.

Siehe auch: Klartext

message

message (engl.) - Nachricht, Mitteilung

Siehe auch: plaintext

plaintext

plaintext (engl.) - Klartext

Klartext

Klartext - (engl.) plaintext

Klartext ist der Inhalt eines Dokument, dessen verschlüsseltes Äquivalent als Geheimtext bezeichnet wird. Den Klartext hat man entweder vor der Verschlüsselung, oder man erhält ihn nach der Entschlüsselung des Geheimtextes. Somit gelten folgende Beziehungen:

1. Entschlüsselung(Geheimtext) = Klartext
2. Verschlüsselung(Klartext) = Geheimtext

Beim Klartext muß es sich nicht um Text handeln. Die Bezeichnung ist historisch gesehen zuerst für reine Texte verwendet worden. Heute bezieht sie sich auf Dokumente, was ebensogut Texte, wie Bilder oder Audiodaten sein können.

Deutsch

Parität

PIN - Personal Identification Number, Persönliche Identifikationsnummer

Pohlig-Hellman-Verfahren

PQS - Polynomisches Quadratisches Sieb

Primfaktorzerlegung

Private Key-Kryptographie

Private-Key-Verschlüsselungsverfahren

privater Schlüssel

Protokoll

Provider

Prüfsumme

PTRegG - Postwesen- und Telekommunikationsregulierungsgesetz

Public-Key-Algorithmus

Public-Key-Kommunikation

Public-Key-Kryptographie

Public-Key-Verfahren

Public-Key-Verschlüsselung

Public-Key-Verschlüsselungssystem

English

packet switch network

parity

PBC - Plaintext Block Chaining

PCA - Policiy Certification Authority

permanent secret key

PES - Proposed Encryption Standard

PGP - Pretty Good Privacy

plaintext

plaintext attack

Pohlig-Hellman

pool key

PQS - Polynomial Quadratic Sieve

private key

private key communication

private key cryptography

private key cryptosystem

protocol

public key

Geheimtext

Geheimtext - (engl.) ciphertext

Ein Geheimtext, auch Chiffrat genannt, ist das Resultat der Verschlüsselung eines Dokumentes. Das unverschlüsselte Dokument wird als Klartext bezeichnet. Die Beziehungen zwischen Geheimtext und Klartext sind:

1. Verschlüsselung(Klartext) = Geheimtext
2. Entschlüsselung(Geheimtext) = Klartext

ciphertext

ciphertext (engl.) - Geheimtext, Chiffrat

Chiffrat

Chiffrat - (engl.) cipher, ciphertext

Chiffrat ist eine alternative Bezeichnung für Geheimtext.

Deutsch

G-10-Gesetz

geheimer Schlüssel

Geheimtext

Geheimtextangriff

Geheimtextangriff mit Anpassung des gewählten Geheimtextes

Geheimtextangriff mit gewähltem Geheimtext

glaubwürdiger Dritter

English

GIP - Global Internet Project

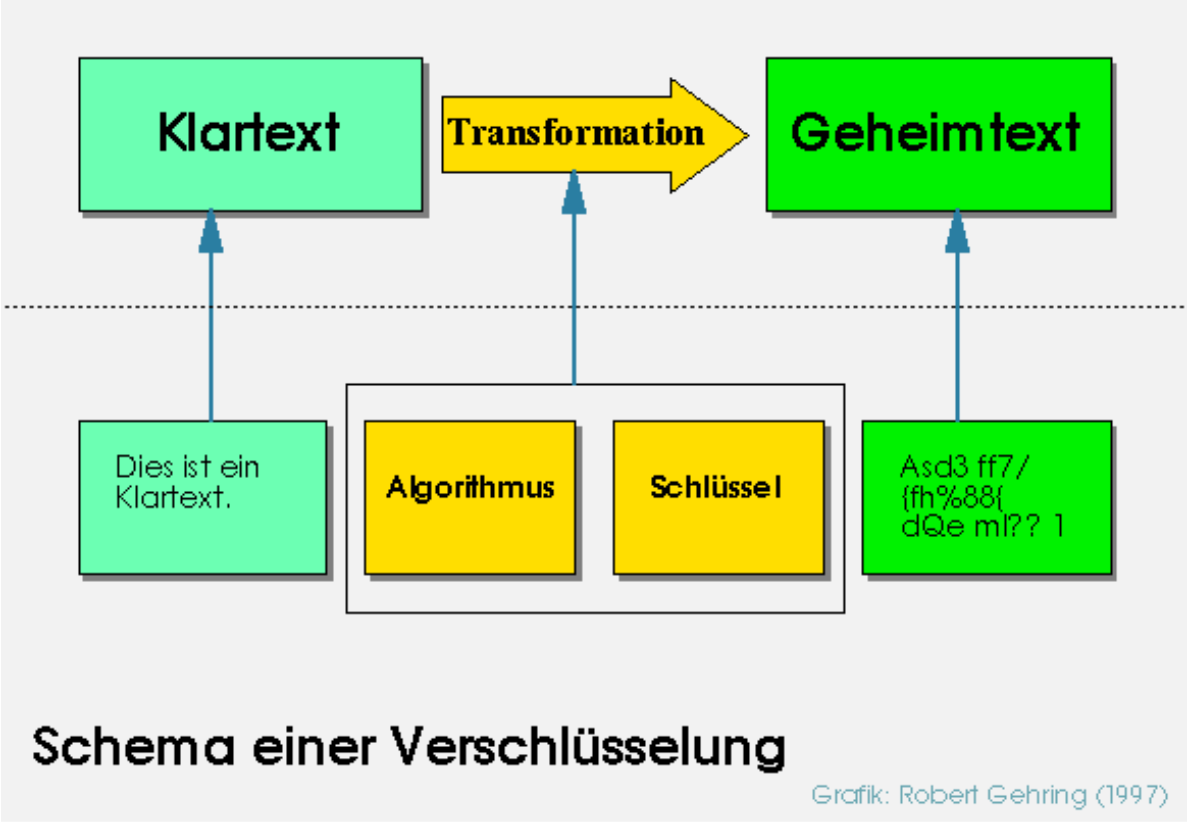
GNFS - General Number Field Sieve

Verschlüsselung

Verschlüsselung - (engl.) encryption

Unter Verschlüsselung, auch: Chiffrierung oder Codierung, versteht man die Transformation mittels geheimer Kenntnisse oder Verfahren von Informationen einer Nachricht, dem sogenannten Klartext, in eine Form, in welcher die Informationen nicht mehr ohne Zuhilfenahme geheimer Kenntnisse oder Verfahren erkannt werden können, den Geheimtext. Der umgekehrte Prozeß, d.h. das Wiederherstellen der ursprünglichen Informationen aus dem Geheimtext heißt Entschlüsselung.

Grafisch läßt sich eine Verschlüsselung folgendermaßen veranschaulichen:



Die Bezeichnungen Klartext und Geheimtext sind historisch und irreführend. In beiden Fällen muß es sich nicht um Texte handeln. Da heutzutage fast ausschließlich mit Computern verschlüsselt wird, kann es sich um nahezu beliebige Daten handeln. Die Verschlüsselung erfolgt auf Bit- oder Byteebene und unterscheidet daher nicht zwischen Qualitäten von Daten (Text, Bild, Ton).

Die Wissenschaft von der Verschlüsselung heißt Kryptographie, was aus dem Griechischen stammt (*crypto*=geheim und *graphein*=schreiben).

Verfahren

Verfahren ohne Schlüssel

Es gibt Verschlüsselungsverfahren, die ohne Schlüssel arbeiten. Deren Sicherheit beruht einzig darauf, daß der Algorithmus, der zur Verschlüsselung verwandt wird, geheim ist. Die Bedeutung dieser Verfahren ist gering, da sie extrem unflexibel sind.

Verfahren mit Schlüssel

Man unterscheidet grundsätzlich zwei Typen von Verschlüsselungsverfahren mit Schlüssel:

- symmetrische Verfahren, bei denen derselbe Schlüssel für die Verschlüsselung und für die Entschlüsselung zum Einsatz kommt
- asymmetrische Verfahren, die für Verschlüsselung und Entschlüsselung unterschiedliche Schlüssel verwenden

Eine Kombination aus beiden bezeichnet man als hybrides Verfahren.

Arbeitsweisen

Man unterscheidet bei symmetrischen Verschlüsselungsverfahren zusätzlich auch danach, wie sie bei der Verschlüsselung des Klartextes vorgehen. Die zwei Typen sind:

- Blockchiffrierungen, die eine feste Anzahl von Daten (Zeichen) des Klartextes verschlüsseln
- Stromchiffrierungen, die jedes einzelne Datum (Zeichen) des Klartextes verschlüsseln

---

encryption

encryption (engl.) - Verschlüsselung, Chiffrierung

Chiffrierung

Chiffrierung - (engl.) encryption, cipher

Chiffrierung ist ein Synonym für Verschlüsselung.

Codierung

Codierung - (engl.) encryption

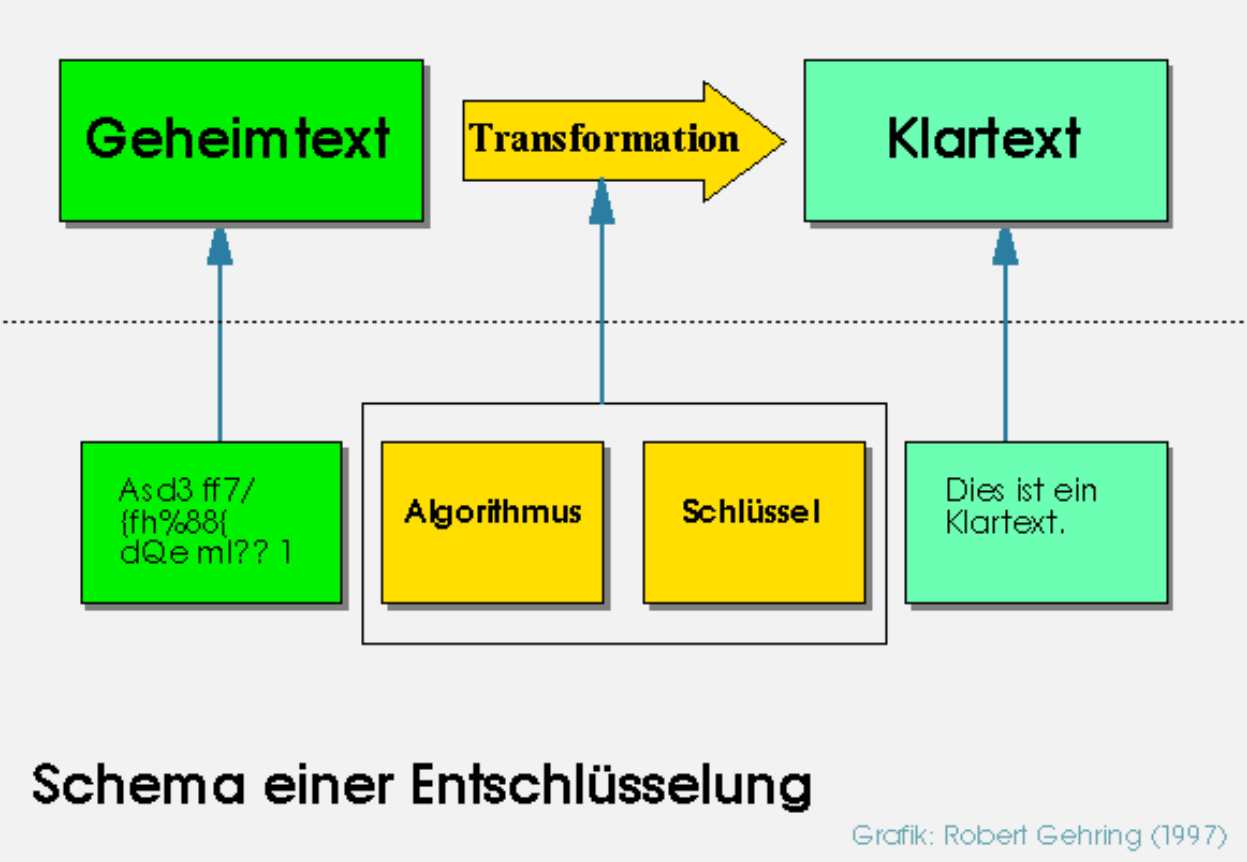
Codierungist ein seltener gebrauchtes Synonym für Verschlüsselung.

Entschlüsselung

Entschlüsselung - (engl.) decryption

Die Entschlüsselungist die Übersetzung eines Geheimtextesin einen Klartext. Dazu benötigt man spezielle, in der Regel geheime Kenntnisse.

Schematisch stellt sich die Entschlüsselung so dar:



Es lassen sich zwei grundsätzliche Varianten der Entschlüsselung unterscheiden.

1. Die befugte Entschlüsselung, die durch den vorgesehenen Empfänger des Geheimtextes bei Kenntnis von Verschlüsselungsverfahren und Schlüssel durchgeführt wird.
2. Die unbefugte Entschlüsselung, die durch andere Personen, als durch den vorgesehenen Empfänger des

Geheimtextes durchgeführt wird. Die systematisch betriebene, unbefugte Entschlüsselung ist die Kryptanalyse. Die unbefugte Entschlüsselung bezeichnet man auch als *Brechen des Codes*.

Die Verschlüsselungist der zur Entschlüsselunginverse Prozeß.

Eingangsseite Index Mail
digitale signaturen diplomarbeit · robert gehring

Kryptographie

Die Kryptographie ist ein Teilgebiet der `Kryptologie'. Das zweite Teilgebiet der `Kryptologie' ist die `Kryptanalyse'.

`Kryptographie' und `Kryptanalyse' verhalten sich komplementär zueinander: Mittels `Kryptographie' wird verschlüsselt und mittels `Kryptanalyse' wird entschlüsselt.

Die `Kryptographie' stellt sich die Aufgabe, Informationen für diejenigen unzugänglich zu machen, die sie nicht verstehen sollen. Anders gesagt werden Informationen so aufbereitet, daß sie nur die Person verstehen kann, die dafür vorgesehen ist. Ziel dieser Anstrengungen ist es, Informationen geheim zu halten. Die Gründe für eine solche Geheimhaltung sind unterschieldicher Art: Schutz von Staatsgeheimnissen, Schutz wirtschaftlicher Interessen und Schutz privaten Informationsaustausches.

Funkt & Wagnalls New Encyclopedia [Funk & Wagnalls] beginnt folgendermaßen, den Begriff zu erklären (Zitat):

> **"CRYPTOGRAPHY,**
>
> science of preparing communication intended to be intelligible only to the person possessing the key, or method of developing the hidden meaning by cryptoanalysis using apparently incoherent text. In its widest sense, cryptography includes the use of concealed messages, ciphers, and codes.
> ..."

Folgt man dieser Definition, so zählt die `Steganographie' (Verstecken von Informationen in anderen Informationen) ebenfalls zur `Kryptographie'. Andere Autoren, so z.B. R. Wobst in [Wobst 1997 (I)] definieren den Begriff enger, als Wissenschaft von Design, Entwurf und Realisierung von Verschlüsselungsalgorithmen.

Kleine Geschichte der kryptographischen Methoden

Eine der ältesten Verschlüsselungsmethoden benutzte Cäsar: Der zu übermittelnde Text wurde aufgeschrieben. Anschließend wurde er buchstabenweise verschlüsselt, indem jeder einzelne Buchstabe durch denjenigen Buchstaben ersetzt wurde, der im Alphabet drei Stellen nach ihm stand. So wurde aus einem `A' ein `D', gemäß der Folge `A'(1), `B'(2), `C'(3), `D'(4), ... Die letzten Buchstaben des Alphabets wurden dabei durch die ersten ersetzt.

Eine andere, sehr alte Methode ist die, das Alphabet in umgekehrter Reihenfolge zu benutzen, d.h. anstelle eines `A' würden wir ein `Z' schreiben; `Y' stünde für `B', usw. usf.

Beide Methoden stellen kein großes Hindernis bei der Entschlüsselung des Textes dar, da sich die Häufigkeit der Zeichen im verschlüsselten Text nicht von der realen Häufigkeit der Zeichen des Alphabets unterscheidet. Wenn man z. B. weiß, daß der Buchstabe `E' (`e') mit ca. 13% Wahrscheinlichkeit in einem Text vorhanden ist, und man feststellt, daß bei der Cäsar-Methode das Zeichen `H' mit 13% Häufigkeit auftritt, so fällt es leicht, in dem Text "*nohh*" die letzen Zeichen als "*ee*" zu identifizieren. Analog wäre bei der zweiten Methode vorzugehen.

Die Schwäche der beiden Methoden besteht in der Eineindeutigkeit, mit der die Zeichen aufeinander abgebildet werden.

Ein Versuch, dem zu begegnen, bestand darin, nicht einzelne Buchstaben zu ersetzen, sondern Zeichenpaare (`polygraphische Substitution'). Solche Texte kann man mit der Untersuchung von Paarhäufigkeiten entschlüsseln. Voraussetzung dafür ist allerdings, daß die Ausgangssprache bekannt ist. Wenn einzelne Zeichen des Ausgangsalphabets durch verschiedene Zeichen des Schlüsselalphabets ersetzt werden, nennt man das `homophone Substitution'.

Anfang des 20. Jahrhunderts wurden sogenannte mechanische Rotormaschinen entwickelt. Mit diesen konnte man wesentlich aufwendigere, polyalphabetische Substitutionen durchführen. Eine Weiterentwicklung führte zu den elektromechanischen Rotormaschinen, deren berühmteste Ausführung die "Enigma" wurde.

Alle diese Verfahren werden unter dem Begriff "Substitutionsverfahren" zusammengefaßt. Sie waren in dieser und jener Form jahrhundertelang die gebräuchlichsten Verfahren.

Ein anderer Ansatz liegt den Transpositionsverfahren zugrunde. Dabei werden die Buchstaben nicht durch andere Buchstaben nach einem Schema ersetzt. sondern ihre Position innerhalb des Textes wird entsprechend einem Schema vertauscht. Verfahren diesen Typs haben nie die Bedeutung der Substitutionsverfahren erlangt.

Die einzige wirklich sichere Methode, Informationen zu verschlüsseln, besteht darin, ohne statistisch wertvolle Informationen zu verschlüsseln. Dies bedeutet, daß es keinen funktional bestimmten Schlüssel gibt. Genauer gesagt, wird folgendermaßen vorgegangen:

> Es wird ein Schlüssel erzeugt, dessen Länge mindestens gleich groß der zu verschlüsselnden Information ist. Bei einem Text mit 70 Zeichen, muß der Schlüssel also mindestens die Länge 70 Zeichen haben. Alle Zeichen des Schlüssels müssen mit gleicher Wahrscheinlichkeit vorkommen, um einer Kryptanalyse mit statistischen Mitteln vorzubeugen. Dann wird die zu verschlüsselnde Information mit dem Schlüssel verknüpft, indem die Buchstaben des Ausgangstextes zu den Buchstaben des Schlüssels `addiert' werden und das Resultat entsprechend der Anzahl der Buchstaben im Ausgangsalphabet normiert wird.
>
> Bsp. (nach [Schneier 1996], S.17/18):
>
> Das Ausgangsalphabet hat 26 Buchstaben (A-Z). Das Alphabet für den Schlüssel muß dann ebenfalls 26 Buchstaben haben. Um das Wort "ONETIMEPAD" zu verschlüsseln, wird der Schlüssel "TBFRGFARFM" verwendet, der zuvor noch nie verwendet wurde und dessen einzelne Zeichen zufällig ausgewählt wurden. Die Position der einzelnen Zeichen entspricht der alphabetischen Reihenfolge, d.h. A hat die Position 1, B die Position 2, ..., Z die Position 26. Jetz wird `addiert': O (Pos. 15) + T (Pos. 20) = (Pos. 35) modulo 26 = 1, Rest (Pos. 9) -> I. Analog wird aus N (Pos. 14) und B (Pos. 2) ein P (Pos. 16). So erhalten wir als verschlüsselten Text das `Wort' "IPKLPSFHGQ". Da die Verteilung der Zeichen im resultierenden Wort zufällig ist, sind statistische Kryptanalyse-Verfahren nutzlos. Damit dies auch so bleibt, muß der Schlüssel nach der Verschlüsselung vernichtet werden. Deshalb heißt das Verfahren auch `one time pad'-Verfahren. Es wurde 1917 von J. Mauborgne und G. Vernam erfunden.

Nun gibt es allerdings ein kleines Problem. Der Empfänger einer solcherart verschlüsselten Nachricht soll diese ja entschlüsseln können. Dazu benötigt er den Schlüssel. Damit auch wirklich niemand außer dem Empfänger die Nachricht entziffern kann, muß dafür gesorgt werden, daß tatsächlich nur der Empfänger den Schlüssel -"TBFRGFARFM"- erhält. Wenn es nun aber einen Weg der geheimen Schlüsselübergabe gibt und der Schlüssel genauso lang wie die Nachricht ist, dann kann anstelle des Schlüssels auch gleich die Nachricht übergeben werden. Die Aktion bliebe geheim und der Aufwand wäre sogar geringer.

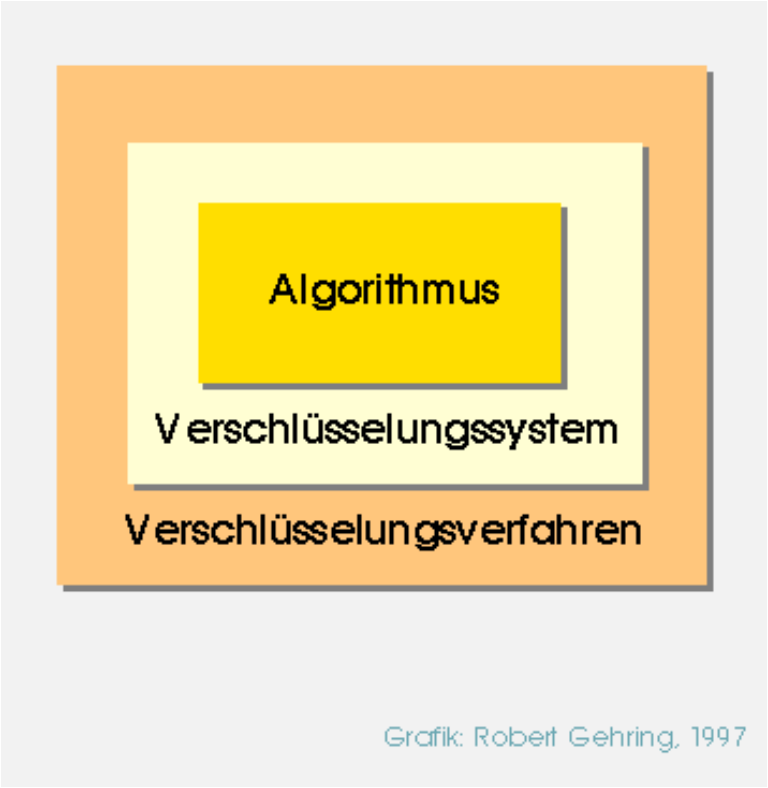
Eingangsseite Index Mail

Verschlüsselungsverfahren

Verschlüsselungsverfahren - (engl.) encryption algorithm, cryptosystem, encryption system, encryption scheme, cipher

Ein Verschlüsselungsverfahrenist eigentlich mehr als das Verfahren, mit dem ein Klartextin einen Geheimtexttransformiert wird. Da eine Verschlüsselung ohne Entschlüsselung sinnlos ist, bilden beide ein Paar. Wenn also von Verschlüsselungsverfahren die Rede ist, müßte immer auch die Rede von Entschlüsselungsverfahren sein. Je nach Kontext bezieht sich der Begriff dann auf die bloße Verschlüsselung oder auf das Paar aus Ver- und Entschlüsselung.

Im Prinzip läßt sich ein Verschlüsselungsverfahren als Funktion auffassen, die Elemente aus einer Eingabemenge auf Elemente einer Ausgabemenge abbildet.



Bei den meisten Verschlüsselungsverfahrenwird bei der Abbildung (Verschlüsselung) eine (geheime) Information verwendet, ohne welche die inverse Abbildung (Entschlüsselung) nicht durchführbar ist. Diese (geheime) Information heißt dann Schlüssel.

In Abhängigkeit vom verwendeten Schlüssel unterscheidet man zwei Typen von Verschlüsselungsverfahren:

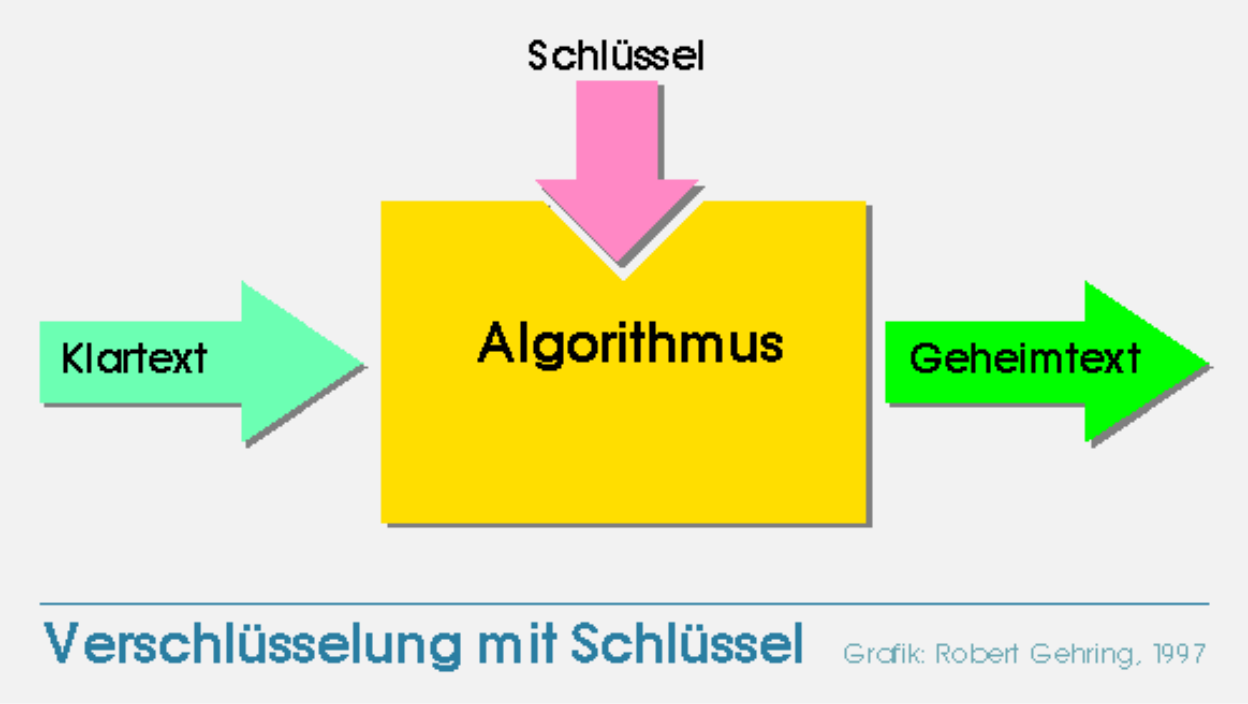
- symmetrische Verschlüsselungsverfahren, bei denen mit demselben Schlüssel ver- und entschlüsselt wird; z.B. DES
- asymmetrische Verschlüsselungverfahren, bei denen ein Schlüssel für die Verschlüsselung und ein anderer für die Entschlüsselung verwendet wird; z.B. RSA

Eingangsseite Index Mail
digitale signaturen diplomarbeit · robert gehring

Schlüssel

Schlüssel - (engl.) key

Der Schlüsselist bei einem Verschlüsselungsverfahreneine Information, die zur Verschlüsselungeines Klartextesbzw. Entschlüsselung eines Geheimtextesverwandt wird. Es kann sich dabei z.B. um eine Zahl oder ein Codewort handeln.



Der Schlüssel stellt quasi einen Parameter des Verschlüsselungsverfahrens (Algorithmus) dar. Die moderne Kryptographie beschäftigt sich in hohem Maße mit Verfahren, deren Sicherheit nur noch vom Schlüssel und nicht vom Verfahren selbst anhängig ist. Solche Verfahren haben den Vorteil, daß sie nicht geheimgehalten werden müssen und deshalb einen breiten Einsatz finden können.

Die Menge aller Schlüssel, die für Verschlüsselung und Entschlüsselung eingesetzt werden können, heißt Schlüsselraum.

symmetrisches Verfahren

symmetrisches Verfahren - (engl.) symmetric cipher, symmetric encryption algorithm, symmetric encryption scheme

Symmetrische Verschlüsselungsverfahren werden oft kurz auch symmetrische Verfahren genannt.

asymmetrisches Verfahren

Siehe: asymmetrisches Verschlüsselungsverfahren

hybrides Verfahren

hybrides Verfahren - (engl.) hybrid encryption system, hybrid encryption scheme

Im Zusammenhang mit Kryptographie spricht man von hybriden Verfahren im folgenden Sinne:

Hybride Verfahren verwenden sowohl asymmetrische Verschlüsselung, als auch symmetrische Verschlüsselung. Sie kombinieren damit die Vorteile beider Verfahren:

- asymmetrische Verfahren bieten öffentliche Schlüssel, sind allerdings viel langsamer, als symmetrische Verfahren
- symmetrische Verfahren sind viel schneller als asymmetrische Verfahren, brauchen jedoch einen sicheren Kanal für die Schlüsselübergabe

Hybride Verfahrenbenutzen einen öffentlichen Schlüssel, um den Sitzungsschlüsselfür die symmetrische Verschlüsselung zu verschlüsseln. Nur der berechtigte Empfänger kann mit seinem privaten Schlüssel den Sitzungsschlüssel entschlüsseln und die damit verschlüsselte Nachricht lesbar machen.

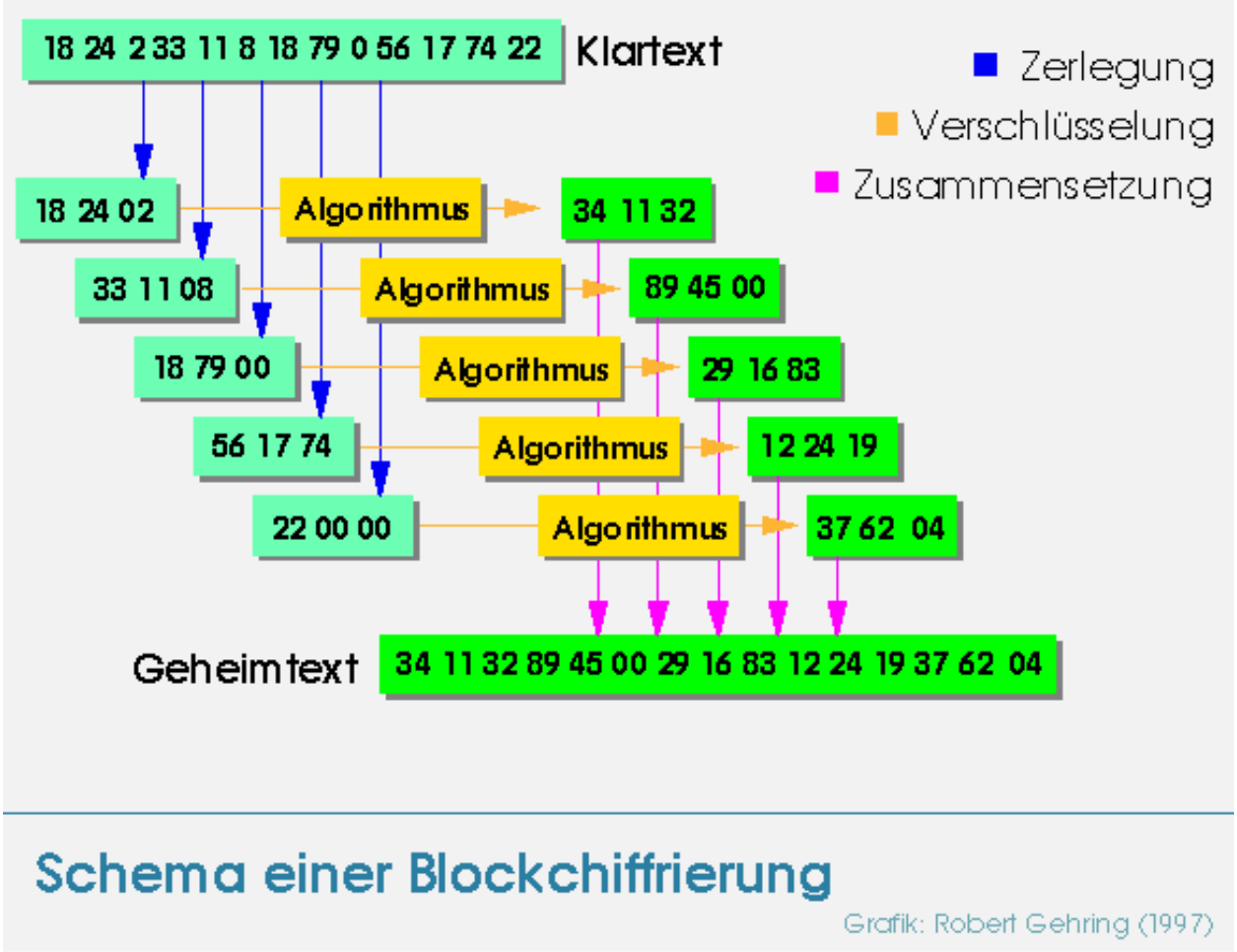
Die Daten der Sitzung werden dann wegen der Geschwindigkeit mit einem symmetrischen Verfahren verschlüsselt.

Blockchiffrierung

Blockchiffrierung - (engl.) block cipher

Eine Blockchiffrierung ist die Verschlüsselung von Stücken des Klartextes mit fester Länge.

Beispiel



Der Klartext wird in Teile gleicher Länge -Blöcke- zerlegt, gegebenenfalls werden zu kurze Teile aufgefüllt. Dann werden die einzelnen Blöcke verschlüsselt und die so entstehenden Geheimtextblöcke aneinandergehangen.

Bedeutung

Alle bedeutsamen symmetrischen Verschlüsselungsverfahren verwenden Blockchiffrierungen. Dies ist darauf zurückzuführen, daß Blockchiffrierungen die Charakteristika des Klartextes besser verbergen (Konfusion und Diffusion) und zudem noch schneller sind, als Stromchiffrierungen.

Blockchiffrierungen werden z.B. von DES, IDEA und RC5 eingesetzt.

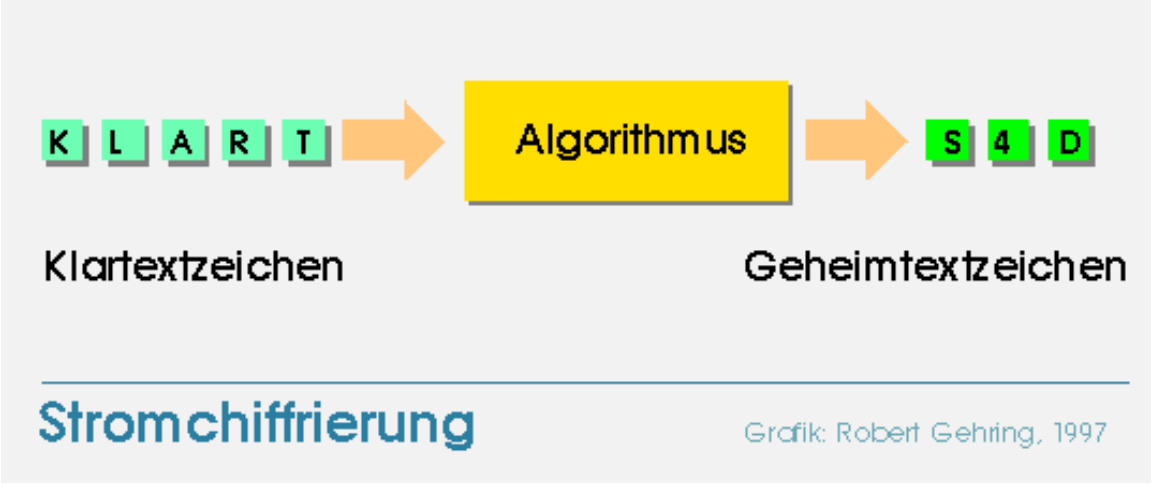
Siehe auch: Stromchiffrierung

Eingangsseite Index Mail
digitale signaturen diplomarbeit · robert gehring

Stromchiffrierung

Stromchiffrierung - (engl.) stream cipher

Eine Stromchiffrierung verschlüsselt fortlaufend einzelne Daten der Eingabe. Solche Daten können zum Beispiel die Buchstaben eines Textes oder die Bits eines binären Datenstroms sein.



Siehe auch: Blockchiffrierung

Deutsch

English

verdeckter Kanal

VPN - Virtual Private Network

Verschlüsselung

Verschlüsselungsalgorithmus

Verschlüsselungsverfahren

Virtuelles Privates Netzwerk

decryption

decryption (engl.) - Entschlüsselung, Dechiffrierung

Kryptanalyse

Kryptanalyse - (engl.) cryptanalysis

Die `Kryptanalyse' ist der Zweig der `Kryptologie', der sich mit dem Aufdecken und Entschlüsseln von Informationen in verschlüsselten Signalen beschäftigt. Die Pendants zur `Kryptanalyse' bilden `Kryptographie' (Verschlüsseln) und `Steganographie' (Verstecken).

Schwerpunkte der kryptanalytischen Tätigkeit sind:

- die Bestimmung der Informationen, die verschlüsselt in Form scheinbar sinnloser Zeichen (Signale) vorliegen, ohne über den Schlüssel zu verfügen
- die Ermittlung von Schlüsseln aus verschlüsselten Informationen
- die unbemerkte Veränderung verschlüsselter Informationen

Da Kryptanalyse und Kryptographie wesentlich im Milieu der Geheimdienste und des Militärs aufgewachsen sind, bedienen sie sich oft entsprechender Ausdrücke. So heißt der Versuch der Kryptanalyse eines Geheimtextes "Angriff" (attack).

[Schneier 1996] unterscheidet prinzipiell sechs wissenschaftliche und eine unwissenschaftliche Methoden der Kryptanalyse (S.6, 7). Die wissenschaftlichen sind:

1. `ciphertext-only attack'
2. `known-plaintext attack'
3. `chosen-plaintext attack'
4. `adaptive-chosen-plaintext attack'
5. `chosen-ciphertext attack'
6. `chosen-key attack'

Die unwissenschaftliche Methode des Angriffs nennt er `*Kryptanalyse mit Gewalt*', was Bedrohen, Erpressen, Bestechen und Quälen umfaßt. Diese Methode soll seiner Meinung nach sehr wirkungsvoll sein, was leicht vorstellbar ist.

Nicht in den Bereich der Kryptanalyse fallen technische Methoden, die sich mit den Schwächen der Realisierung (Implementierung) von Verschlüsselungsverfahren beschäftigen.

Beispiele dafür sind aufgeschliffene integrierte Schaltkreise (Chips), falsche Betriebsspannungen, gekochte Chips, Säureangriffe und solche mit ionisierter Strahlung, lasergenaues Ausschalten von einzelnen Transistoren, ... Der Phantasie scheinen keine Grenzen gesetzt zu sein. Für alle hier aufgezählten Verfahren findet man im Internet Erfolgsbeispiele.


Deutsch **English**

ECB - Electronic Code Book

ECC - Error Correction Code; Error Checking and Correction

EES - Escrowed Encryption Standard

Einweg-Hashfunktion

EISS - European Institute for Systems Security

ElGamal

encryption

encryption algorithm

Entschlüsselung

escrow agent

Deutsch

English

Key Escrow Initiative

Key Escrow Initiative (engl.) - Schlüsselhinterlegungsinitiative

Siehe auch: Clipper-Initiative

Klartextangriff

Klartextangriff - (engl.) known-plaintext attack, plaintext attack

Bei einem Klartextangriff stehen sowohl der Geheimtext, bzw. ein Stück davon, als auch der Klartext, bzw. ein Stück davon, zur Kryptanalyse zur Verfügung.

Beispiel

Die Funktsprüche der deutschen Wehrmacht wurden im zweiten Weltkrieg selbstverständlich verschlüsselt. Dazu diente die Enigma.

> Da die Alliierten einiges über die deutsche Mentalität wußten, vermuteten sie in den Funktsprüchen bestimmte Phrasen, wie z.B. "*Heil Hitler*" oder "*Oberkommando*" etc. Sie untersuchten die abgefangenen Funksprüche deshalb auf Stellen, an denen solche Phrasen wahrscheinlich stehen würden. Im Falle von "*Oberkommando*" wäre das am Anfang (Anrede) oder am Ende (Unterzeichnung) eines Textes. Mit "*Heil Hitler*" wurden Funksprüche üblicherweise unterzeichnet. So gelang es, Stücken des Geheimtextes zu entschlüsseln, und Erkenntnisse über den Schlüssel zu gewinnen, die zur Entschlüsselung des restlichen Textes dienlich waren.

Siehe auch: Klartextangriff mit gewähltem Klartext, Klartextangriff mit Anpassung des gewählten Klartextes

Klartextangriff mit Anpassung des gewählten Klartextes

Klartextangriff mit Anpassung des gewählten Klartextes - (engl.) adaptive chosen-plaintext attack

Bei einem Klartextangriff mit Anpassung des gewählten Klartextes wird ein ausgewählter Klartext ``untergeschoben''. Nach der Verschlüsselung wird der Geheimtext abgefangen und analysiert. Entsprechend den Untersuchungsergebnissen wird ein neuer Klartext untergeschoben. Dieses Verfahren wird solange wiederholt, bis der Schlüssel oder besser noch Verschlüsselungsverfahren und Schlüssel ermittelt sind. (Und solange es möglich ist, mußman anfügen.)

Für diese Art von Angriff versichert man sich tunlichst der Mithilfe einer Person auf der Seite des Gegenspielers. Diese kann zu passender Zeit einen gewählten Klartext in den Verschlüsselungsprozeß einschleusen. Oder man beschafft sich ein Exemplar des Verschlüsselungsgerätes, um damit in aller Ruhe herumspielen zu können (engl.: *to tamper with*)

Siehe auch: Klartextangriff mit gewähltem Klartext, Klartextangriff

Klartextangriff mit gewähltem Klartext

Klartextangriff mit gewähltem Klartext - (engl.) chosen-plaintext attack

Bei einem Klartextangriff mit gewähltem Klartext wird ein Klartext zur Verschlüsselung "untergeschoben". Anschließend stehen sowohl der Geheimtext, als auch der Klartext zur Kryptanalyse zur Verfügung. Durch eine geschickte Wahl des Klartextes läßt sich die Schlüsselfindung erheblich beschleunigen.

Beispiel

Das Beispiel ist historisch und wird in vielen Büchern über Kryptologie erwähnt.

> Im zweiten Weltkrieg wurde die deutsche Kommunikation mit der Enigma verschlüsselt. Um herauszufinden, wie das Wort "Leuchtboje" verschlüsselt wurde, bombardierte die Royal Air Force eine wichtige Leuchtboje. Ein in der Nähe befindliches deutsches Kriegsschiff sandte daraufhin einen verschlüsselten Funktspruch ab, in dem über das Erlöschen der Leuchtboje berichtet wurde: "*erloschen ist leuchtboje*". Nach der erfolgreichen Entschlüsselung wußten die Engländer wieder etwas mehr über die Enigma.

Siehe auch: Klartextangriff, Klartextangriff mit Anpassung des gewählten Klartextes

kodieren

kodieren - (engl.) encode

Siehe:codieren

Kollision

Kollision - (engl.) collision

Eine Kollisiontritt ein, wenn zu mehr als einem vorgegebenen Argumentwert $x_i$derselbe Funktionswert y einer Funktion f gebildet wird: $f(x_1) = f(x_2) = y$. Ein einfaches Beispiel aus der Mathematik ist die Funktion des absoluten Betrages. Bei dieser gilt: ABS(-1) = ABS(1) = 1 - eine Kollision.

In der Kryptologie ist die Frage interessant, ob es möglich ist, eine Kollision zu finden, d.h. ein passendes Argument, wenn man einen Funktionswert und ein zweites Argument kennt, z.B. durch Raten oder Rechnen. Ist die Wahrscheinlich so gering, daß es praktisch unmöglich ist, spricht man in Bezug auf die Funktion von Kollisionsfreiheit. Diese Eigenschaft ist insbesondere bei kryptographischen Hashfunktionen von Bedeutung.

kollisionsfrei

kollisionsfrei - (engl.) collision free

Eine kryptographische Hashfunktionh ist (praktisch) kollisionsfrei, wenn es nicht möglich ist, in vertretbarer Zeit, mit vertretbarem Aufwand zu einem gegebenen HashwertH eine sinnvolle Eingabe E für die Hashfunktion zu finden, so daßgilt: H=h(E).

Siehe auch: Kollisionsfreiheit

Kollisionsfreiheit

Kollisionsfreiheit - (engl.) *keine direkte Übersetzung möglich*; sinngemäß: collision-free

Von Kollisionsfreiheitspricht man bei kryptographischen Hashfunktionen, wenn es praktisch nicht möglich ist, zu einem Hashwerteinen sinnvollen Ausgangswert zu finden. D.h. es ist zwar möglich, den Hashwert z.B. H(D) einer Datei zu bestimmen. Ist die Hashfunktion H kollisionsfrei, so ist es umgekehrt nicht möglich, ausgehend vom Hashwert H(D) eine sinnvolle Datei D zu rekonstruieren.

Das sind theoretische Überlegungen. Praktisch sieht es so aus, daß Hashfunktionen *nicht kollisionsfrei* sind. Gleichzeitig sieht es in der Praxis so aus, daß es zu aufwendig ist, eine Kollision zu finden; der Rechenaufwand ist einfach zu hoch. Hat man ein Kollision gefunden, so ist es in der Regel viel zu spät, um damit noch etwas anfangen zu können. Der hohe Aufwand zur Berechnung resultiert aus der geringen Wahrscheinlichkeit, mit der eine Kollision auftritt. D.h. es müssen sehr viele Möglichkeiten ausprobiert werden - zu viele.

kollisionsresistent

kollisionsresistent - (engl.) collision-resistant

Statt kollisionsresitentwird oft *kollisionsfrei*benutzt. Besser sollte man aber von *praktisch kollisionsfrei*sprechen. Gemeint ist, daßKollisionennicht mit vertretbarem Aufwand in vertretbarer Zeit bestimmt werden können.

Siehe: Kollisionsfreiheit

Kompromittierung

< Text >

Konfusion

Konfusion - (engl.) confusion

Unter Konfusion versteht man die Verschleierung der Zusammenhänge zwischen den einzelnen Elementen eines Verschlüsselungsvorganges, also zwischen Klartext, Schlüssel und Geheimtext. Der Begriff geht auf Claude Shannon, den "Vater der Informationswissenschaft" zurück.

Durch Konfusion wird die Kryptanalyse mit statistischen Mitteln erschwert.

Siehe auch: Diffusion

Kryptograph

Kryptograph - (engl.) cryptographer (???)

Ein Kryptographbefaßt sich mit Kryptographie, d.h. mit dem Verschlüsselnvon Nachrichten(Texte etc.).

Siehe auch: Kryptologe, Kryptanalytiker

kryptographische Hashfunktion

kryptographische Hashfunktion - (engl.) cryptographic hash function

Eine kryptographische Hashfunktionist eine Hashfunktion, die auf Grund ihrer Einweg-Eigenschaft (praktische Unumkehrbarkeit) zu Zwecken der Integritätssicherung eingesetzt werden kann. Man spricht dann von Einweg-Hashfunktionenoder kryptographischen Einweg-Hashfunktionen.

Kryptographische Hashfunktion werden für digitale Signaturen benötigt.

Kryptologe

Kryptologe - (engl.) cryptologist

Ein Kryptologeist jemand, der sich (von Berufs wegen) mit der Kryptologiebefaßt, d.h. mit Entschlüsselungund Verschlüsselung.

Siehe auch: Kryptograph, Kryptanalytiker

Kryptologie

Die `Kryptologie' ist die Wissenschaft vom Verschlüsseln und Entschlüsseln von Informationen. Dem Verschlüsseln widmet sich das Teilgebiet der `Kryptographie' und dem Entschlüsseln die `Kryptanalyse'.

Im Zusammenhang mit dem Verschlüsseln (Kryptographie) wird häufig auch noch die Steganographie (Verstecken von Information) erwähnt. Dazu ein paar Worte von David Kahn:

> *"Steganographie conceals the very existence of the secret message. It's therefore broader than cryptography, but there's no theory yet, as far as I now, of steganography."*
>
> [Kahn 1996]

Es muß sich also noch eine Theorie über Steganographie herausbilden. Ob diese dann der Kryptologie unter- oder beigeordnet wird, bleibt abzuwarten. Von ihren Anwendungen her betrachtet, sind Kryptologie (Kryptographie) und Steganographie verwandt.

Bis zum Anfang der 70'er Jahre war Kryptologie eine wenig systematische Angelegenheit.

In den 70'er Jahren begann eine Entwicklung, in deren Verlauf sich der Charakter der Kryptologie stark geändert hat: Die Mathematik wurde zum bestimmenden Element.

Die Zahlentheorie , ein Gebiet der Mathematik, hat dabei großen Einfluß erlangt. Dies ist zurückzuführen auf die Entwicklung von kryptographischen Verfahren, deren Sicherheit auf den Schwierigkeiten bestimmter Berechnungen basieren. Dabei gibt es im wesentlichen zwei unterschiedliche Ansätze, die Bedeutung gewonnen haben:

1. Verfahren, die auf dem Vertrauen in das Faktorisierungsproblem basieren (siehe RSA)
2. Verfahren, die auf dem Vertrauen in die Schwierigkeiten bei der Berechnung diskreter Logarithmen basieren (siehe ElGamal)

Keines dieser Verfahren ist *beweisbar sicher*. Sie werden als *praktisch sicher* bezeichnet, weil alle bisher bekannten Lösungsverfahren einen Aufwand erfordern, der nachweislich größer ist, als die notwendige Dauer des Schutzes, der durch die Verschlüsselung erreicht werden soll. Diese Aussagen gelten natürlich nur für die bekannten Lösungsansätze. Experten gehen aus plausiblen Gründen davon aus, daß die NSA in der kryptologischen Forschung etwa 20 Jahre Vorsprung vor der öffentlichen Forschung hat (siehe z.B. [Wobst 1997 (I)], S.115).

key

key (engl.) - Schlüssel

< Terminus >

< Text >

key distribution

key distribution (engl.) - Schlüsselverteilung, Schlüsselübergabe

Siehe auch:key delivery, key transport

Glossar Digitale Signaturen

key escrow

key escrow (engl.) - Schlüsselhinterlegung

In der Literatur zum Thema Verschlüsselung findet man in den jeweiligen Abschnitten über politische Konsequenzen oft den Ausdruck `*key escrow*'. Versucht man herauszufinden, woher dieser Ausdruck stammt, steht man unerwartet vor einem Problem. Das Wort `escrow' findet sich nämlich nicht in jedem handelsüblichen Wörterbuch. Im "Duden/Oxford Großwörterbuch Englisch" in der Ausgabe von 1990 fehlt `escrow' jedenfalls. Auch in einem alten "Taschenwörterbuch der englischen und deutschen Sprache" von 1941 sucht man es vergebens. Erst unter Zuhilfenahme moderner Technik, in diesem Falle der "Compton's Infopedia 2.0" (englische Ausgabe) auf CD-ROM, hat man Erfolg. Dort kann man in den verschiedenen Werken dann lesen (zitiert):

- **Merriam Webster's Dictionary ([Webster's])**

  "**escrow**

  ...
  1 : a deed, a bond, money, or a piece of property held in trust by a third party to be turned over to the grantee only upon fulfillment of a condition

  2 : a fund or deposit designed to serve as an escrow

  ... "

- **Funk & Wagnalls New Encyclopedia ([Funk & Wagnalls])**

  "ESCROW,

  in law, conditional delivery of money or property, or documents evidencing or transferring rights therein, to a third person to be kept by that person until certain conditions are satisfied and then to be delivered over to the obligee or grantee. The property or documents thus conditionally held are also called the escrow, and the contract defining the conditions of the second delivery is called the escrow agreement.

  The escrow is a device most frequently applied in real-estate transactions. A deed, for example, delivered in escrow does not operate as an obligation or conveyance so long as it remains in the hands of the third person. When the prescribed conditions are fulfilled, the deed generally takes effect from the second delivery. Although the term escrow was originally applied only to such conditional delivery of instruments for the conveyance of land, it is now applied to any kind of written instrument or form of property that may be deposited for later delivery on fulfillment of prescribed conditions.
  ... "

- **Funk & Wagnalls New Encyclopedia ([Funk & Wagnalls])**

  "JARGON,

  vocabulary used by a special group or occupational class, usually only partially understood by outsiders.
  ...
  Examples of occupational jargon include such formal technical expressions as perorbital hematoma (black eye, to the layperson), in medicine, and escrow and discount rate, in finance
  ... "

Das einzige Buch, daß auf die Geschichte und Bedeutung des `escrow' eingeht, ist **[CRISIS 1996]**. Dort liest man:

> "The term `escrow', as used conventionally, implies that some item of value (e.g., a trust deed, money, real property, other physical object) is delivered to an independent trustet party that might be a person or an organization (i.e., an escrow agent) for safekeeping, and is accompagnied by a set of rules provided by the parties involved in the transaction governing the actions of the escrow agent. Such typically specify what is to be done with the item, the schedule to be followed, and the list of other events that have to occur.
> ...
> As it applies to cryptography, the term `escrow' was introduced by the U.S. government's April 1993 Clipper initiative in the context of encryption keys. Prior to this time, the term `escrow' had not been widely associated with cryptography, ...
> ...
> ..., since all escrowed encryption schemes proposed to date are intended to provide very strong cryptographic confidentiality (strong algorithms, relatively long keys) for users against *unauthorized* third parties, but no confidentiality at all against third parties who have *authorized* exceptional access."

Es scheint also zulässig zu sein, zu sagen, daß es sich um einen Begriff handelt, dessen Wurzeln im Jargon der Finanz- und Handelswelt liegen. Bemerkenswert scheint dabei zu sein, daß ein `escrow' ursprünglich mit dem Ziel hinterlegt wurde, daß nach Erbringung einer Leistung eine Übertragung stattfindet. Über diese Übertragung sind sich beide Seiten von Anfang an einig.

Im Falle des `key escrow' sollte es sich nach Aussagen der initiierenden Stellen aber nicht um ein Tauschgeschäft handeln. Vielmehr sollten die Sicherheitsdienste Zugriff ohne Gegenleistung erhalten. Das Verfahren sieht dabei folgendermaßen aus:

> Eine Person (ggf. eine juristische Person) will elektronische Dokumente verschlüsseln. Damit die Verschlüsselung ausreichend wirksam erfolgen kann, greift die Person auf sogenannte "starke Verschlüsselungsalgorithmen" zurück. Sie verwendet z.B. eine asymmetrische Verschlüsselung, bei der ein Schlüssel geheim und einer öffentlich zugänglich ist, bzw. dem Kommmunikationspartner zur Verfügung steht. Starke Verschlüsselungsalgorithmen stellen allerdings auch ein Hindernis für Geheimdienste, Polizei und Staatsanwaltschaft dar: Die verschlüsselten Dokumente könnten ohne Schlüssel nicht in absehbarer Zeit entschlüsselt werden. Damit diese Institutionen trotzdem mitlesen können, wird gesetzlich verfügt, daß ein Duplikat des geheimen Schlüssels bei einer dritten Instanz, dem sogenannten `escrow agent' hinterlegt wird. Nach Maßgabe der Gesetze sollen die Geheimdienste etc. dann Zugriff auf das hinterlegte Duplikat erhalten und somit in die Lage versetzt werden, verschlüsselte Dokumente zu lesen.
>
> Siehe auch: [Schneier 1996], S.672ff

Im Zusammenhang mit der gescheiterten `clipper-chip'-Initiative kam der Begriff `key escrow' in Verruf. Auch wurde er in vielfältigen Zusammenhängen benutzt und verlor so seine Eindeutigkeit.

Zusammenfassend könnte man feststellen:

1. Bei einem `key escrow'-Verfahren wird ein Duplikat des geheimen Schlüssels bei einer dafür bestimmten Stelle (escrow agent) hinterlegt. Eventuell wird der geheime Schlüssel auch in mehrere Teile zerlegt und diese Teile bei unterschiedlichen Stellen hinterlegt (siehe: key recovery). Die Institutionen des Staatsschutzes, der Geheimdienste, etc. haben Zugriff auf den geheimen Schlüssel und können verschlüsselte Dokumente mitlesen (Sie könnten also sogar Dokumente fälschen!)
2. `key escrow' hat in den Ohren der Wirtschaftsfachleute einen vertrauten Klang und suggeriert Seriosität. Naheliegendere und umgangssprachlich gebräuchlichere Begriffe, wie z.B. `deposit', wurden vermieden. Das Verfahren, das im Zusammenhang mit einem `key escrow' ablaufen sollte, funktioniert aber anders, als das in der Wirtschaft bekannte `escrow'-Verfahren. Auch hat es andere Ziele.
3. Verschlüsselung mit einem solchen Verfahren gibt keine Sicherheit darüber, wer mitliest. Man weiß allerdings, wer auf jeden Fall mitlesen kann.
4. Ein solches System dürfte generell wenig Zustimmung finden, da es dem Ziel der *zuverlässigen Verschlüsselung* zuwiderläuft. Die entsprechende `clipper chip'-Initiative in den USA ist denn auch gescheitert.

Da der Begriff des key escrow und das damit zusammenhängende Verfahren auf Ablehnung gestoßen sind, versuchen US-Regierung und NSA mit etwas neuem: `key recovery'. Bei diesem Verfahren wird der Schlüssel in zwei oder mehr Teile zerlegt und die Teile werden bei unterschiedlichen Stellen (recovery agent) hinterlegt. (Für einfache Fälle wird der Schlüssel komplett hinterlegt.)Auf richterliche Anordnung hin müssen diese Teile herausgegeben werden, woraus dann der Schlüssel rekonstruiert (recovery) werden kann. Somit wird die Kommunikation abhörbar.

Im Prinzip handelt es sich um das gleiche Verfahren. Allerdings scheint ihm etwas mehr Erfolg vergönnt zu sein. Namhafte Firmen, wie z.B. IBM, haben ihren Widerstand aufgegeben und beteiligen sich an einer `key recovery initiative'. Dadurch wollen sie die Exportchancen für ihre Verschlüsselungstechnologie verbessern.

---

key establishment

key establishment (engl.) - Schlüsseleinführung

Unter `key establishment' versteht man die initiale Vereinbarung und Verteilung von Schlüsseln unter den zukünftigen Teilnehmern einer verschlüsselten Kommunikation.

`key establishment' ist ein Teil des `key management', dem die Schlüsselerzeugung (`key generation') vorausgeht. Das `key establishment' selbst kann in zwei Schritte unterteilt werden:

1. Schlüsselvereinbarung (`key agreement')
2. Schlüsselübergabe (`key transport', `key delivery')

Der Begriff `key establishment' ist nicht sehr gebräuchlich.

key generation

key generation (engl.) - Schlüsselgenerierung, Schlüsselerzeugung

key management

key management (engl.) - Schlüsselverwaltung

key recovery

key recovery (engl.) - Schlüsselwiederherstellung

key recoveryist ein mit einem neuen Namen versehenes, leicht abgewandeltes Verfahren des `key escrow'.

Bei key recovery wird der Schlüssel im Ganzen oder in mehreren Teilen bei sogenannten `key recovery'-Agenten (`key recovery agents') hinterlegt. Auf Verlangen der berechtigten Behörden muß der Agent den Schlüssel herausgeben bzw. zusammensetzen und herausgeben, so daß die Behörden von da an die Kommunikation `abhören' können. Der einzige Unterschied zu `key escrow' ist darin zu sehen, daß die Behörden nicht schon von vornherein Zugriff auf den Schlüssel haben. Sie können sich ihn allerdings jederzeit verschaffen.

Innerhalb von Firmen wird eine ähnliche Strategie verfolgt. Dort geht es aber meist um die Sicherung von Dokumenten für den Fall, daß der Schlüsselinhaber aus der Firma ausscheidet, ohne den Schlüssel einer berechtigten Person zu überlassen.

key retrieval

key retrieval (engl.) - Zurückholung des Schlüssels

Für key retrievalgibt es (noch) keinen passenden deutschen Terminus.

Gemeint ist die `Wiederzugängigmachung' eines Schlüssels, der bereits aus dem Verkehr gezogen wurde. Der Schlüssel wurde jedoch nicht vernichtet (Schlüsselvernichtung), sondern sicher archiviert. So kann man Streitfälle, die sich auf lange zurückliegende verschlüsselte Kommunikation beziehen, unter Umständen klären.

key retrievalsollte nicht mit key recoveryverwechselt werden, wo es um das Abhören verschlüsselter Kommunikation geht.

key transport

key transport (engl.) - Schlüsselübergabe, Schlüsseltransport

`key transport'bezeichnet im Falle der Schlüsselverwaltung(key management) die Schlüsselübergabe. Im engeren Sinne kann aber auch der bloße Transport gemeint sein.

Siehe auch:key delivery

knapsack

knapsack (engl.) - Rucksack, Tornister

Die Bezeichnung `knapsack' wählte Ralph Merkle 1974 für einen von ihm entwickelten Ansatz zur Public Key-Kryptographie. Manchmal findet man auch die Bezeichnung *Merkle-Hellman knapsack*.

Das Problem basiert auf mengentheoretischen Überlegungen (*superincreasing subset sum problem*) und liefert nur eine ``geringe'' Sicherheit, da der Zeitaufwand zum unbefugten Entschlüsseln gegenüber dem Zeitaufwand zum befugten Entschlüsseln nicht unverhältnismäßig hoch ist.

known-key attack

known-key attack (engl.) - Angriff mit bekanntem Schlüssel

Bei der known-key attackgeht es darum, aus bekannten Schlüsseln oder Schlüsselteilen andere Schlüssel abzuleiten. Dazu benötigt man in der Regel den Zugriff auf die Wege des Schlüsselaustausches oder die Verfahrensschritte des Verschlüsselungsverfahrens.

Eingangsseite Index Mail

known-plaintext attack

known-plaintext attack (engl.) - Klartextangriff, Angriff mit bekanntem Klartext

Siehe auch: plaintext attack

Glossar Digitale Signaturen

Sektionen des Glossars

Benutzungshinweise

Die abgebildete "Tastatur" gestattet den Zugriff auf die Indizes zu den jeweils angegebenen Sektionen des Glossars.

Alle Begriffe, die mit A oder a beginnen, sind über die A-Taste zu erreichen. Analog sind alle Begriffe, die mit B oder b beginnen über die B-Taste zu erreichen. Für jeden Buchstaben des Alphabets gibt es die entsprechende Taste.

Bei Betätigung einer Taste wird der Index zum entsprechenden Buchstaben geladen. Vom Index gibt es Links zu allen Begriffen, die in der ausgewählten Sektion des Glossars behandelt werden. Für die Suche nach einem konkreten Begriff kann die "Find"-Funktion des verwendeten Browser benutzt werden.

Parität

Parität - (engl.) parity

Mittels Paritätsichert man die Integrität von Daten während einer Übertragung oder Speicherung ab. Es handelt sich um Zusatzinformationen (redundante Informationen) in Form von Bits, die den Zustand der Daten zum Zeitpunkt der Übertragung bzw. Speicherung beschreiben. Weichen die Daten beim Empfang oder beim Wiedereinlesen nach der Speicherung von dieser Beschreibung ab, ist ein Fehler (sind mehrere Fehler) aufgetreten, d.h. die Integrität ist verletzt.

Siehe auch:CRC, ECC

parity

parity (engl.) - Parität

CRC [*Cyclic Redundancy Check*][*Cyclic Redundancy Code*]

1. Cyclic Redundancy Check (engl.) - zyklische Redundanzprüfung
2. Cyclic Redundancy Code (engl.) - zyklischer, redundanter Code

1. Der CRC (C. R. Check) ist ein Checksummen-Verfahren, mit dem zufällige Datenveränderungen festgestellt werden können. Solche Datenveränderungen können z.B. bei der Datenübertragung auftreten. Ist das der Fall, werden die Daten erneut angefordert.
2. Als CRC (C. R. Code) bezeichnet man ein paar zusätzliche Bits, die im CRC (C. R. Check) (1) verwendet werden. Zur Berechnung zieht man üblicherweise Operationen mit Polynomen heran.

Siehe auch: Error Correction Code (ECC)

ECC [*Error Correction Code*] [*Error Checking and Correction*]

- Error Correction Code (engl.) - Code zur Fehlerkorrektur
- Error Checking and Correction (engl.) - Fehlererkennung und -korrektur

Mittels ECCkönnen Fehler eines einzelnen Bits bei gespeicherten Daten korrigiert werden. Solche Fehler können z.B. auftreten, wenn Magnetbänder lange Zeit gelagert werden.

Zur Absicherung werden bei der Datenspeicherung redundante Informationen zu den Daten hinzugefügt (parity, Parität). Wenn ein Fehler nur in einem Bit eines Bytes auftritt, kann er korrigiert werden. Tritt der Fehler in mehreren Bits auf, kann er nur festgestellt werden.

Beispiel

Intelverwendet im Pentium II-Prozessor ECC, um Fehler im Cache automatisch zu korrigieren.

Siehe auch: Cyclic Redundancy Check (CRC), Secret Error Correcting Code (SECC)

PIN [*Personal Identification Number*][*Persönliche Identifikationsnummer*]

PINs sind mehrstellige Zahlen und werden zur Authentifizierungverwendet. Sie werden persönlich zugeteilt, mit der Auflage, sie weder zu notieren, noch weiterzugeben.

Anwendung finden sie z.B. bei EC-Karten, beim Homebanking, bei Mobiltelefonen oder beim Zugang zu Online-Diensten. Solange die PIN nicht -absichtlich oder unabsichtlich- weitergegeben wurde, ist davon auszugehen, daß sie nur dem berechtigten Inhaber bekannt sind. Sie können somit als Identifikationsmerkmal herangezogen werden.

Werden PINs nicht sehr sorgfältig ausgewählt und weisen sie nicht eine ausreichende Länge auf (4 Stellen sind meist nicht ausreichend!), sind sie nicht als sicher einzustufen.

Authentifizierung

Authentifizierung - (engl.) authentication

Der Begriff der Authentifizierung wird im Zusammenhang mit Konzepten und Systemen zur Absicherung verwendet. In der Hauptsache geht es dabei um die Absicherung von Informationen und Informationssystemen.

Es lassen sich zwei Gebiete beschreiben, mit denen Authentifizierung insbesondere verbunden ist:

- Zugangssicherung bzw. Zugriffssicherung bei technischen Systemen
- Integrität und Urheberschaft elektronischer Dokumente .

Technische Systeme

Im ersten Fall soll die Identität der Person, die Zugang zu einem technischen System bzw. Zugriff auf Informationen über ein technisches System erhalten will, festgestellt werden. In Abhängigkeit von der erfolgreichen Identifizierung wird Zugang ge- oder verwährt.

Konkrete technische Systeme enthalten z.B. Komponenten zur Personenidentifikation anhand biometrischer Merkmale (Fingerabdrücke, Stimme, Iris) oder mittels Überprüfung spezifischen Wissens (password, PIN).

Elektronische Dokumente

Im zweiten Fall geht es um die Authentizität, also die Echtheit von elektronischen Dokumenten. Diese Echtheit hat zwei Aspekte:

- ***Ist Dokument X unverändert?***
  Bei der Speicherung und Übertragung elektronischer Dokumente soll die Integrität, d.h. die Unverändertheit des Inhaltes sichergestellt werden. Die Bedeutung dieses Aspektes ist besonders groß, wenn elektronische Dokumente über lange Zeiträume hinweg unverändert bleiben müssen. Ein Beispiel sind elektronische Grundbücher oder Geburtsurkunden.
- ***Stammt Dokument X von Person A?***
  Elektronische Dokumente sollen ihrem Urheber eindeutig zuzuordnen sein. Nur, wenn die Urheberschaft zweifelsfrei nachweisbar ist, lassen sich z.B. die Urheberrechte durchsetzen.

Bei Verträgen, die z.B. im Internet geschlossen werden, kommt beiden Aspekten eine herausragende Bedeutung zu. Beide Vertragspartner wollen einerseits sicherstellen, daß der Vertragstext nicht im Nachhinein manipuliert werden kann. Andererseits wollen sie zur Durchsetzung des Vertrages im Streifalle den Vertragspartner eindeutig identifizieren können.

Die Authentizität elektronischer Dokumente wird z.B. mit digitalen Signaturen sichergestellt.

Anmerkung:

Häufig wird statt `*Authentifizierung* ' auch `*Authentizierung*', `*Authentisierung*' oder `*Authentikation*' verwandt. Auch wenn das englische Wort `*authentication*' heißt, wird ` *authenticate*' mit `*authentifizieren*' übersetzt. Somit müßte das zugehörige Substantiv `*Authentifizierung* ' (ev. noch `*Authentifikation*') lauten. Die Lektüre des Oxford Großwörterbuches Englisch läßt keinen anderen Schluß zu.

Eingangsseite Index Mail
digitale signaturen diplomarbeit · robert gehring

Pohlig-Hellman-Verfahren

Das Verfahren wurde nach seinen Entwicklern, S.C. Pohlig und M.E. Hellman benannt.

Es handelt sich sich um ein asymmetrisches Verfahren, jedoch nicht um ein Public-Key-Verfahren. Es ist insofern asymmetrisch, als zwei unterschiedliche Schlüssel für die Ver- und die Entschlüsselung verwendet werden. Diese Schlüssel lassen sich allerdings leicht voneinander ableiten, weshalb es kein Public-Key-Verfahren ist.

Sieht man sich das Verfahren genauer an, weist es große Ähnlichkeit mit dem RSA-Verfahren auf.

Public-Key-Verfahren

Siehe: Public-Key-Verschlüsselungsverfahren

RSA [*Rivest-Shamir-Adleman*]

RSAhat seinen Namen nach denen seiner Entwickler erhalten: Ronald L. Rivest, Adi Shamir und Leonard Adleman[*], die das Verfahren 1977 ("*On Digital Signatures and Public Key Cryptosystems*", MIT Laboratory for Computer Science Technical Memorandum 82, April 1977) bzw. 1978 (*"A Method for Obtaining Digital Signatures and Public-Key Cryptosystems"* , Communications of the ACM 2/1978) vorstellten.

RSA gehört, wie auch z.B. ElGamal , zu den asymmetrischen Verschlüsselungsverfahren , bei denen ein Schlüssel für die Verschlüsselung und ein anderer für die Entschlüsselung benutzt wird. Somit ist RSA für die Erzeugung digitaler Signaturen geeignet.

Grundlage von RSA sind zahlentheoretische Überlegungen, bei denen angenommen wird, daß große Zahlen nur schwer faktorisierbar, d.h. in Primfaktoren zerlegbar sind. Es handelt sich um das sogenannte Faktorisierungsproblem. Der vermutete Rechenaufwand ist dabei so groß, daß die Verschlüsselung bei geeignet gewählten Schlüsseln praktisch nicht zu brechen ist. Die Schlüssel sollten dabei mindestens 512 Bit lang sein, bei notwendiger Geheimhaltung über lange Zeiträume entsprechend länger.

Arbeitsweise

Es werden zwei große Primzahlen benötigt. Da es kein Verfahren gibt, das große Primzahlen generiert (das `Sieb des Erathostenes' ist nur für kleine Primzahlen praktibabel), werden zwei Zahlen gewählt und mit einem geeigneten Verfahren auf die Primzahleigenschaft geprüft.

Übliche Tests sind (z.B. nach [Damm 1995]):

- das Verfahren von Miller-Rabin
- das Verfahren von Solovay-Strassen

Beide Verfahren stellen mit einer gewissen Wahrscheinlichkeit fest, ob eine gegebene Zahl eine Primzahl ist, oder nicht. Aufgrund der Einschränkung, daßmit Wahrscheinlichkeiten operiert wird, sind derartige Verfahren deutlich schneller als Faktorisierungsverfahren.

Aus beiden Primzahlen, in der Literatur üblicherweise mit p und q bezeichnet, wird das Produkt n berechnet:

$$n = p * q$$

p und q müssen unterschiedliche Zahlen sein. Die Länge von n sei dabei k Bit. Normalerweise wird k vorgegeben und p und q so gewählt, daßn die Länge k hat. n wird zum ersten Bestandteil des öffentlichen Schlüssels.

Dann berechnet man das Produkt z der Vorgänger von p und q:

$$z = (p - 1) * (q - 1)$$

Nun werden der geheime Schlüssel und der zweite Bestandteil des öffentlichen Schlüssels gewählt. Beide müssen so gewählt werden, daßsie folgende Bedingung erfüllen:

$e * d \equiv 1 \bmod(z)$, e hat keinen gemeinsamen Teiler mit z

Ob dabei e oder d als privater Schlüssel verwendet werden, ist im Prinzip egal. Der andere wird dann zum Bestandteil des öffentlichen Schlüssels. In der Literatur (z.B. bei [Schneier 1996]) steht e üblicherweise im öffentlichen Schlüssel und d ist der private Schlüssel.

p und q müssen unbedingt geheim bleiben! Wenn man ganz sicher gehen will, sollte man sie vernichten.

Damit hat man folgende Schlüssel erhalten:

- Privater Schlüssel: d
- Öffentlicher Schlüssel: (e, n)

Man könnte auch (d, n) als den privaten Schlüssel bezeichnen. In der Literatur findet man es allerdings so, wie oben angegeben.

Verschlüsselung

Der Klartext wird in Blöcke zerlegt, die kürzer als n sind. Handelt es beim Klartext sich nicht um Zahlen oder Bitmuster, so mußman diese erst entsprechend aufbereiten. (Buchstaben könnte man z.B. durch ihre Stellung im Alphabet ersetzen.) Die einzelnen Blöcke sollten gleich lang sein, wozu man ggf. Nullen voranstellt. Ein solcher Block wird dann entsprechend der folgenden Formel verschlüsselt:

Geheimtextblock = (Klartextblock ^ e) mod n

Entschlüsselung

Die Entschlüsselung erfolgt dann so:

Klartextblock = (Geheimtextblock ^ d) mod n

Durch die Verschlüsselung mit dem öffentlichen Schlüssel ist sichergestellt, daßnur der berechtigte Empfänger, der als einziger über den geheimen (privaten) Schlüssel d verfügt, den Klartext wiederherstellen kann.

Beispiel

Beispiel aus Bruce Schneier: Angewandte Kryptographie, S. 533, 534

Seien p = **47** und q = **71.**

Dann ist n = p * q = **3337** und z = (p - 1) * (q - 1) = **3220**.

Der öffentliche Schlüssel e darf dann keine gemeinsamen Teiler mit z = **3220** haben. e kann also gewählt und dann auf diese Eigenschaft überprüft werden.

e wird gewählt: e = **79**

Dann gilt: e * d = **1** mod **3220**, d.h. d = **1/79** mod **3220** = **1019.**

Der öffentliche Schlüssel lautet dann: (e, n) = (**79, 3337**).

Der geheime Schlüssel lautet: (d) = **1019**.

Der Klartext **688232687966668 3** soll verschlüsselt werden. Zuerst wird er in Blöcke zerlegt, die kürzer als n sind.

b_1=**688** b_4=**966**

b_2=**232** b_5=**668**

b_3=**687** b_6=**003**

Die Blöcke werden nach der Vorschrift $g_i = b_i^e \bmod n$ verschlüsselt.

g_1=688^{79} mod **3337** = **1570** g_4=966^{79} mod **3337** = **2276**

g_2=232^{79} mod **3337** = **2756** g_5=668^{79} mod **3337** = **2423**

g_3=687^{79} mod **3337** = **2091** g_6=003^{79} mod **3337** = **0158**

Die Blöcke werden nach der Vorschrift $b_i = g_i^d \bmod n$ entschlüsselt.

b_1=1570^{1019} mod **3337** = **688** usw. usf.

Wenn zur Verschlüsselung anstelle des öffentlichen Schlüssels e der geheime Schlüssel d verwendet wird, kann jeder, der die Nachricht mit dem öffentlichen Schlüssel entschlüsselt, sicher sein, daß die Nachricht vom Besitzer des geheimen Schlüssels stammt. Dies ist der Grundgedanke bei der Verwendung von RSA für die Erstellung digitaler Signaturen.

Sicherheit

RSAist seit 1977 (1978) bekannt. Bis heute ist kein erfolgreicher Angriff auf eine korrekte RSA-Implementierung mit ausreichend langem Schlüssel bekannt.

Die Sicherheit von RSA beruht auf dem Faktorisierungsproblem. Bisher ist keine Methode bekannt, RSA zu brechen, die schneller als die Faktorisierung wäre. Die schnellsten bekannten Faktorisierungsverfahren sind ([Damm 1995], S. 17):

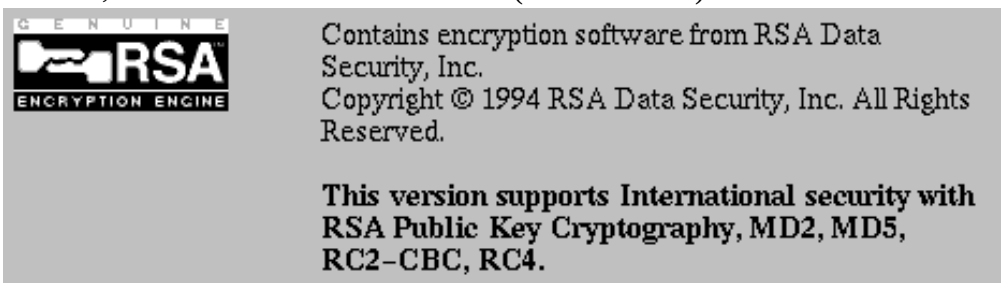
- Multiple Polynomial Quadratic Sieve (MPQS)
- General Number Field Sieve (GNFS)

Es gibt verschiedene Angriffsmöglichkeiten auf *Systeme*, die RSAverwenden (nach [Schneier 1996], S. 537 ff):

Angriffsmethode	Gegenmaßnahme
Chosen-Ciphertext-Attack	Keine unbekannten Dokumente signieren, ohne vorher eine Einweg-Hashfunktion anzuwenden.
Angriff mit gemeinsamem Modul	Niemals den gleichen Wert von n für mehrere Benutzer wählen.
Angriff bei kleinem Verschlüsselungsexponenten	Der Klartext sollte etwa die gleiche Größe wie n haben. Gegebenenfalls sollte der Klartext mit Zufallswerten ergänzt werden.
Angriff bei kleinem Entschlüsselungsexponenten	d sollte einen Großen Wert ggü. e haben.

Bedeutung

RSAist der zivil meistgenutzte asymmetrische Verschlüsselungsalgorithmus. Er wird zum Beispiel im Programm PGPverwendet. RSAist gut für die Erzeugung digitaler Signaturen geeignet. Der Netscape Navigator/Communicator setzt ebenfalls auf RSA-Sicherheit, wie aus der Startseite ersichtlich (Bildausschnitt):



Patente

RSAist in den USA unter der Nummer 4.405.829 bis zum 20. September 2000 patentiert. Anwender benötigen demnach ein gültige Lizenz, die von RSADSIerhältlich ist.

Es gibt allerdings begründete Zweifel an der Gültigkeit des Patents. Der Umfang des Patents ist ebenfalls zweifelhaft. (Siehe dazu die Annotation.)

Annotation

Patrick J. Flinn, James M. Jordan III:

Using the RSA Algorithm for Encryption and Digital Signatures: Can You Encrypt, Decrypt, Sign and Verify without Infringing the RSA Patent?

Internet: http://www.cyberlaw.com

Eine Zusammenfassung.

Internet

PQS [*Polynomial Quadratic Sieve*][*Polynomisches Quadratisches Sieb*]

Das PQS ist ein Verfahren zur Faktorisierung und wurde aus dem Quadratischen Sieb (QS) entwickelt.

Faktorisierung

Faktorisierung - (engl.) factorisation

Siehe: Primfaktorzerlegung

QS [*Quadratic Sieve*][*Quadratisches Sieb*]

quadratic sieve (engl.) - Quadratisches Sieb

Das Quadratische Siebist das schnellste Verfahren, um die Primfaktoren einer Zahl mit weniger als 110 Dezimalstellen zu bestimmen. Aus dem QSwurde das Polynomische Quadratische Sieb(PQS) entwickelt.

Siehe auch: Zahlkörpersieb (Number Field Sieve - NFS)

Primfaktorzerlegung

Primfaktorzerlegung - (engl.) factorisation, factoring

Jede ganze Zahl ist entweder eine Primzahl oder das Produkt mehrerer Primzahlen. Die Bestimmung der Primzahlen, durch deren Multiplikation sich eine ganze Zahl ergibt, heißt Primfaktorzerlegung. Die Primfaktorzerlegung wird auch als Faktorisierung bezeichnet.

Beispiel

Die ersten neun Primzahlen heißen 1, 2, 3, 5, 7, 11, 13, 17, 19.

Die Primfaktorzerlegung der Zahl 60 ergibt folgende Primfaktoren:

$$60 = 6 * 10 = 2 * 3 * 2 * 5 = \underline{2} * \underline{2} * \underline{3} * \underline{5}$$

Da 2, 3 und 5 Primzahlen sind, wurde 60 faktorisiert.

Verfahren

Das schnellste, bekannte Verfahren zur Faktorisierung von Zahlen mit mehr als 110 Dezimalstellen ist das Zahlkörpersieb (Number Field Sieve, NFS). Für zahlen mit weniger als 110 Dezimalstellen ist das Quadratische Sieb (Quadratic Sieve, QS) schneller.

Das klassische Verfahren ist die versuchsweise Division. Dabei wird für jede Primzahl, die kleiner oder gleich der Quadratwurzel der zu faktorisierenden Zahl ist getestet, ob sie Teiler der Zahl ist.

Siehe auch: Faktorisierungsproblem, Sieb des Erathosthenes

factorisation

factorisation (engl.) - Faktorisierung, Primfaktorzerlegung

Anmerkung: In der Literatur findet man auch factoring. Andererseits heißt faktorisieren aber eindeutig factorise (factorize), nach Oxford Dictionary.

factoring

factoring (engl.) - Faktorisierung

Siehe auch: factorisation

NFS [*Number Field Sieve*]

number field sieve (engl.) - Zahlkörpersieb

Faktorisierungsproblem

Faktorisierungsproblem - (engl.) problem of factorisation

Das Faktorisierungsproblemist eine klassische Aufgabe aus der Zahlentheorie. Die Aufgabe lautet, zu einer gegebenen Zahl alle Primfaktoren zu ermitteln. Für große Zahlen ist diese Aufgabe nur schwer zu lösen, insbesondere, wenn es sich um sogenannte "schwere Zahlen" handelt, d.h. Zahlen, die nur große Primfaktoren besitzen.

Große Zahlen lassen sich nur noch mit einem gewaltigen Rechenaufwand faktorisieren. Für eine 129-stellige Dezimalzahl wurde im März 1994 die Faktorisierung von 600 Leuten mit 1600 Rechnern nach 8 Monaten Berechnungen abgeschlossen.

Zahlen mit 140 und mehr Dezimalstellen lassen sich praktisch noch nicht faktorisieren. Darauf basiert die Sicherheit der RSA-Verschlüsselung, d.h. die Unlösbarkeit des Faktorisierungsproblems bildet die kryptologische Annahme des RSA-Verfahrens.

Praxis

*Frank Damm*gibt die zur Faktorisierung von 100-stelligen Dezimalzahlen notwendige Rechenzeit 1994 mit 2-3 Tagen (50-70 Stunden) an, wenn folgende Hardware zum Einsatz kommt: Parallelrechner mit 1024 Transputern (Inmos T805) mit je 4 MByte Speicher, betrieben bei 30 MHz ([Damm 1995], S. 32).

Im April 1994 wurde eine Zahl mit 129 Dezimalstellen, d.h. 428 Bit faktorisiert. Nötig waren dazu etwa 1600 Computer, die im Internet verbunden waren. *Ronald L. Rivest* hatte 1977 die Zahl veröffentlicht und die notwendige Zeit auf 40 Quadrillionen Jahre abgeschätzt. Statt dessen wurden etwa 150 Billiarden Rechenoperationen benötigt ([Wobst 1997 (I)], S. 153). Ein anderes Maß gibt an: 4000-6000 MIPS-Jahre. (1 MIPS = 1 Million Instructions Per Second) Mit einer neueren mathematischen Methode wäre nur etwa ein Zehntel der Zeit benötigt worden (nach [Schneier 1996], S. 301).

Siehe auch: Primfaktorzerlegung

Sieb des Erathostenes

Das Sieb des Erathostenesist ein Verfahren zur Erzeugung aller Primzahlen (in einem bestimmten Zahlenbereich).

Funktionsweise

Zuerst markiert man alle Zahlen im Bereich von 2 bis x als Primzahlen. Dann beginnt man mit der 2 und entfernt bei allen Vielfachen von 2, d.h. 4, 6, 8, ... , die Markierung. Wenn man die Obergrenze x erreicht oder überschritten hat, ist man mit der ersten Runde fertig. Dann sucht man von vorn beginnend die nächste Zahl, die markiert ist und demarkiert alle ihrer Vielfachen. Damit fährt man fort, bis man die Vielfachen aller Zahlen im Bereich 2 bis x demarkiert hat. Alle Zahlen, die danach noch markiert sind, sind Primzahlen.

In einer Art Pseudo-Programmcode sieht das im einfachsten Fall so aus:

```
/* Alle Primzahlen im Bereich bis 1000 finden */

CONST x=1000
CONST TRUE=1
CONST FALSE=0
bereich=ARRAY[1..1000]

/* Das Feld initialisieren */

FOR i=1 TO x DO

     ARRAY[i]=TRUE

END FOR

FOR i=2 TO x STEP 1 DO

     IF ARRAY[i] EQUAL TRUE

          /* i ist eine Primzahl */

          FOR j=2 TO x STEP 1 DO

               /* Markiere alle Vielfachen von i, daß sie keine Primzahlen sind */

               IF (i*j) GREATER x
```

```
                    /* Interessant sind nur Zahlem im Bereich 2 bis x */

                    BREAK

                END IF

                /* Vielfache sind keine Primzahlen */

                ARRAY[i*j] = FALSE

            END FOR

        END IF

END FOR
```

Dieses Verfahren hat zwei wesentliche Nachteile:

1. Es ist für große Primzahlen sehr langsam.
2. Der Speicherplatzverbrauch ist sehr groß.

Der Vorteil des Verfahrens besteht darin, daß auf diese Art alle Primzahlen gefunden werden können.

Private Key Kryptographie

Private Key Kryptographie - (engl.) private key cryptography

Die Private Key Kryptographieist die `klassische' Kryptographie, die mit einem einzigen Schlüssel für die Verschlüsselung und für die Entschlüsselung auskommt. Früher hießsie einfach nur Kryptographie. Erst nach der Einführung der Public Key Kryptographiewurde sie zur Unterscheidung als Private Key Kryptographiebezeichnet.

private key cryptography

private key cryptography (engl.) - Private Key Kryptographie

Public Key Kryptographie

Public Key Kryptographie - (engl.) public key cryptography

Bei der Public Key Kryptographie[**Anm.:** Eine bessere Übersetzung gibt es anscheinend nicht.]handelt es sich um das Gebiet der Kryptographie, daßsich mit Verschlüsselungsverfahren beschäftigt, die auf zwei unterschiedlichen Schlüsseln basieren: einem geheimen Schlüssel (secret key) und einen nicht geheimen Schlüssel, auch öffentlicher Schlüssel (public key) genannt.

Traditionelle Verschlüsselungsverfahren arbeiten dagegen mit einem einzigen Schlüssel (key, secret key) bzw. mehreren Schlüsseln, die sich jedoch leicht voneinander ableiten lassen.

Die Idee zu dieser Form der Verschlüsselung haben Whitfield Diffie und Martin Hellman 1976 vorgestellt. Die erste Implementierung, das RSA-Verfahren, stammt von R. Rivest (**R**), A. Shamir (**S**) und L. Adleman (**A**) (1977 bzw. 1978).

Die Verfahren der Public Key Kryptographie werden der asymmetrischen Verschlüsselung zugerechnet.

Private-Key-Verschlüsselungsverfahren

Private-Key-Verschlüsselungsverfahren - (engl.) private key cryptosystem

Private-Key-Verschlüsselungsverfahrensind symmetrische Verschlüsselungsverfahren, die mit einem geheimen Schlüssel (secret key) arbeiten.

Siehe auch:asymmetrisches Verschlüsselungsverfahren

private key cryptosystem

private key cryptosystem (engl.) - Private-Key-Verschlüsselungsverfahren

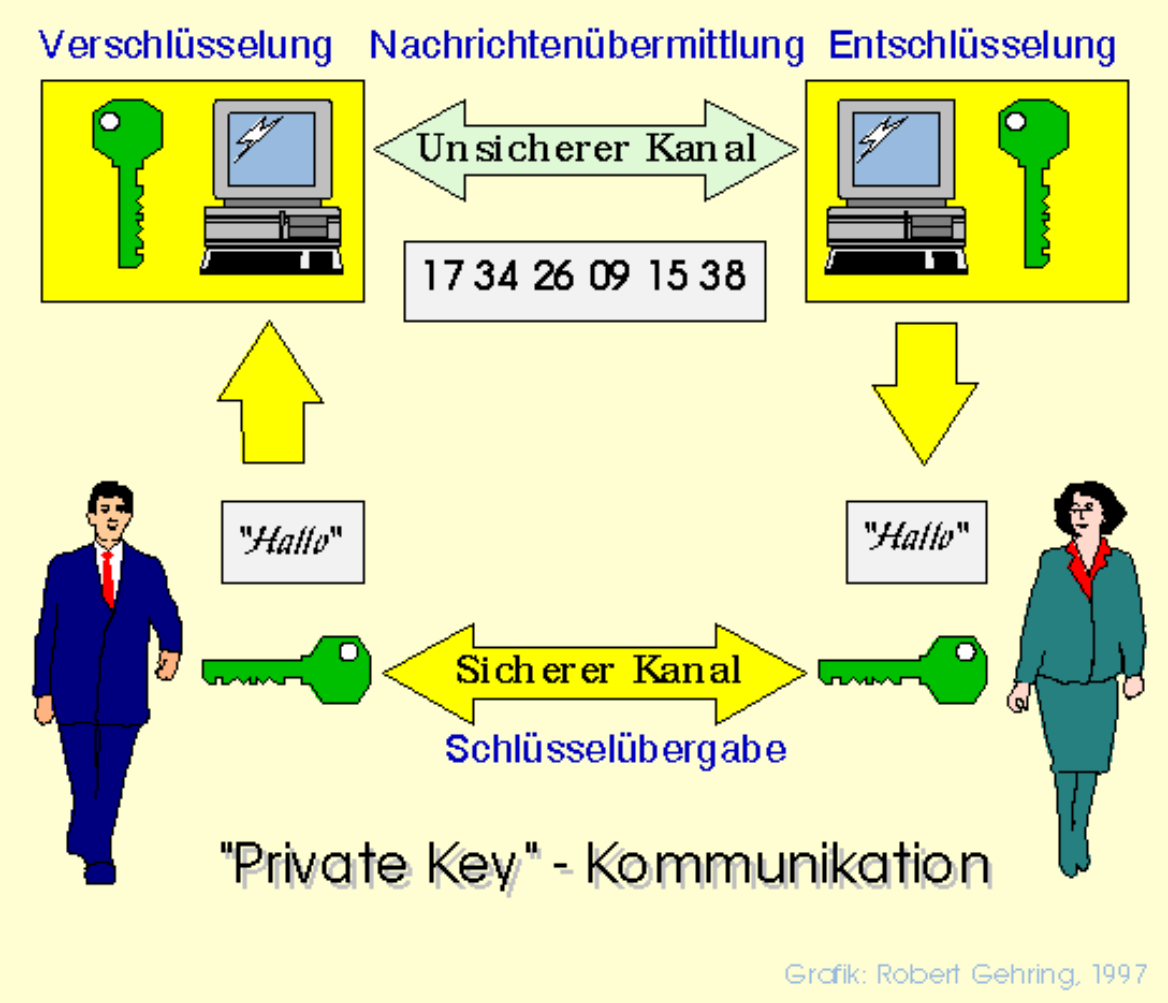
symmetrisches Verschlüsselungsverfahren

symmetrisches Verschlüsselungsverfahren - (engl.) symmetric cryptosystem, symmetric encryption scheme, symmetric cipher

Bei einem symmetrischen Verschlüsselungsverfahrenverwendet man zur Verschlüsselungund zur Entschlüsselungdenselben Schlüssel. Es gibt nur einen, geheimen Schlüssel, weshalb man bei Kommunikation mit symmetrischer Verschlüsselung oft von "private key communication" spricht.

Schema

Symmetrische Verschlüsselung wird nach folgendem Schema vorgenommen:



Zuerst mußdie Schlüsselübergabe bzw. der Schlüsseltausch über den sicheren Kanal erfolgen. Danach können die Teilnehmer Nachrichten, die vom Sender/von der Senderin stammen, entschlüsseln. Selbst können sie Nachrichten für den Enpfänger/die Empfängerin verschlüsseln. Solange der Schlüssel geheim bleibt, sollte der Nachrichtenaustausch undurchschaubar bleiben.

Sicherheit

Die Sicherheit eines solchen Verfahrens hängt in der Hauptsache vom geheimen Schlüsseltausch ab. Man benötigt dazu mindestens einen sicheren Kanalzum Schlüsseltausch.

Vorteile

Symmetrische Verfahren sind schnell, etwa 1000-mal schneller als vergleichbar sicher verschlüsselnde asymmetrische Verfahren. Die Schlüssellängen sind deutlich kleiner, als bei asymmetrischen Verfahren. Diese beiden Eigenschaften prädestinieren symmetrische Verschlüsselungsverfahrenfür die Verschlüsselung großer Datenmengen.

Nachteile

Man benötigt einen sicheren Kanal für den Schlüsseltausch, bzw. die Schlüsselübergabe.

Siehe auch:asymmetrisches Verschlüsselungsverfahren

---

secret key

secret key (engl.) - geheimer Schlüssel

Die Bezeichnung `secret key' ist eher ungebräuchlich. Statt dessen wird in der Regel die Bezeichnung private key verwendet, wenn es um die Verschlüsselung in Public-Key-Cryptosystemen geht.

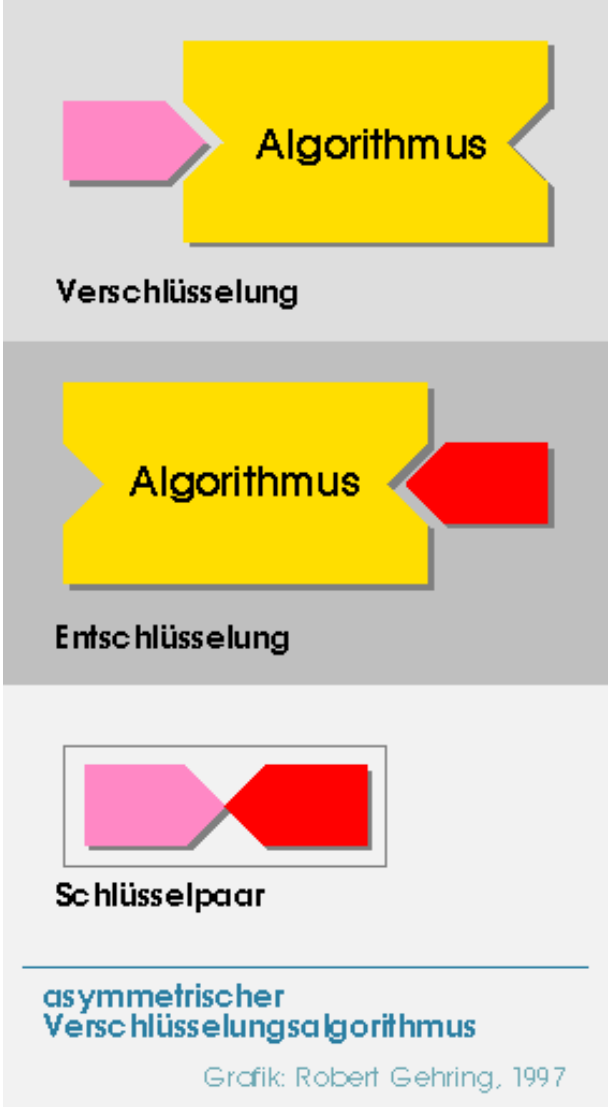
Im Zusammenhang mit herkömmlichen, symmetrischen Verschlüsselungsverfahren spricht man üblicherweise einfach nur von key, auch wenn dieser geheim (*secret*) bleiben muß.

Siehe auch: private key, public key

asymmetrisches Verschlüsselungsverfahren

asymmetrisches Verschlüsselungsverfahren - (engl.) asymmetric cryptosystem, asymmetric encryption

Bei der Verschlüsselung mit einem asymmetrischen Verschlüsselungsverfahren werden zur Verschlüsselung und zur Entschlüsselung unterschiedliche Schlüssel verwendet.



Eine bestimmte Sorte von asymmetrischen Verschlüsselungsverfahren hat in letzter Zeit besonders großes Interesse gefunden, die Public-Key-Verschlüsselungsverfahren. Bei diesen Verfahren ist es möglich, sicher über unsichere Kanäle zu kommunizieren, bzw. die Kommunikation über unsichere Kanäle zu authentifizieren.

Siehe auch: symmetrisches Verschlüsselungsverfahren, asymmetrischer Verschlüsselungsalgorithmus

---

privater Schlüssel

privater Schlüssel - (engl.) private key

Ein privater Schlüssel ist der geheime Schlüssel (secret key) in einem Schlüsselpaar aus geheimem und öffentlichem Schlüssel. Solche Schlüsselpaare werden bei Public-Key-Verschlüsselungsverfahren, einer Sorte von asymmetrischen Verschlüsselungsverfahren, eingesetzt.

Siehe auch: geheimer Schlüssel, öffentlicher Schlüssel, public key

private key

private key (engl.) - privater Schlüssel, geheimer Schlüssel

Siehe auch: secret key

Public-Key-Verschlüsselungsverfahren

Public-Key-Verschlüsselungsverfahren - (engl.) public key cryptosystem

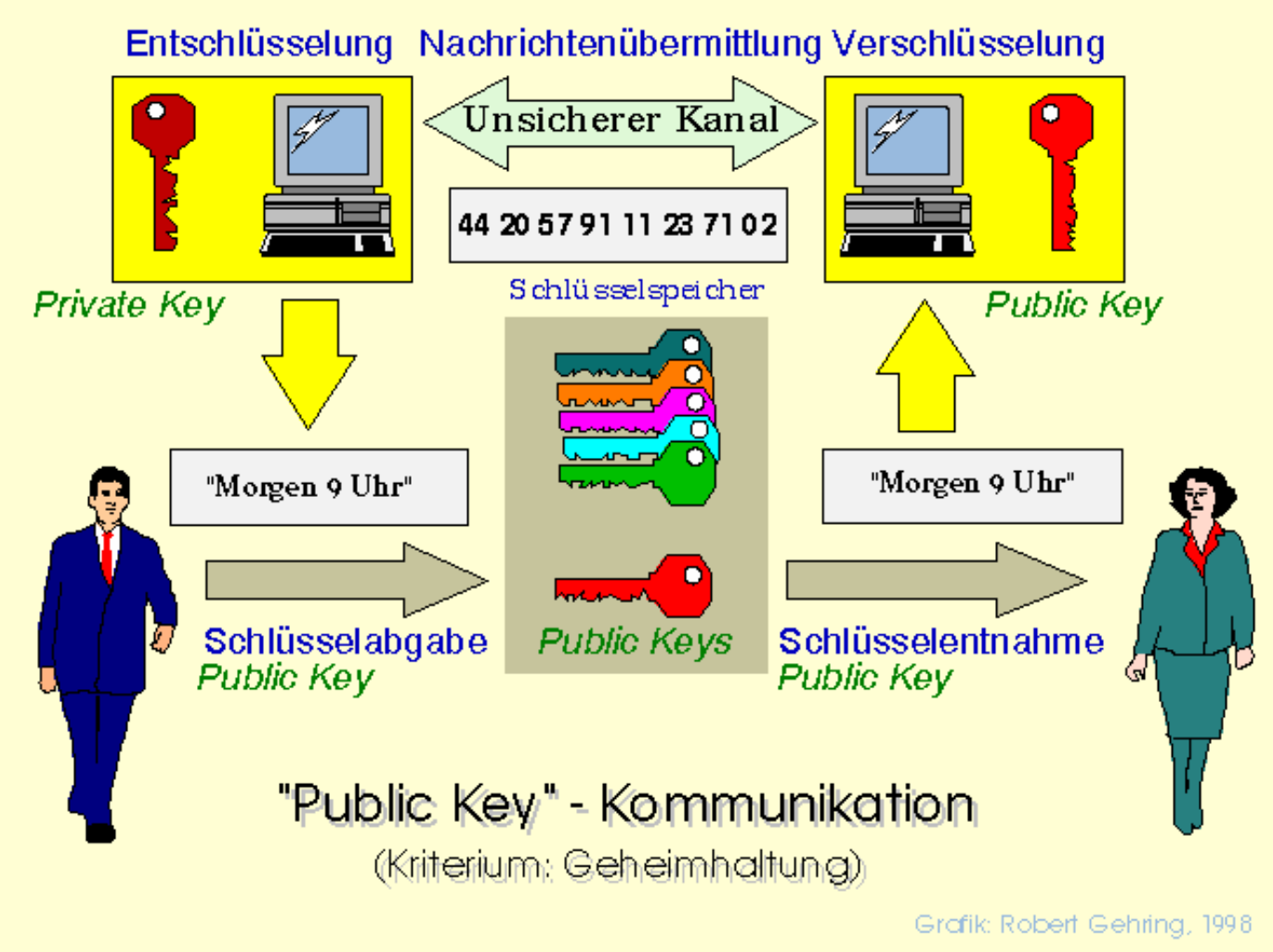
Public-Key-Verschlüsselungsverfahren sind asymmetrische Verfahren.

Bei der Verschlüsselung mit einem Public-Key-Verschlüsselungsverfahren werden zur Verschlüsselung und zur Entschlüsselung unterschiedliche Schlüssel verwendet, die nicht leicht voneinander ableitbar sind. Ein Schlüssel heißt öffentlicher Schlüssel, der zweite heißt privater oder geheimer Schlüssel.

Es gibt zwei unterschiedliche Varianten, diese Schlüssel einzusetzen:

- zur vertraulichen Kommunikation
- zur Authentifizierung

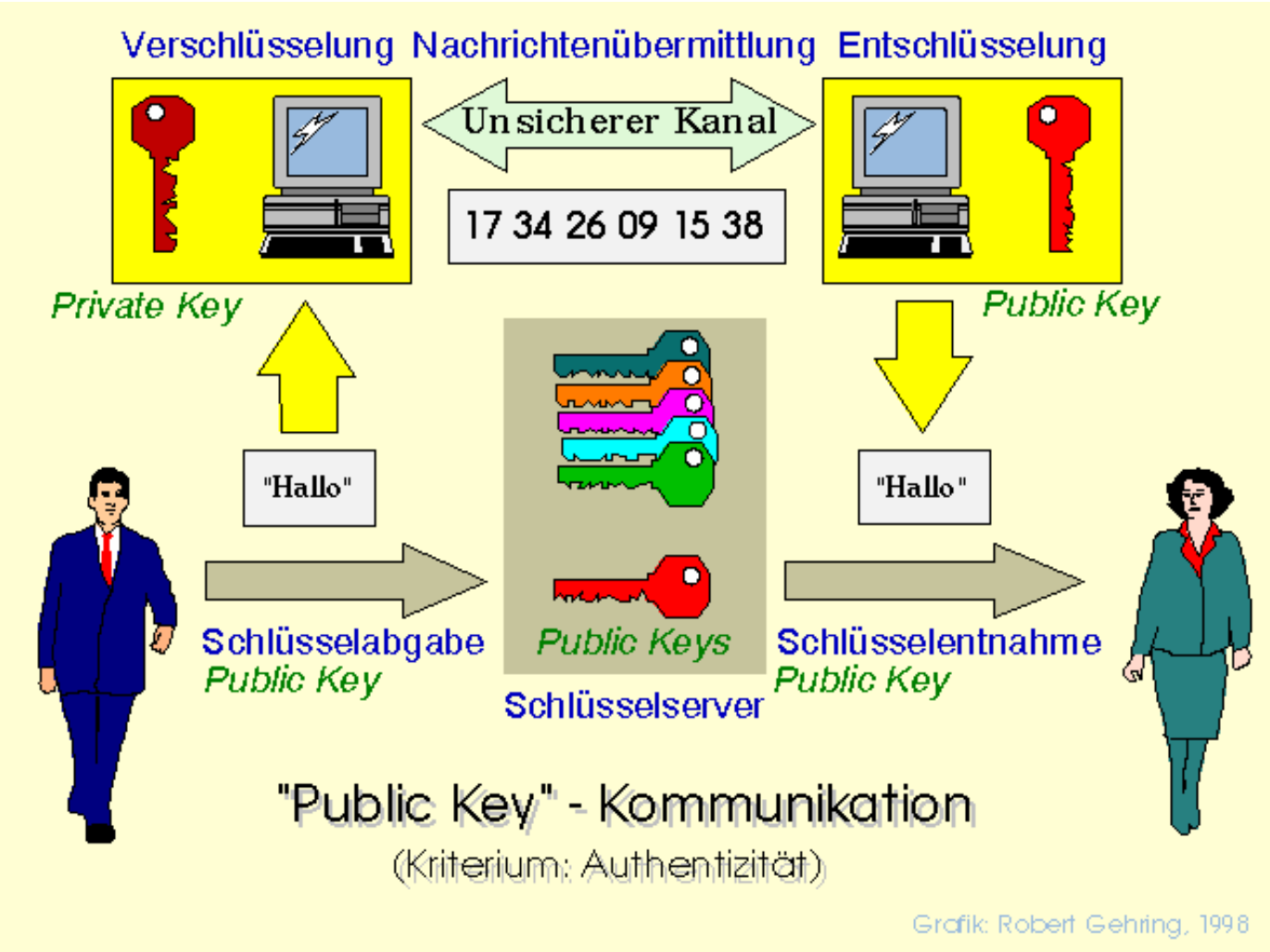
Vertrauliche Kommunikation



Ablauf

Der Empfänger einer vertraulichen Nachricht erzeugt zwei Schlüssel, einen öffentlichen Schlüssel (public key) und einen privaten Schlüssel (private key). Den öffentlichen Schlüssel hinterlegt er in einem öffentlichen Schlüsselspeicher, was in der Regel ein öffentliches Verzeichnis auf einem öffentlich zugänglichen Server sein wird. Wenn ihm jemand eine vertrauliche Nachricht zukommen lassen will, so nimmt er (in unserem Falle sie) den öffentlichen Schlüssel aus dem Schlüsselspeicher und verschlüsselt die Nachricht damit. Die verschlüsselte Nachricht kann nun von niemandem mehr entschlüsselt werden, mit Ausnahme des Besitzers des geheimen Schlüssels. Somit kann die verschlüsselte Nachricht über einen unsicheren Kanal, z.B. das Telefonnetz oder das Internet übertragen werden. Vor Abhören ist sie gut geschützt.

Authentifizierung



Ablauf

Jemand will eine Nachricht übermitteln. Diese Nachricht muß nicht geheim gehalten werden, aber sie soll auf keinen Fall verfälscht werden. Der Emfänger (hier: die Empfängerin) soll gleichzeitig ganz sicher sein können, von wem die Nachricht stammt, d.h. sie will die Authentizität der Nachricht gesichert wissen.

Der Absender der Nachricht greift also zu seinem geheimen Schlüssel und verschlüsselt die Nachricht. Dann schickt er sie über den unsicheren Kanal an die Empfängerin. Diese entnimmt dem Schlüsselspeicher den öffentlichen Schlüssel des Absenders und entschlüsselt die Nachricht damit. Gelingt ihr dies, so weiß sie, daß die Nachricht unverfälscht ist und daß sie vom Inhaber des geheimen Schlüssels stammt, dessen öffentlichen Schlüssel sie zur Dechiffrierung benutzt hat. Die Nachricht ist demnach authentisch.

Zertifizierung

In beiden Fällen sind Absender und Empfänger ohne Schlüsselübergabe ausgekommen! Ungeklärt ist allerdings in beiden Szenarien, wie denn Empfänger und Absender Sicherheit über die Identität der Person auf der anderen Seite gewinnen können. Eine Möglichkeit wäre die persönliche Schlüsselübergabe. Damit würde aber ein großer Vorteil des Konzeptes der asymmetrischen Verschlüsselungsverfahren wieder zunichte gemacht. Bei Personen, die über Länder- oder gar Kontinentsgrenzen hinweg kommunizieren, dürfte der persönliche Schlüsselaustausch ohnehin unpraktikabel sein.

Eine Alternative bieten Zertifizierungen. Instanzen, sogenannte "glaubwürdige Dritte" (trusted third parties), übernehmen dabei die Aufgabe, Identitäten von Personen, deren öffentliche Schlüssel im Schlüsselspeicher hinterlegt werden, zu prüfen und zu bestätigen, mit einem Zertifikat. Wer nun sichergehen will, daß ein öffentlicher Schlüssel tatsächlich zu der Person

gehört, die solches behauptet, kann das Zertifikat einsehen und sich davon überzeugen.

"Web of Trust"

Anstelle der Beglaubigung der Schlüsselzugehörigkeiten durch dritte Instanzen könnte man sich aber auch vorstellen, daß Personen, die einander vertrauen sich gegenseitig zertifizieren. Die Idee dabei ist folgende:

> A kennt B. A bestätigt B, daß dieser Schlüsselinhaber des öffentlichen Schlüssels K_B ist und nimmt den Schlüssel in seine Sammlung öffentlicher Schlüssel auf. B bestätigt A, daß dieser Inhaber von K_A ist und speichert B's Schlüssel. Gleiches macht A mit seiner Bekannten C und B mit seinem Bekannten C.
>
> Bei passender Gelegenheiten tauschen A und B ihre Sammlungen von öffentlichen Schlüsseln aus. Dabei vertrauen sie einander, daß die Identitäten der Schlüsselinhaber von einer vertrauenswürdigen Person überprüft wurden, bevor jene die Schlüssel in die Schlüsselsammlung aufgenommen hat.

Auf diese Weise `pflanzt sich das Vertrauen fort' und das `Web of Trust' entsteht. Der Vorteil bei dieser Variante ist, daß auf eine Bürokratie für die Schlüsselverwaltung verzichtet werden kann.

Siehe auch: symmetrisches Verschlüsselungsverfahren, asymmetrisches Verschlüsselungsverfahren, Private-Key-Verschlüsselungsverfahren

---

geheimer Schlüssel

geheimer Schlüssel - (engl.) private key, secret key

Der geheime Schlüssel ist der einzige Schlüssel in einem symmetrischen Verschlüsselungsverfahren oder der zu einem öffentlichen Schlüssel zugehörige private Schlüssel in einem asymmetrischen Verschlüsselungsverfahren.

Siehe auch: privater Schlüssel

öffentlicher Schlüssel

öffentlicher Schlüssel - (engl.) public key

Öffentliche Schlüsselgibt es nur bei Verfahren der asymmetrischen Verschlüsselung.

Zu jedem öffentlichen Schlüssel existiert ein geheimer Schlüssel (privater Schlüssel). Es gibt zwei Möglichkeiten, mit einem Schlüsselpaar aus öffentlichem und privatem Schlüssel zu verschlüsseln:

1. Verschlüsselung des Klartextes mit dem öffentlichen Schlüssel. Dann kann nur der Inhaber des geheimen Schlüssels den Geheimtext lesen (weil entschlüsseln).
2. Verschlüsselung des Klartestes mit dem geheimen Schlüssel. Dann können alle, die Zugriff auf den öffentlichen Schlüssel haben, den Geheimtext lesen. Gleichzeitig haben sie die Sicherheit, daß nur der Inhaber des geheimen Schlüssels den Text verschlüsselt haben kann.

Siehe auch:geheimer Schlüssel, privater Schlüssel

public key

public key (engl.) - öffentlicher Schlüssel

Protokoll

Protokoll - (engl.) protocol

Protokollwird im kryptologischen Sinne als Kurzform von `*kryptographisches Protokoll*' verstanden. Es gibt keine eindeutige Abgrenzung dafür, was als Protokollgelten kann, und was nicht.

An dieser Stelle wird folgender Vorschlag für eine Definition gemacht:

> Sind zwei oder mehr Personen in einen verschlüsselten Nachrichtenaustausch einbezogen und existieren Vorgaben für ihr Verhalten, so spricht man von einem (kryptographischen) Protokoll, wenn man die Verhaltensregeln meint.

Im weiteren Sinne wird unter einem Protokoll eine Menge von Regeln für die Interaktion verstanden. Dabei bezieht sich *Interaktion* sowohl auf Personen, als auch auf Computer(-teile).

protocol

protocol (engl.) - Protokoll

Provider

provider (engl.) - Anbieter

Provider wird oft als Kurzform für Internetprovider benutzt.

Siehe auch: Internetanbieter

Internetprovider

internet provider (engl.) - Internetanbieter

Das aus dem Englischen stammende Internetprovider wurde allgemein in die deutsche Sprache übernommen. Oft wird es mit Provider abgekürzt.

Internetprovider sind Firmen, die Interessenten einen Zugang zum Internet anbieten. Die wichtigste Aufgabe, die sie dabei erfüllen, ist die Verteilung der Internetadressen.

Oft übernehmen sie auch weitergehenden Service, wie z.B. die Pflege von Homepages oder Internetservern. Die Leistungen differieren von Provider zu Provider oft stark. Bevor man sich für einen Internetprovider entscheidet, sollte man sich die Vergleiche, die von den Fachzeitschriften regelmäßig durchgeführt werden, genau ansehen.

Internetanbieter

Internetanbieter - (engl.) internet provider

Internetanbieter ist die -korrekte- deutsche Übersetzung des englischen `*internet provider*'. Weitaus gebräuchlicher ist halbfertige Übersetzung Internetprovider, auch Internet-Provider oder kurz Provider.

Prüfsumme

Prüfsumme - (engl.) check sum(*checksum*)

Das englische *check sum*sollte korrekt mit Prüfsummeübersetzt werden. Es hat sich aber etabliert, auch Checksummezu verwenden.

check sum; checksum

check sum; checksum (engl.) - Checksumme, Prüfsumme

Checksumme

Checksumme - (engl.) checksum

Checksummen-auch Prüfsummengenannt- sind gespeicherte `*Aussagen*' über den Zustand von Daten. Sie werden ermittelt, indem mathematische Berechnungen über den Daten ausgeführt werden. Das Resultat -die `*Aussage*'- heißt dann Checksumme. Wenn man feststellen will, ob Daten unverändert sind, führt man die Berechnungen erneut aus und vergleicht das Resultat mit der Checksumme. Stimmen beide überein, geht man davon aus, daßdie Daten unverändert sind.

Siehe auch: Cyclic Redundancy Code (CRC), Error Correction Code (ECC)

PTRegG [Postwesen- und Telekommunikationsregulierungsgesetz]

Postwesen- und Telekommunikationsregulierungsgesetz - (engl.) ???

Der Name des PTRegG lautet in voller Schönheit: *Gesetz über die Regulierung der Telekommunikation und des Postwesens*. Es enthält Reglungen zum Umgang mit den Monopolbefugnissen von Post und Telekom, z.B. die Genehmigung von Preisänderungen der Telekom durch den Bundespostminister.

Es trat zum 1. Januar 1995 in Kraft. Da der Telekommunikationsbereich zum 1. Januar 1998 vollständig liberalisiert wird, gilt das Gesetz nur noch bis zum 31. Dezember 1997.

Siehe auch: TKG

TKG [*Telekommunikationsgesetz*]

Telekommunikationsgesetz - (engl.) Telecommunications Act (???)

Das Telekommunikationsgesetz wurde im Sommer 1996 vom Bundestag beschlossen und legt die Regelungen für die Teilnehmer am liberalisierten Telekommunikationsmarkt ab 1. Januar 1998 fest:

> ``*Zweck dieses Gesetzes ist es, durch Regulierung im Bereich der Telekommunikation den Wettbewerb zu fördern und flächendeckend angemessene und ausreichende Dienstleistungen zu gewährleisten sowie eine Frequenzordnung festzulegen.*" (TKG, §1).

Angestoßen wurde die stufenweise Liberalisierung des Telekommunikationsmarktes vom Rat der Europäischen Union im Jahre 1990 (90/387/EWG). Die vollständige Liberalisierung wird zum 1. August 1998 vollzogen sein.

Einige Gesetze und Verordnungen werden vollständig vom TKG abgelöst, so z.B. das Telegrafenwegegesetz (TWG).

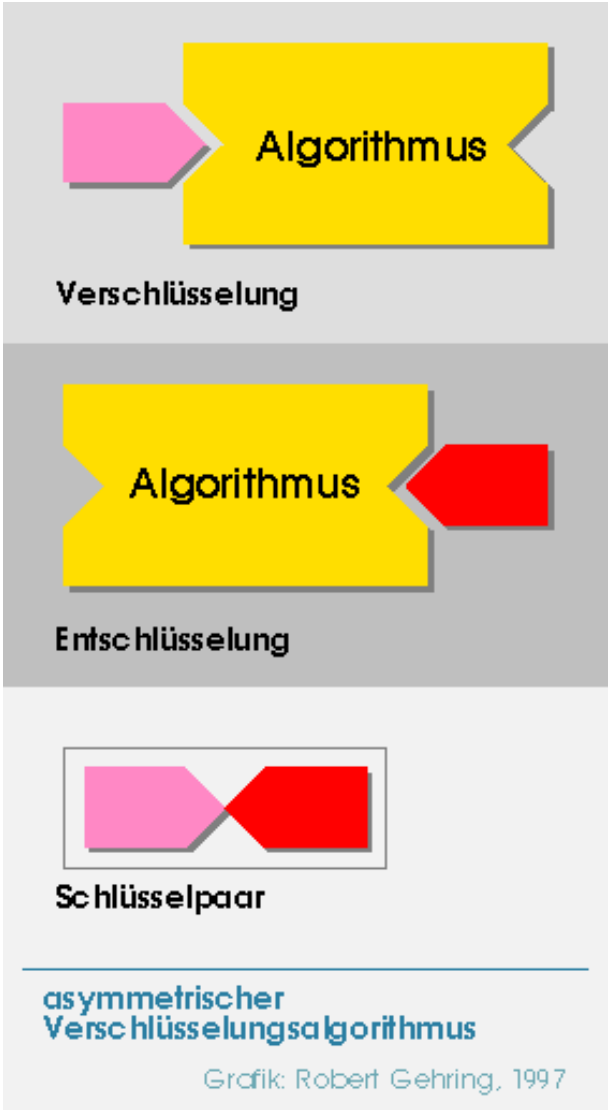
Siehe auch: IuKDG, G10-Gesetz

Gesetzestext

public key-Algorithmus

Public key-Algorithmen sind Verschlüsselungsalgorithmen, die mit paarweise zusammengehörigen Schlüsseln arbeiten.

Das Verhältnis von Algorithmus und Schlüsselpaar läßt sich grafisch so darstellen:



Es handelt sich um asymmetrische Verschlüsselungsalgorithmen, deren einer Schlüssel öffentlich zugänglich gemacht und deren anderer Schlüssel geheimgehalten wird. Wird eine Nachricht mit dem öffentlichen Schlüssel verschlüsselt, kann sie nur mit Hilfe des geheimen Schlüssels entschlüsselt werden. Umgekehrt kann eine mit dem geheimen Schlüssel verschlüsselte Nachricht nur bei Kenntnis des öffentlichen Schlüssels entziffert werden. Diese Form der verschlüsselten Kommunikation heißt public key communication.

public key communication

public key communication (engl.) - Kommunikation mit öffentlichem Schlüssel

Anmerkung: Es hat sich bisher kein deutscher Begriff etabliert, statt dessen wurde der Terminus als `Public-Key-Kommunikation' übernommen. Wollte man korrekt sein, so müßte man von asymmetrisch verschlüsselter Kommunikation sprechen.

Siehe auch:private key communication

Public-Key-Kommunikation

Public-Key-Kommunikation - (engl.) public key communication

public key cryptography

public key cryptography (engl.) - Public Key Kryptographie

asymmetrische Verschlüsselung

asymmetrische Verschlüsselung - (engl.) asymmetric encryption

Siehe: asymmetrisches Verschlüsselungsverfahren

Public Key-Verschlüsselung

Public Key-Verschlüsselung - (engl.) public key encryption

Public Key-Verschlüsselungist ein Synonym für die asymmetrische Verschlüsselung.

Public-Key-Verschlüsselungssystem

Public-Key-Verschlüsselungssystem - (engl.) public key cryptosystem

Ein Public-Key-Verschlüsselungsystem ist ein technisches System (Geräte+Protokolle), mit dem eine asymmetrische Verschlüsselung nach einem Public-Key-Verschlüsselungsverfahren abgewickelt wird.

Siehe auch: Verschlüsselungssystem

public key cryptosystem

public key cryptosystem (engl.) - Public-Key-Verschlüsselungsverfahren, Public-Key-Verschlüsselungssystem

Verschlüsselungssystem

Verschlüsselungssystem - (engl.) cryptosystem, encryption system

Der Begriff des Verschlüsselungssystemswird unterschiedlich ausgelegt. Im engeren Sinne wird darunter ein Paar aus Verschlüsselungsalgorithmusund Entschlüsselungsalgorithmusverstanden. Im weiteren Sinne bezieht man noch die Menge der Schlüssel, ggf. ein Verfahren zu ihrer Generierung, sowie Klartextund Geheimtextmit ein. Im umfassendsten Sinne beschreibt der Begriff zusätzlich die Implementierung (in einem Gerät, in einer Software) und das Protokoll, d.h. die Ablauforganisation.

Anmerkung: Den scheinbar naheliegenden Begriff `*Entschlüsselungssystem'* gibt es nicht!

PBC [*Plaintext Block Chaining*]

Plaintext Block Chaining (engl.) - Klartextblockverkettung

PCA [*Policy Certification Authority*]

Policy Certification Authority (engl.) - *sinngemäß:*Regulierungsinstanz, Regulierungsauthorität

PCA's sind Bestandteile einer Zertifizierungshierarchie, wie sie in X.509vorgeschlagen wird. Die PCA's sind dafür zuständig, Richtlinien für die Vergabe von und den Umgang mit Zertifikatenzu erarbeiten.

Siehe auch:RFC 1422(PEM)

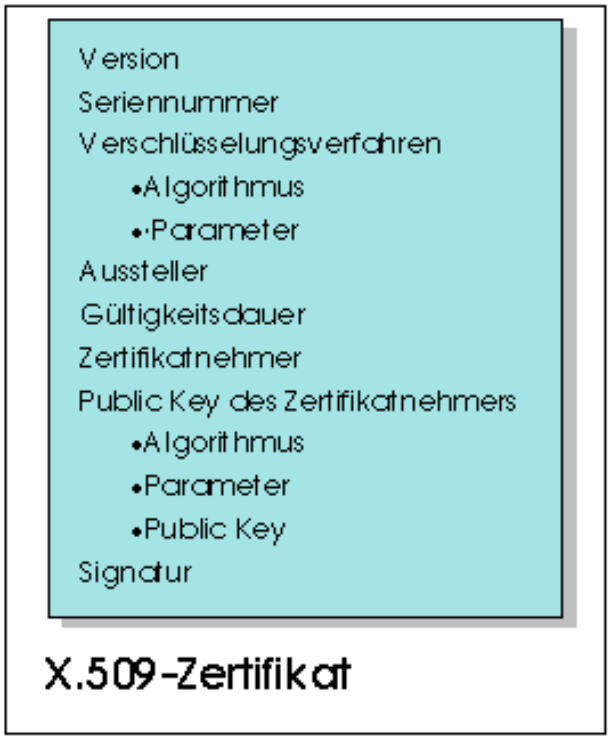
< Terminus >

<Text >

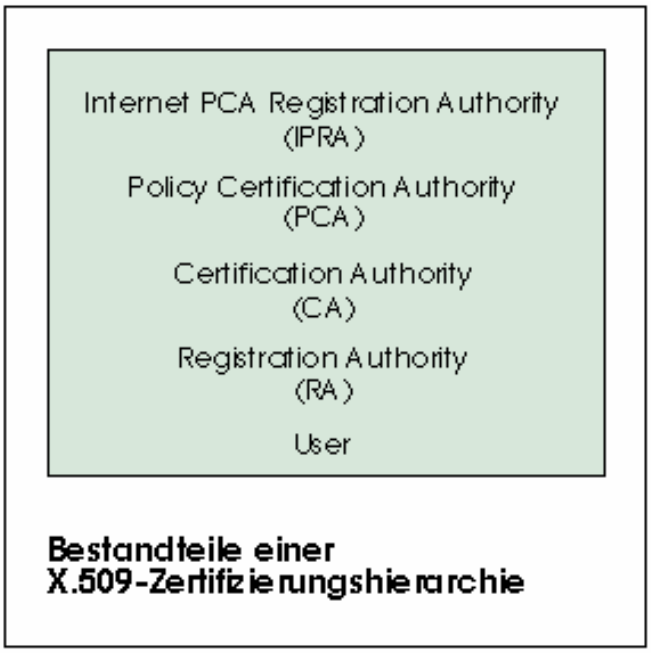
X.509

X.509ist ein Standard der ISO/IEC für die Authentifizierung in offenen Netzen aus dem Jahr 1988. Darin werden die einfache Authentifizierung, gesichert durch ein Paßwort, und die verschärfte Authentifizierung, mit geheimen Schlüsselinformationen, definiert.

Unter anderem werden in X.509 Zertifikate für digitale Signaturen beschrieben.



Die Zertifizierungsstruktur nach X.509 hat folgende Elemente:



Bestandteile einer X.509-Zertifizierungshierarchie

Eingangsseite | Index | Mail

Zertifikat

Zertifikat - (engl.) certificate

PEM [*Privacy Enhanced Mail*]

Privacy Enhanced Mail (engl.) - sinngemäß: vertrauliche (elektronische) Post

Eingangsseite Index Mail

permanent secret key

permanent secret key (engl.) - dauerhafter geheimer Schlüssel, *auch:*Poolschlüssel, Generalschlüssel

Um die Sicherheit symmetrischer Verschlüsselunggegenüber Klartextangriffenzu verbessern, teilt man den Verschlüsselungsprozeßin zwei Teile:

1. Die Kommunikationspartner einigen sich auf einen Schlüssel für die symmetrische Verschlüsselung. Dieser wird als `dauerhafter geheimer Schlüssel' (permanent secret key) bezeichnet.
2. Zum Nachrichtenaustausch wird für jede einzelne Datenübermittlung vom Sender ein neuer Schlüssel erzeugt, der Sitzungsschlüssel (session key). Mit diesem wird die Nachricht verschlüsselt. Anschließend wird der Sitzungsschlüssel mit dem `dauerhaft geheimen Schlüssel' verschlüsselt, der bereits verschlüsselten Nachricht hinzugefügt und beides an den Empfänger übermittelt. Zuletzt vernichtet der Sender den Sitzungsschlüssel (siehe: Schlüsselvernichtung).

   Der Empfängerverfügt seinerseits über den `dauerhaft geheimen Schlüssel' und ist somit in der Lage, den verschlüsselten Sitzungsschlüssel zu entschlüsseln. Anschließend kann er mit dem Sitzungsschlüssel die eigentliche Nachricht entschlüsseln.

Unter der Voraussetzung, daßdie Erzeugung der Sitzungsschlüssel (siehe: Schlüsselerzeugung) korrekt vorgenommen wird, kann der Fall, daßmit ein und demselben Schlüssel eine gleiche Nachricht mehrfach verschlüsselt wird, praktisch ausgeschlossen werden. So erhält man eine hohe Resistenz gegen Klartextangriffe.

symmetrische Verschlüsselung

symmetrische Verschlüsselung - (engl.) symmetric encryption

Siehe: symmetrisches Verschlüsselungsverfahren

Sender

Sender - (engl.) sender

Der Senderist im allgemeinen Sinne der Absender einer Nachricht. Im kryptographischen Sinne ist der Senderderjenige/diejenige, welcher/welche eine Nachricht verschlüsselt und an den Empfängerschickt.

Sitzungsschlüssel

Sitzungsschlüssel - (engl.) session key

Sitzungsschlüsselsind Schlüssel, die nur einmal zur Kommunikation verwendet werden. Sie werden vor dem Aufbau einer Kommunikationsverbindung erzeugt (Schlüsselerzeugung), zur Verschlüsselungder Kommunikation benutzt und anschließend vernichtet (Schlüsselvernichtung).

session key

session key (engl.) - Sitzungsschlüssel, Einmalschlüssel

Empfänger

Empfänger - (engl.) receiver

Der Empfängerist im allgemeinen der Adressat einer Nachrichtvon einem Sender. Unter einem kryptologischen Gesichtspunkt ist ein Empfängerder Adressat einer verschlüsselten Nachricht, die er zu entschlüsselnhat, um sie für sich verständlich (*intelligible*) zu machen. Dazu benötigt er einen Schlüssel.

Schlüsselvernichtung

Schlüsselvernichtung - (engl.) key destruction

Die Schlüsselvernichtung bildet das Gegenstück zur Schlüsselerzeugungund sollte ebenso sorgfältig vorgenommen werden.

Nur, wenn ein Schlüssel mit an absolute Sicherheit grenzender Wahrscheinlichkeit nicht mehr existent ist, hat man Gewißheit, daß der Schlüssel nicht mehr verwendet werden kann. Nur so läßt sich unter Umständen bestimmten kryptographischen Angriffen vorbeugen. Die Schlüsselvernichtung muß die Vernichtung aller Hinweise auf den Schlüssel einschließen.

Viele Anwendungen (z.B. Banktransaktionen) arbeiten mit Einmalschlüsseln (session keys) in Verbindung mit permanenten Schlüsseln (pool keys, permanent secret keys). Die Sicherheit solcher Anwendungen ist nur gewährleistet, wenn jeder Sitzungsschlüssel nur einmal verwendet und dann vernichtet wird. So läßt sich nicht nachträglich ein Transaktionsprotokoll einfach manipulieren.

Beispiele

Werden Schlüssel durch Prozessoren von Chipkarten erzeugt, ist der einzig sichere Weg der Schlüsselvernichtungdie vollständige Zerstörung des Prozessors: Über den Schmelzpunkt des Siliziums, aus dem die Schaltung hergestellt wurde, erhitzen.

Wurden Schlüssel auf Festplatten gespeichert, müssen die Datenblöcke, in denen sich die Schlüssel befanden mehrfach mit zufälligen Bitfolgen überschrieben werden. Einige zig-Mal dürften genügen, die Restmagnetisierung in ein Rauschen zu verwandeln.

Schlüsselerzeugung

Schlüsselerzeugung - (engl.) key generation

Unter Schlüsselerzeugungversteht man die Erzeugung (Festlegung) der Schlüsselinformation (Schlüssel) für eine Verschlüsselung. Mögliche Formen sind z.B. die Berechnung von Primzahlen beim RSA-Verfahren, die Generierung von Zufallszahlen oder die Festlegung eines Codewortes.

Die Schlüsselerzeugung ist erfolgreich und korrekt, wenn zum einen die erzeugten Schlüssel (der erzeugte Schlüssel) während der Erzeugung geheim bleibt und zum anderen die Qualität der Schlüssel hinreichend ist. Sogenannte schwache Schlüssel oder auch zu kurze Schlüssel sollten vom Generierungsverfahren vermieden werden.

Nach der Erzeugung müssen die Schlüssel verteilt bzw. übergeben (Schlüsselverteilung, Schlüsselübergabe) und in den Schlüsselverwaltungszyklus (key management cycle) integriert werden.

Siehe auch: Schlüsselgenerierung

PES [*Proposed Encryption Standard*]

proposed encryption standard (engl.) - vorgeschlagener Standard für Verschlüsselung

PES wurde 1990 von James Massey und Xueija Lai vorgestellt. Er wurde an der ETH Zürich in Zusammenarbeit mit der Firma Ascom entwickelt. Der Nachfolger von PES hieß IPES (Improved Encryption Standard) und wurde später (1992) in IDEA (International Data Encryption Algorithm) umbenannt.

IPES [*Improved Proposed Encryption Standard*]

improved proposed encryption standard (engl.) - verbesserter vorgeschlagener Standard für Verschlüsselung

IPES ist ein Blockchiffrieralgorithmus und heißt inzwischen IDEA (seit 1992). IPES ist der Nachfolger von PES (Proposed Encryption Standard).

IDEA [*International Data Encryption Standard*]

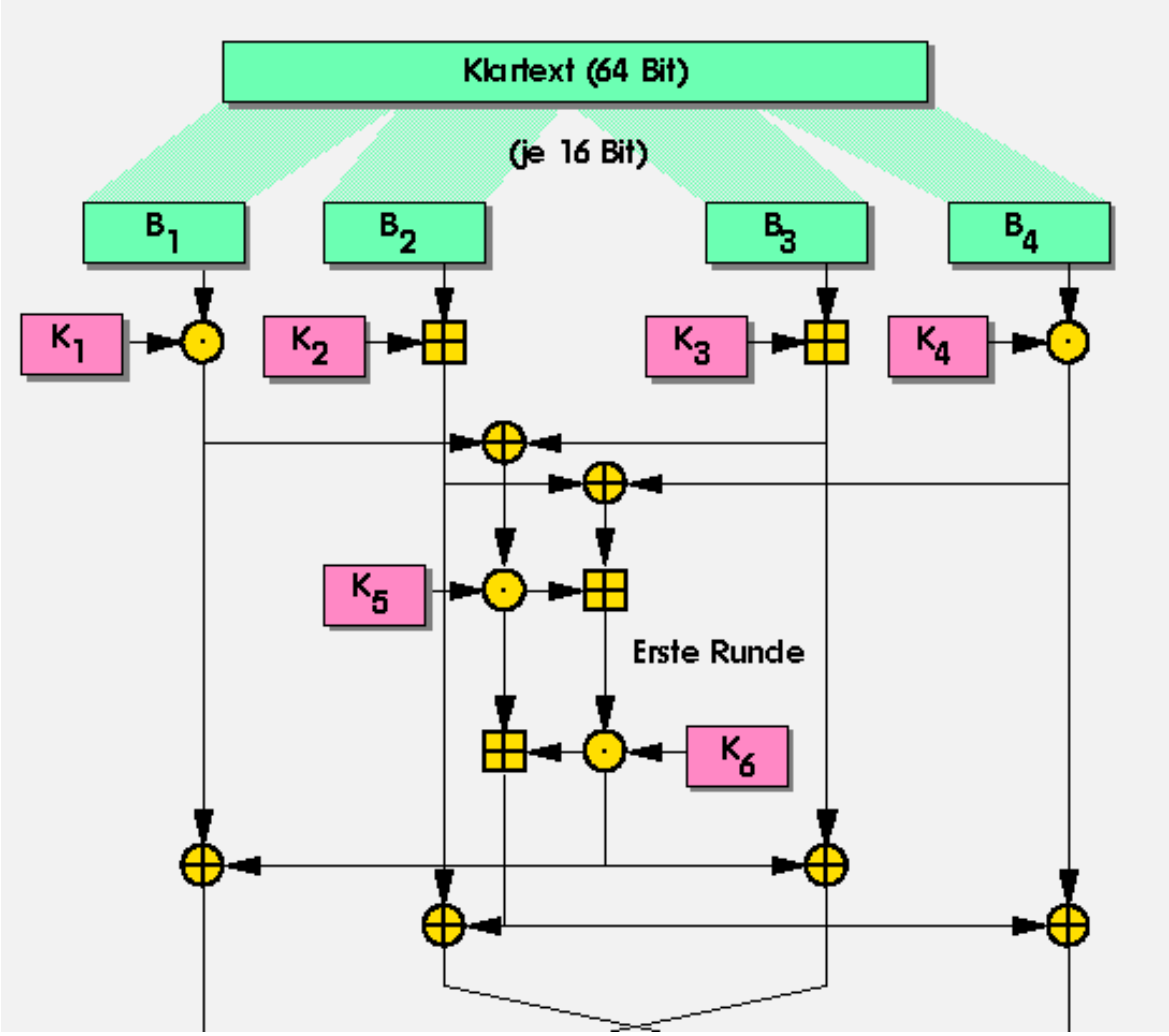
international data encryption standard (engl.) - internationaler Verschlüsselungsstandard

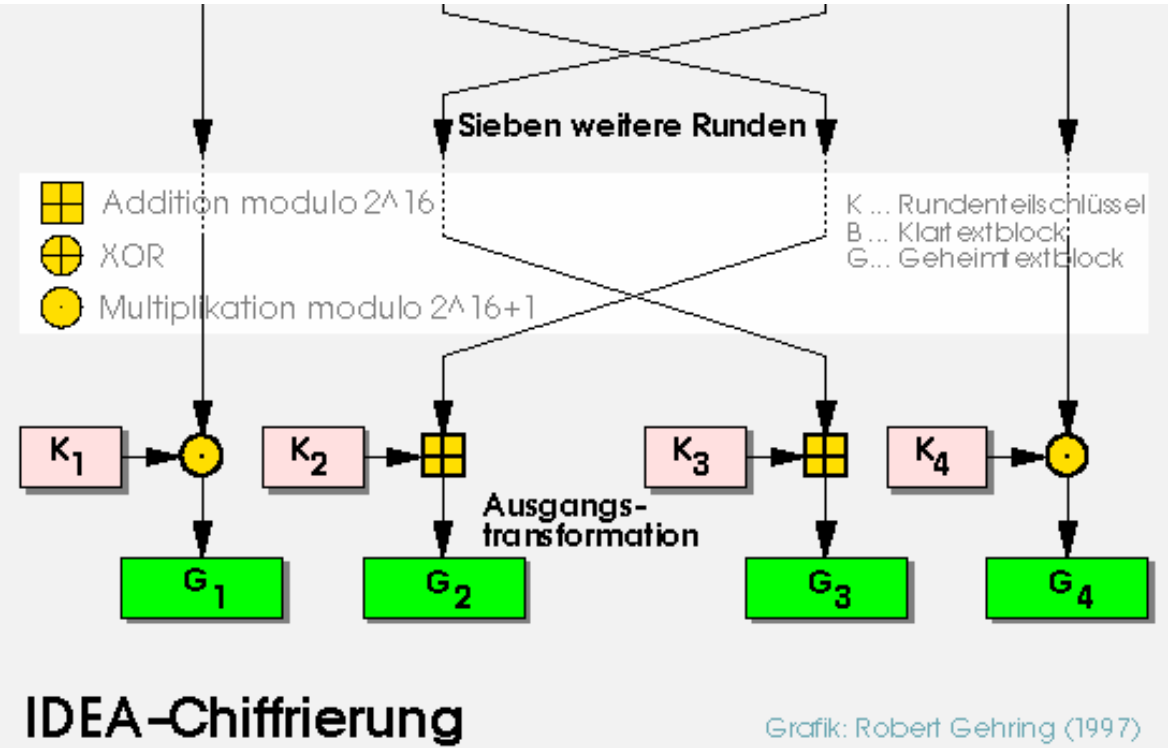
IDEAwurde von Xueija Lai und James Massey entwickelt. Seine Vorgänger waren PES(Proposed Encryption Standard) und IPES(Improved Proposed Encryption Standard). IDEAverwendet sowohl Diffusion, als auch Konfusion.

Arbeitsweise

IDEAarbeitet auf 64 Bit-Klartextblöcken, die mit einem Schlüssel der Länge 128 Bit in 8 Runden verschlüsselt werden. Die Teilschlüssel werden in jeder Runde aus dem Schlüssel generiert.

Schematisch läßt sich IDEA so darstellen:





Bedeutung

Bruce Schneier schätzt IDEAals den zur Zeit sichersten Blockchiffrieralgorithmusein ([Schneier 1996], S.370). IDEAist für nichtkommerzielle Anwendung lizenzfrei erhältlich und wird z.B. in PGPverwendet.

Patente

IDEA ist in verschiedenen Ländern patentiert; in den USA unter Patentnummer 5214703.

PGP [*Pretty Good Privacy*]

Pretty Good Privacy (engl.) - ganz annehmbar geschützte/gesicherte Privatsphäre

Der Ausdruck `Pretty Good Privacy' läßt sich nur schwer übersetzen. Man sollte ihn lieber im Original verwenden.

PGP ist ein Programm zum Verschlüsseln und authentifizieren von Dateien und von email. Dazu verwendet es ein hybrides Verfahren: Zuerst wird der geheime Sitzungsschlüssel mit dem RSA-Verfahren verschlüsselt, anschließend die email (die Datei) mittels IDEA und Sitzungsschlüssel verschlüsselt. Primär wurde PGP für die sichere Kommunikation in unsicheren Computernetzwerken, insbesondere dem Internet, entwickelt. Zum Verschlüsseln großer Datenmengen auf lokalen Speichermedien ist es nur bedingt geeignet.

plaintext attack

plaintext attack (engl.) - Klartextangriff

Siehe: known-plaintext attack

pool key

pool key (engl.) - Poolschlüssel

...

private key communication

private key communication (engl.) - Kommunikation mit geheimem Schlüssel

Anmerkung: Es hat sich bisher kein deutscher Begriff etabliert. Korrekterweise müßte von symmetrisch verschlüsselter Kommunikation gesprochen werden.

Siehe auch: public key communication

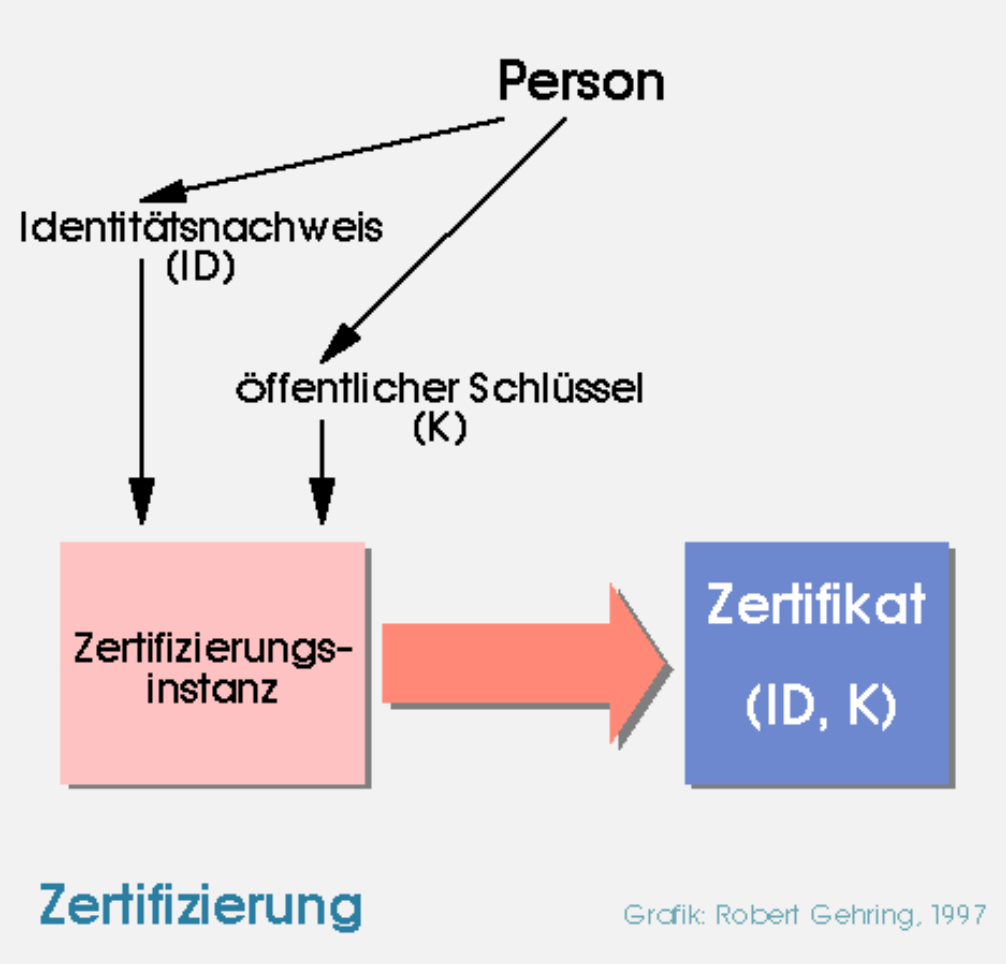
Glossar Digitale Signaturen

Zertifizierung

Zertifizierung - (engl.) certification

Unter Zertifizierung versteht man einen Akt der Beglaubigung, der in einem Zertifikat bestätigt wird.

Im Zusammenhang mit digitalen Signaturen sind die Beglaubigung der Zuordnung eines öffentlichen Schlüssels zu einer bestimmten Person und die Beglaubigung des Identitätsnachweises der Person gemeint. Festgehalten werden diese Beglaubigungen in einem personengebundenen Zertifikat.



glaubwürdiger Dritter

glaubwürdiger Dritter - (engl.) trusted third party

Glaubwürdiger Dritterist ein Synonym für vertrauenswürdiger Dritter. Vom Konzept her handelt es sich um eine unabhängige Instanz, der alle Beteiligten ihr Vertrauen -Glauben- schenken. Solch eine Instanz wird mit Aufgaben betreut, die für die Beteiligten von Bedeutung sind. Es handelt sich um eine Art `Schiedsrichter', der die Interessen aller wahrnehmen soll.

Man benötigt solche dritten Instanzen z.B. für die Verwaltung öffentlicher Schlüssel für die Public Key-Verschlüsselung oder für die Verwaltung von Zertifikaten bei der Zertifizierung.

Siehe auch:trusted third instance

trusted third party

trusted third party (engl.) - glaubwürdiger Dritter, vertrauenswürdiger Dritter

Abbrev.:TTP

See also:trusted third instance

Web of Trust

Web of Trust (engl.) - Netz des Vertrauens

Web of Trustist die Bezeichnung für eine Zertifizierungsstruktur, die nicht hierarchischen Charakter hat. Eine solche Zertifizierungsstruktur ist für den effektiven Einsatz digitaler Signaturenunumgänglich, findet jedoch nicht überall genug Vertrauen. Die Idee des Web of Trustwurde von *P. Zimmerman*zusammen mit PGPentwickelt.

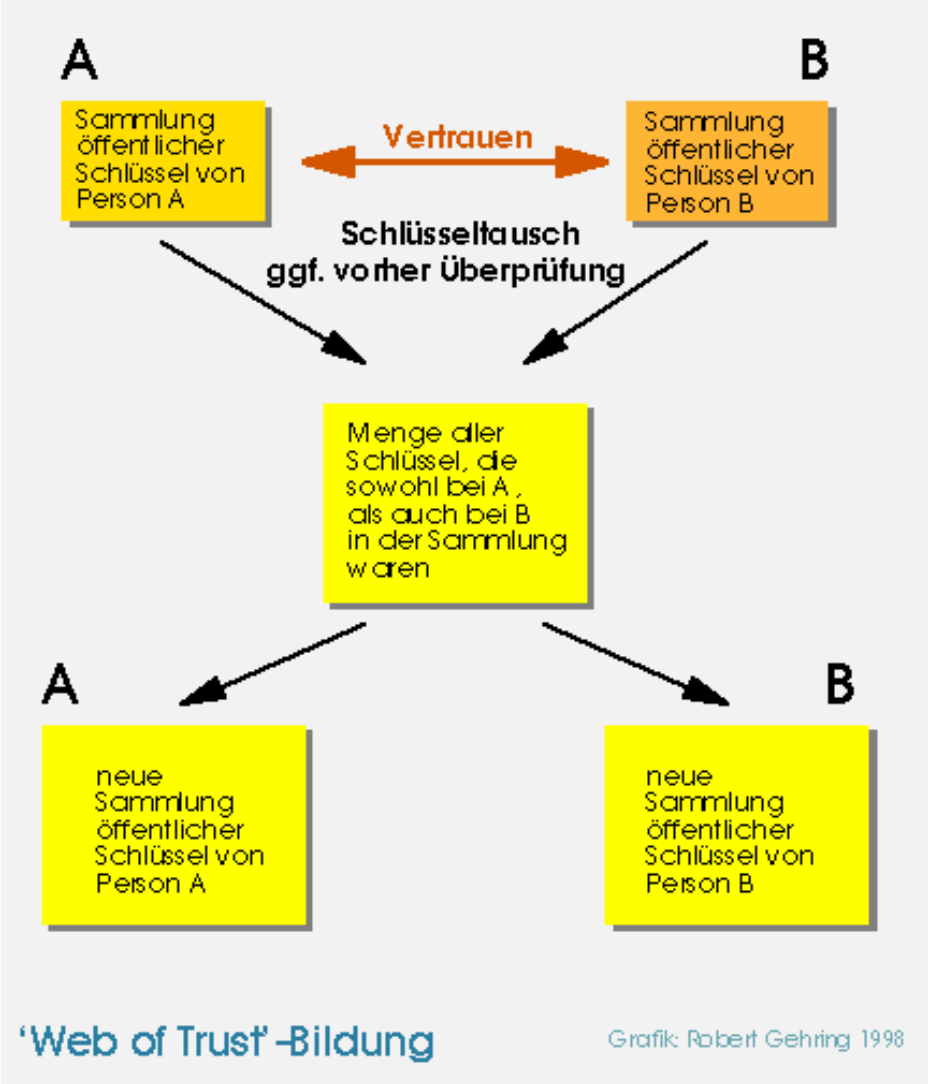
Alternativ zu einem Web of Trust läßt sich eine Zertifizierungshierachie installieren. Diese kann einerseits effektiver arbeiten, andererseit ist sie anfälliger gegen Angriffe.

Funktion

Angenommen, eine Person A hat eine Anzahl öffentlicher Schlüsselvon ihr bekannten Personen erhalten. Schlüssel, die A unmittelbar vom Inhaber in Empfang nimmt, signiert er/sie `eigenhändig' und gibt dem Inhaber eine Kopie davon zurück. Schlüssel, die nicht unmittelbar vom Inhaber stammen überprüft er/sie wenn es notwendig erscheint. Dazu wird mit einem geeigneten Hashverfahren (bei PGPist dies MD5) ein digitaler Fingerabdruckvom signierten Schlüssel erzeugt und vom angeblichen Inhaber ebenfalls ein digitaler Fingerabdruck von dessen Schlüssel angefordert. Stimmen beide überein, ist der Schlüssel in Ordnung (oder es geht um einen ausgefeilten Betrug).

Nun trifft A sich mit einer anderen Person B, die ihrerseits über eine Anzahl öffentlicher Schlüssel aus erster Hand und zweiter Hand verfügt. Vertrauen sich die beiden Personen genügend, so kann jeder dem Gegenüber die Schlüssel aus seiner Sammlung öffentlicher Schlüssel übergeben und bürgt so für die Richtigkeit der Zuordnungen der öffentlichen Schlüssel zu den Identitäten der Besitzer.

Wenn viele Personen so handeln, entsteht das Web of Trust.



PGPkennt unterschiedliche Stufen des Vertrauens. In Abhängigkeit davon werden die gesammelten Schlüssel behandelt.

---

confusion

cookies

CRC

cryptanalist

cryptanalysis

cryptographer

cryptography

cryptologist

cryptology

cryptosystem

CU - See You

DAC - Data Authentication Code

DARPA - Defense Advanced Research Projects Agency

Datenschutz

DEA - Data Encryption Algorithm

decipher

decode

decodieren

decrypt

dekodieren

DES - Data Encryption Standard

Diffusion

digitaler Fingerabdruck

digital fingerprint

digitale Signatur

digitales Wasserzeichen

digital signature

digital watermark

DIN - Deutsche Industrienorm

DSA - Digital Signature Algorithm

DSS - Digital Signature Standard

Deutsch

FAG - Fernmeldeanlagengesetz

Faktorisierung

Faktorisierungsproblem

Falltür

Falltürinformation

FBeitrV - Frequenznutzungsbeitragsverordnung

Feistel-Netzwerk

FGebV - Frequenzgebührenverordnung

Fortezza-Initiative

Fortezza-Karte

FreqZutV - Frequenzzuteilungsverordnung

FÜV - Fernmeldeverkehrsüberwachungsverordnung

English

factoring

factorisation

FIPS - Federal Information Processing Standard

Fortezza Card

Deutsch	English
Hashfunktion	hash function
Hashwert	hash value
HAVAL	
hybrides Verfahren	

Deutsch

English

IAB - Internet Activities Board

IDEA - International Data Encryption Algorithm

IETF - Internet Engineering Task Force

Internetanbieter

Internetprovider

IP - Internet Protocol

IPES - Improved Proposed Encryption Standard

IP-Tunnel

IP-Tunneling

IRTF - Internet Research Task Force

ISAKMP - Internet Security Association and Key Management Protocol

ISO - International Standards Organisation

IuKDG - Informations- und Kommunikationsdienstegesetz

IV - Initialisierungsvektor

IW - Information Warfare

insecure channel

Deutsch

English

JCE - Java Cryptography Engine

JIS - Japanese Industrial Standardisation Committee

Deutsch	English
LOKI	LEAF - Law Enforcement Access Field
LOKI'89	Lucifer
LOKI'91	

Deutsch English

MAC - Message Authentication Code

MD - Message Digest

MD4 - Message Digest 4

MD5 - Message Digest 5

MDC - (1) Modification Detection Code, (2) Message Digest Cipher, (3) Manipulation Detection Code

MDC-2 - Modification Detection Code 2

MDC-4 - Modification Detection Code 4

MEMEX

message

MPQS - Multiple Polynomial Quadratic Sieve

Deutsch

English

öffentlicher Schlüssel

OSI-Referenzmodell

OSIRM - OSI-Referenzmodell

OECD - Organization for Economic Cooperation and Development

OID - Object Identifier

one-time pad

one-way hash function

one-way function

OPS - Open Profiling Standard

OSI - Open Systems Interconnect(ion)

OSS - Ong-Schnorr-Shamir

OT - Oblivious Transfer

OWF - One-Way Function

OWHF - One-Way Hash Function

Deutsch

QS - Quadratisches Sieb

Quantenkryptographie

English

QC - Quantum Cryptography

QS - Quadratic Sieve

quantum cryptography

Deutsch	English
Router	related-key attack
Routing-Rechner	replay attack
Rucksack	RC2 - Rivest Cipher 2
	RC4 - Rivest Cipher 4
	RC5 - Rivest Cipher 5
	RFC - Request For Comment
	RFC-1701 - Request For Comment No. 1701
	ROTFL - Rolling-On-The-Floor-Laughing
	RSA - Rivest-Shamir-Adleman
	RSADSI - RSA Data Security Inc.

Deutsch

S-Box

Schlüssel

Schlüsselerzeugung

Schlüsselgenerierung

Schlüsselhinterlegung

Schlüsseltransport

Schlüsselübergabe

Schlüsselvernichtung

Schlüsselverteilung

Schlüsselverwaltung

schwache Verschlüsselung Sender

sicherer Kanal

Sieb des Erathostenes

SigG - Signaturgesetz

SigV - Signaturverordnung

Sitzungsschluessel

starke Verschlüsselung

Steganographie

English

SECC - Secret Error Correction Code

secret key

secure channel

session key

SHA - Secure Hash Algorithm

SKIP

SKIPJACK

Snefru

SSL - Secure Socket Layer

steganography

stream cipher

stream encryption scheme

strong encryption

substitution

symmetric cipher

symmetric cryptosystem

symmetric encryption

symmetric encryption algorithm

Deutsch

Tesserakarte

TKG - Telekommunikationsgesetz

Transposition

TWG - Telegrafenwegegesetz

English

tamper

tamper-proof

tamper-proof device

tamper resistance

tamper-resistant device

tap

Tessera

Tessera card

trusted third instance

trusted third party

tunneling

Deutsch

English

unsicherer Kanal

UDSA - Utah Digital Signature Act

user profile

Deutsch	English
Wanze	weak encryption
Wörterbuchangriff	Web of Trust

Eingangsseite Index Mail

digitale signaturen diplomarbeit · robert gehring

Deutsch

English

X.509

XOR - eXclusive OR

Eingangsseite Index Mail

digitale signaturen diplomarbeit · robert gehring

Deutsch

English

[Yuval's birthday attack]


Deutsch **English**

MAC [*Message Authentication Code*]

message authentication code (engl.) - Nachrichtenauthentifizierungscode, digitale Signatur

Funktionen zur Erzeugung von MACs sind kollisionsfreie (kollisionsresistente) Einweg-Hashfunktionen, die mit Schlüssel arbeiten.

Siehe auch: message digest (MD), data authentication code (DAC), digitaler Fingerabdruck, modification detection code (MDC)

digitale Signatur

digitale Signatur - (engl.) digital signature

...

Siehe auch: message digest (MD), data authentication code (DAC), message authentication code (MAC)

digital signature

digital signature (engl.) - digitale Signatur

Siehe auch: message digest (MD), data authentication code (DAC), message authentication code (MAC)

MD [*Message Digest*]

message digest (engl.) - digitaler Fingerabdruck

See also:digital fingerprint, message authentication code (MAC), data authentication code (DAC), manipulation detection code (MDC), digital signature, MD4, MD5, RIPE-MD

DAC [*Data Authentication Code*]

data authentication code (engl.) - Datenauthentifizierungscode, digitale Signatur, digitaler Fingerabdruck

Siehe auch: message digest (MD), message authentication code (MAC)

Glossar Digitale Signaturen

Einweg-Hashfunktion

Einweg-Hashfunktion - (engl.) one-way hash function

Eine Einweg-Hashfunktionist eine spezielle Hashfunktion. Einweg-Hashfunktionensind Hashfunktionen, die folgende Kriterien erfüllen:

1. Eingaben beliebiger Größe werden Ausgaben bestimmter Größe zugeordnet (Kompression).
2. Aus der Ausgabe kann nicht auf die Eingabe geschlossen werden (Unumkehrbarkeit).
3. Die Funktion arbeitet kollisionsfrei, d.h. zu jeder möglichen, sinnvollen Eingabe generiert die Einweg-Hashfunktion genau eine Ausgabe. Anders gesagt: Es ist nicht möglich zu einem Hashwert zwei sinnvolle Eingaben zu konstruieren.

Wenn man diese Definition betrachtet, lassen sich die Hashwerte, die von Einweg-Hashfunktionenzu Eingaben generiert werden, als Aussagen über die Eingaben auffassen. Jede Eingabe läßt sich mit genau einer Aussage beschreiben.

Diese Eigenschaft von Einweg-Hashfunktionen wird ausgenutzt, um sogenannte `digitale Fingerabdrücke' von Daten zu erstellen. Die Metapher paßt zwar nicht so recht, hat sich aber durchgesetzt.

Besondere Einweg-Hashfunktionen

Ergänzt man Einweg-Hashfunktionennoch um die Eigenschaft, nur mit einem geheimen Schlüssel zu arbeiten, erhält man sichere Aussagen über die Eingaben. Andere Bezeichnungen für (Ausgaben) solcher Einweg-Hashfunktionensind: message authentication code (MAC), digital fingerprint, data authentication code (DAC), digitale Signatur, message digest (MD), ... Es werden ständig neue Namen gefunden.

In der Praxis verwendet man zuerst eine Einweg-Hashfunktion und verschlüsselt den Hashwert mit einem asymmetrischen Verschlüsselungsverfahren, z.B. RSA. Auf diese Weise erhält man eine digitale Signatur.

Beispiele

Bekannte Einweg-Hashfunktionen sind:

- Secure Hash Algorithm (SHA)
- MD4, MD5
- HAVAL
- Snefru

Siehe auch:kryptographische Hashfunktion

one-way hash function

one-way hash function (engl.) - Einweg-Hashfunktion

Hashfunktion

Hashfunktion - (engl.) hash function

Eine Hashfunktionist eine deterministische Funktion, die Eingaben beliebiger Größe aus einer Menge von Eingabewerten Ausgaben bestimmter Größe aus einer Menge von Ausgabewerten zuordnet. Die Menge der möglichen Ausgabewerte ist (erheblich) kleiner als die der möglichen Eingabewerte, gleiches gilt für die Länge der Ausgabe.

Allgemein: Für alle Elemente einer Menge von Argumenten existiert ein Funktionswert, dessen Informationsgehalt geringer ist, als der seines Argumentes. Eine Funktion, die eine solche Abbildung leistet, ist eine Hashfunktion.

In der Informatik: Eine Hashfunktion ist eine Funktion, die binären Werten aus einer Menge beliebig langer Binärwerte (Argumente) binäre Werte aus einer Menge von Binärwerten mit bestimmter Länge zuordnet (Hashwerte).

Geschichte

Hashfunktionensind immer schon Bestandteil des Alltags, ohne allerdings als solche beschrieben und benannt gewesen zu sein. (Siehe Beispiel)

Hashfunktionen wurden in der Informatik für schnelle Sortier- und Suchverfahren eingeführt. Die Geschwindigkeitssteigerung wurde durch die Komprimierung der Eingabedaten erreicht: Unterschiedliche Eingaben unterschiedlicher Länge erhalten gleiche Ausgabewerte (Hashwerte) gleicher Länge.

Die Kryptographie hat spezielle Hashfunktionen eingeführt - universelle Hashfunktionen und daraus abgeleitet die Einweg-Hashfunktionen. Die Spezialität solcher Einweg-Hashfunktionen, von der auch ihr Name abgeleitet ist, besteht darin, daß aus den Hashwerten nicht auf die Eingaben geschlossen werden kann.

Während es bei Such- bzw. Sortierverfahren unumgänglich ist, von den Hashwerten auf die Eingaben zu schließen, sollen Einweg-Hashfunktionen genau dies unmöglich machen. Zusätzlich sollen Einweg-Hashfunktionen noch kollisionsfrei sein, d.h. zwei unterschiedlichen, sinnvollen Eingaben soll auf keinen Fall derselbe Hashwert zugeordnet werden.

Beispiel

Die Zuordnung von Wörtern zu Anfangsbuchstaben ist eine Hashfunktion(solange die Wörter nicht noch sortiert werden). Wörter mit unterschiedlichster Bedeutung und Länge werden in derselben Menge erfaßt.

Wahrscheinlich wird fast jeder diese einfache Hashfunktion schon angewandt haben, in seinem persönlichen Adreßbuch. Der endlichen Menge der Buchstaben des Alphabets können unendlich viele Namen und Adressen zugeordnet werden. Die Suche nach einer Person wird dadurch beschleunigt, daß anhand des Anfangsbuchstaben des Namens feststeht, wo nach dieser Person zu suchen ist. Die Suche in allen notierten Namen würde einen wesentlich höheren Aufwand erfordern.

digitaler Fingerabdruck

digitaler Fingerabdruck - (engl.) digital fingerprint

Ein digitaler Fingerabdruckeines elektronischen Dokumentsist die Ausgabe einer Einweg-Hashfunktion, die als Eingabe das Dokument erhalten hat. Der digitale Fingerabdruckist in der Regel kürzer, als das Dokument selbst. Er sollte weiterhin eindeutig sein, d.h. es sollte kein zweites, sinnvolles Dokument mit gleichem digitalen Fingerabdruck existieren. Dieser Idealfall ist nur schwer sicherzustellen.

Siehe auch: Digitale Signatur

digital fingerprint

digital fingerprint (engl.) - digitaler Fingerabdruck

SHA [*Secure Hash Algorithm*]

Secure Hash Algorithm (engl.) - sichere Hashfunktion

SHAist eine Entwicklung des NISTin Zusammenarbeit mit der NSA. Es handelt sich um eine kryptographische Hashfunktion, deren Anwendung speziell für regierungsamtlichen Einsatz in den USA empfohlen wird.

SHA erzeugt für die Eingabe mit einer Länge kleiner oder gleich 2^{64} Bit einen 160 Bit-Hashwert.

Sicherheit

Erfolgreiche Angriffe gegen SHAsind nicht bekannt.

Bedeutung

SHAwird zum Beispiel im DSA(Digital Signature Algorithm) verwendet.

MD4 [*Message Digest 4*]

MD4 ist eine Einweg-Hashfunktion und wurde von Ron Rivest entwickelt.

MD4 erzeugt in drei Runden 128-Bit-Hashwerte. Dabei kommen keine S-Boxen zum Einsatz. Da MD4 teilweise erfolgreich kryptanalysiert wurde, verbesserte Rivest MD4 zu MD5.

MD5 [*Message Digest 5*]

MD5ist eine Einweg-Hashfunktion, die Ron Rivest als Nachfolger von MD4entwickelt hat.

Arbeitsweise

MD5erzeugt in 4 Runden Hashwerte von 128 Bit Länge. Wie schon MD4, kommt MD5ohne S-Boxenaus.

Bedeutung

MD5wird z.B. im SNMP(Simple Network Management Protocol) und von PGPverwendet.

Sicherheit

MD5wurde bisher nicht erfolgreich attackiert. Bruce Schneier empfiehlt den Einsatz von MD5dennoch nicht [Schneier 1996], S. 503.

HAVAL

Bei HAVAL handelt es sich um eine Einweg-Hashfunktion. HAVAL wurde von Y. Zheng, J. Pieprzyk und J. Seberry aus MD5 entwickelt.

Arbeitsweise

HAVAL arbeitet mit Ausgabewerten variabler Länge und mit variabler Rundenanzahl.

Snefru

Snefru ist eine von Ralph Merkle vorgeschlagene Einweg-Hashfunktion.

Snefru erzeugt unter Verwendung von S-Boxen in mehreren Runden 128- bzw. 256-Bit-Hashwerte. Ralph Merkle empfiehlt zur Sicherheit 8 Runden.

Da Snefru langsamer als MD4 ist, hat er nicht so große Verbreitung gefunden.

Schlüsselraum

Schlüsselraum - (engl.) key space

Der Schlüsselraumist die Menge aller Schlüssel, mit denen ein Verschlüsselungsverfahrenarbeitet, d.h. alle Schlüssel für die Verschlüsselungund alle Schlüssel für die Entschlüsselung. Sichere Verschlüsselungsverfahren haben einen Schlüsselraum, der so groß ist, daß er nicht durch exhaustive Suche mit Erfolg durchsucht werden kann. Die Schlüssel im Schlüsselraum sollten außerdem so gewählt sein, daß sie immun gegen Wörterbuchangriffe sind.

MDC

(1) ***[Modification Detection Code]***

(2) ***[Message Digest Cipher]***

(3) *[Manipulation Detection Code]*

---

(1)Modification Detection Code (engl.) - Code zur Feststellung von Veränderungen

(2) Message Digest Cipher (engl.) - Verschlüsselung der Nachrichtenzusammenfassung

(3) Manipulation Detection Code (engl.) - Code zur Manipulationsfeststellung

---

(1) Funktionen, die MDCsliefern, sind kollisionsfreie (kollisionsresistente) Einweg-Hashfunktionen. Sie arbeiten im Gegensatz zu MACsohne Schlüssel.

(3) *Manipulation Detection Code* ist ein seltener gebrauchtes Synonym für *Modification Detection Code*.

---

(2) MDC (Message Digest Cipher; P. Gutmann, 1993) verwendet eine beliebige Einweghashfunktion zur Verschlüsselung im CFB-Modus. Als Schlüssel kommt die Eingabe der Hashfunktion zum Einsatz; der vorangegangene Hashzustand bildet den Klartextblock.

Sicherheit

Die Sicherheit dieser Verschlüsselung hängt unmittelbar von der Sicherheit der Hashfunktion ab. Schneier [Schneier 1996], S.408, 409, weist darauf hin, daßHashfunktionen nicht zu diesem Zwecke entworfen werden und sieht darin einen möglichen Angriffspunkt für einen chosen-plaintext-attack.

Patente

MDCist nicht patentiert.

Siehe auch:message digest (MD), message authentication code (MAC), digital fingerprint, digital signature, MDC-2, MDC-

[4](#)

RIPE-MD [*RIPE Message Digest*]

RIPE-MDist eine kryptographische Hashfunktion, die im Rahmen des RIPE-Projektes der Europäischen Union aus MD4entwickelt wurde.

elektronisches Dokument

elektronisches Dokument - (engl.) electronic document

Ein elektronisches Dokument ist ...

CFB [*Cipher Feedback*]

Cipher Feedback (engl.) - Verschlüsselung mit Rückkopplung

CFB ist ein Verschlüsselungsmodus von Blockchiffrierungen. Damit können Daten beliebiger Länge, auch kleiner als ein Block, verschlüsselt werden. Ausgehend von einem Initialisierungsvektor (IV) wird das erste Datum per XOR verschlüsselt und das Resultat ausgegeben, sowie rückgekoppelt. Auf diese Art und Weise hängt der Geheimtext vom kompletten, vorher bearbeiteten Klartext ab.

chosen-plaintext attack

chosen-plaintext attack (engl.) - Klartextangriff mit gewähltem Klartext

Siehe auch: adaptive chosen-plaintext attack, plaintext attack

MDC-2 [*Modification Detection Code 2*]

modification detection code (engl.) - Code zur Feststellung von Veränderungen

MDC-2 ist eine kryptographische Einweghashfunktion.

Sicherheit

In Abhängigkeit vom verwendeten Verschlüsselungsalgorithmus ist MDC-2 mehr oder weniger sicher.

Patente

MDC-2 ist gemeinsam mit MDC-4 in den USA unter der Nummer 4.908.861 patentiert (13. März 1990). Patentinhaber sind: *B.O. Brachtl*, *D. Coppersmith*, *M.M. Hyden*, *S.M. Matyas*, *C.H. Meyer*, *J. Oseas*, *S. Pilpel* und *M. Schilling*.

Siehe auch: modification detection code (MDC), MDC-4

MDC-4 [*Modification Detection Code 4*]

modification detection code (engl.) - Code zur Feststellung von Veränderungen

MDC-4ist eine kryptographische Einweghashfunktion.

Sicherheit

In Abhängigkeit vom verwendeten Verschlüsselungsalgorithmus ist MDC-4mehr oder weniger sicher.

Patente

MDC-4ist gemeinsam mit MDC-2 in den USA unter der Nummer 4.908.861 patentiert (13. März 1990). Patentinhaber sind: *B.O. Brachtl, D. Coppersmith, M.M. Hyden, S.M. Matyas, C.H. Meyer, J. Oseas, S. Pilpel*und *M. Schilling*.

Siehe auch:modification detection code (MDC), manipulation detection code (MDC), MDC-2

S-Box

S-Boxen sind elementare Bestandteile von Feistel-Netzwerken. Es handelt sich dabei um Funktionen, die eine m-n Abbildung realisieren, d.h. *m* Eingabe-Bits werden auf *n* Ausgabe-Bits abgebildet. Mit S-Boxen werden nichtlineare Abbildungen implementiert.

Zu unterscheiden sind im wesentlichen zwei Varianten:

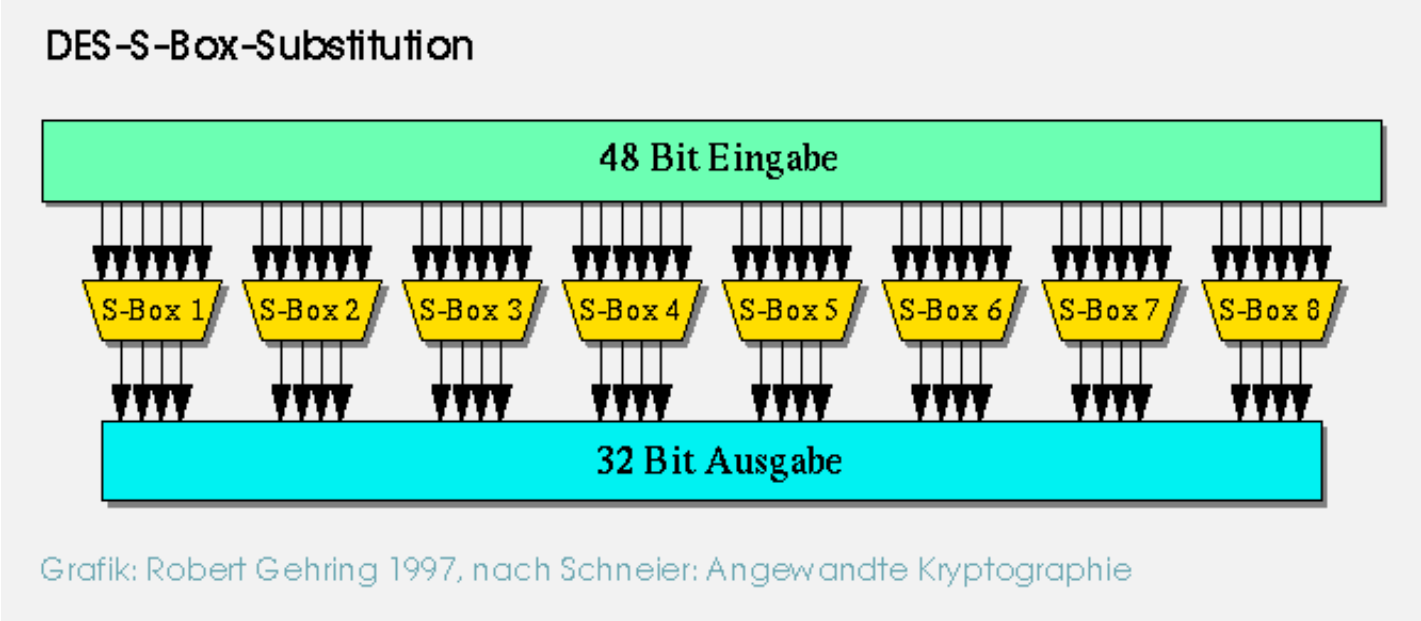
- zufällige S-Boxen
- S-Boxen mit mathematischen Verfahren

Die Sicherheit von Verschlüsselungsalgorithmen, die auf Feistel-Netzwerken basieren, hängt in der Hauptsache von den gewählten S-Boxen ab.

Bruce Schneier empfiehlt (in [Schneier 1996], S.405):

> "*..., ich persönlich meine jedoch, daß S-Boxen so groß wie möglich, zufällig und schlüsselabhängig sein sollten.*"

DES verwendet S-Boxen entsprechend folgendem Schema:



Eine einzelne S-Box wird dabei durch eine Tabelle repräsentiert. Für S-Box 4 sieht diese so aus:

S-Box Nummer 4 des DES

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

Die Abbildung von Eingangsbits auf Ausgangsbits geschieht folgendermaßen:

- Bit 0 und Bit 5 bilden adressieren die Zeile (0-3) der S-Box
- Bit 1-4 adressiert die Spalte (0 bis 15)
- wenn Box 4 die Eingabe 101011 bekommt, so wird der Wert in Spalte 0101, d.h. 5 und in Zeile 11, d.h. 3 ausgewählt; der Ausgangswert ist demnach 1

SNMP [*Simple Network Management Protocol*]

Simple Network Management Protocol (engl.) - Protokoll zur einfachen Netzwerkverwaltung

Das SNMPwurde von der IETFentwickelt und 1987 vorgestellt. Es enthält Spezifikationen für Protokolleund Datenformate, mit deren Hilfe die Verwaltung von Netzwerken vereinfacht wird.

RIPE [*RACE Integrity Primitives Evaluation*]

RIPEist ein Projekt, das im Rahmen des RACE-Projektes der Europäischen Union angesiedelt ist.

Von RIPE wurde u.a. RIPE-MD, eine kryptographische Hashfunktion, entwickelt.

...

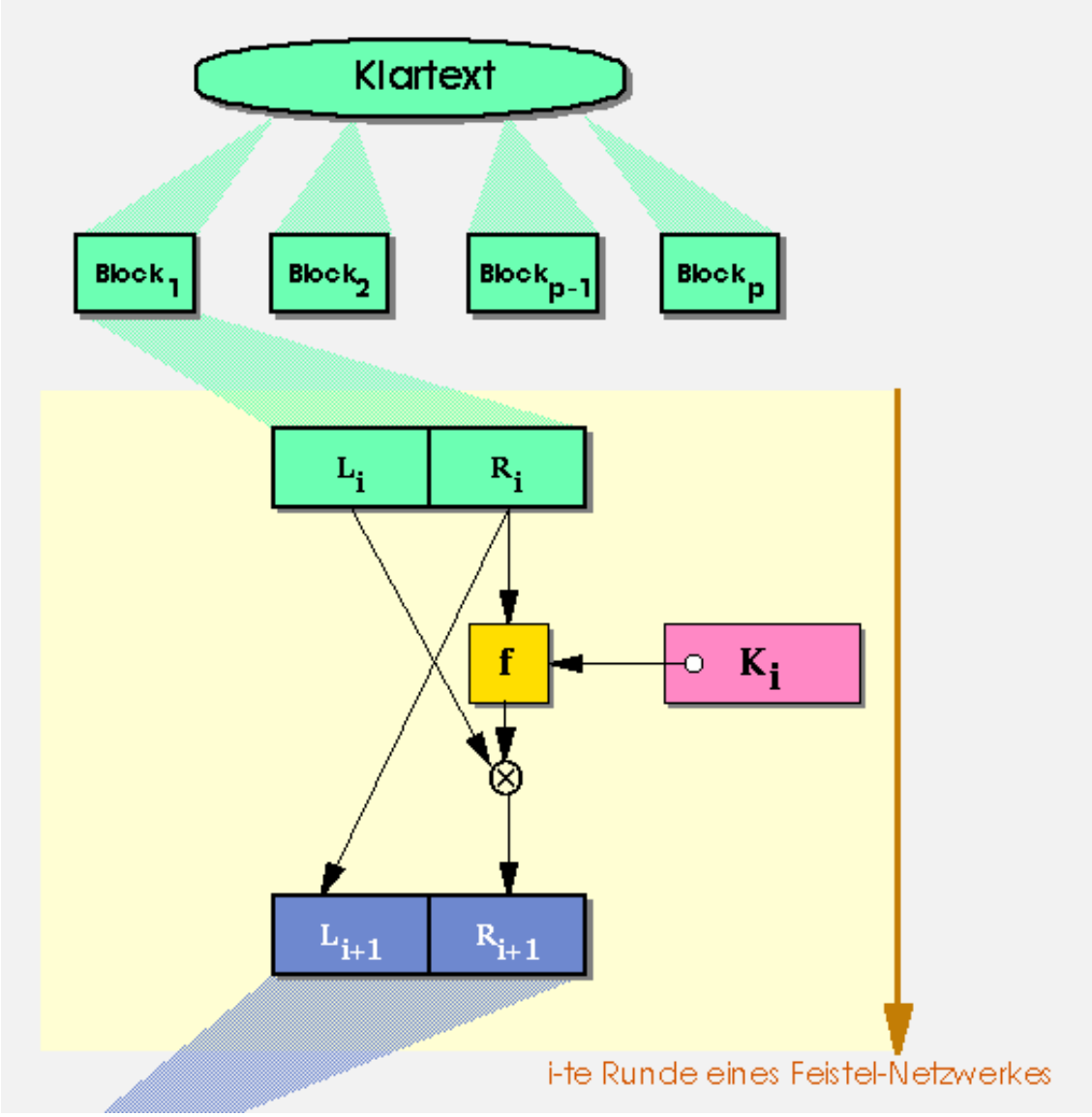
Feistel-Netzwerk

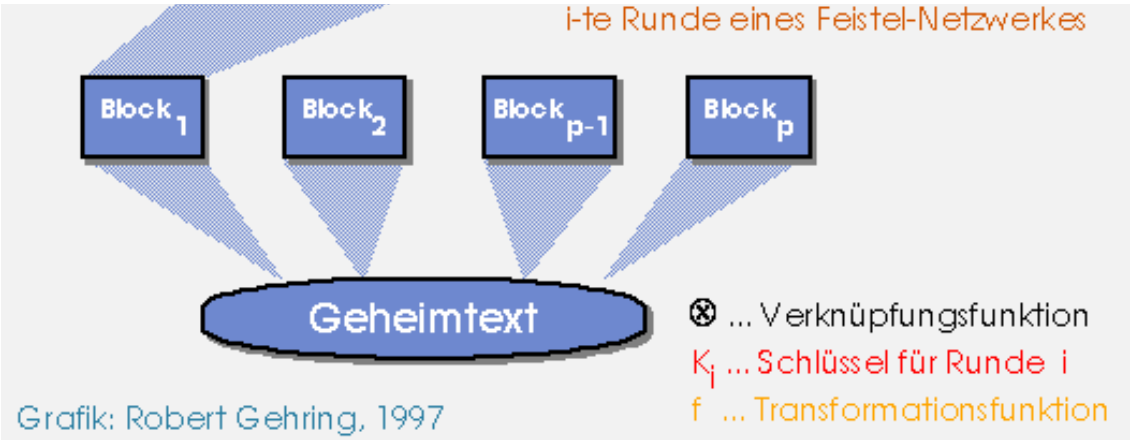
Das Feistel-Netzwerk geht auf den IBM-Entwickler Horst Feistel zurück und wurde in den 70'er Jahren im Rahmen des Projektes `Lucifer' (aus dem später das DES-Verfahren hervorging) entwickelt.

Arbeitsweise

Zuerst wird der Klartext in Blöcke zerlegt. Jeder Block wird dann in zwei Teilblöcke zerlegt, in mehreren Runden verschlüsselt und anschließend wieder zusammengesetzt. Für jede Runde wird dabei ein neuer Schlüssel generiert. Ausgangspunkt für die Generierung ist der geheime Schlüssel *S*. Die Zusammensetzung aller Geheimtextblöcke ergibt den Geheimtext (Chiffre).

Grafisch läßt sich ein Feistel-Netzwerk so darstellen:





Der gelbe Bereich stellt die i-te Runde eines Feistel-Netzwerkes für die Verschlüsselung eines Blockes aus dem Klartext dar. Für eine effektive Implementierung wird für die Verknüpfungsfunktion in der Regel die XOR-Funktion gewählt, die sich leicht in Hardware realisieren läßt. Die Transformationsfunktion f bildet in Abhängigkeit vom Schlüssel für die jeweilige Runde einen Halbblock auf einen Halbblock ab.

$$L_{i+1} = R_i$$
$$R_{i+1} = L_i \otimes f_{s,i}(R_i)$$

Bei der richtigen Wahl von f und K genügen schon wenige Runden (5 Runden bei DES), um jedes Bit aus dem Klartextblock von jedem Bit des Schlüssels abhängig zu machen. Diesen Effekt nennt man `*Lawineneffekt*'. Er bewirkt, daß kein Bit des Klartextes oder des Schlüssels ohne gravierende Änderungen des Geheimtextes variiert werden kann.

Die hervorragende Eigenschaft eines Feistel-Netzwerkes ist dabei, daß Verschlüsselung und Entschlüsselung nicht getrennt implementiert werden müssen, da die Verschlüsselung mit f durch Vertauschung der Rundenschlüssel umkehrbar ist.

Einsatz

Die bekanntesten Verschlüsselungsverfahren, die Feistel-Netzwerke verwenden sind:

- DES
- FEAL
- Blowfish
- LUCIFER
- Khufu
- Khafre
- LOKI
- GOST
- CAST

Literatur:

[Wobst 1997 (I)], [Schneier 1996], [Bauer 1994]

DES [*Data Encryption Standard*]

Geschichte

Der DES geht auf das Projekt `Lucifer' der IBM zurück. IBM reichte diesen Algorithmus als Vorschlag auf eine Ausschreibung der NBS hin ein. In dieser Ausschreibung wurde nach einer Verschlüsselungstechnologie gesucht, die folgende Kriterien erfüllt (nach [Schneier 1996], S.310):

- hoher Grad an Sicherheit
- vollständige Spezifikation
- leicht nachvollziehbar
- Sicherheit darf nur vom Schlüssel abhängen
- Algorithmus muß veröffentlichbar sein
- Algorithmus muß anpaßbar sein
- leichte, billige und effiziente Hardware-Implementierbarkeit
- effiziente Benutzung
- Validierbarkeit muß gegeben sein
- Algorithmus muß exportierbar sein

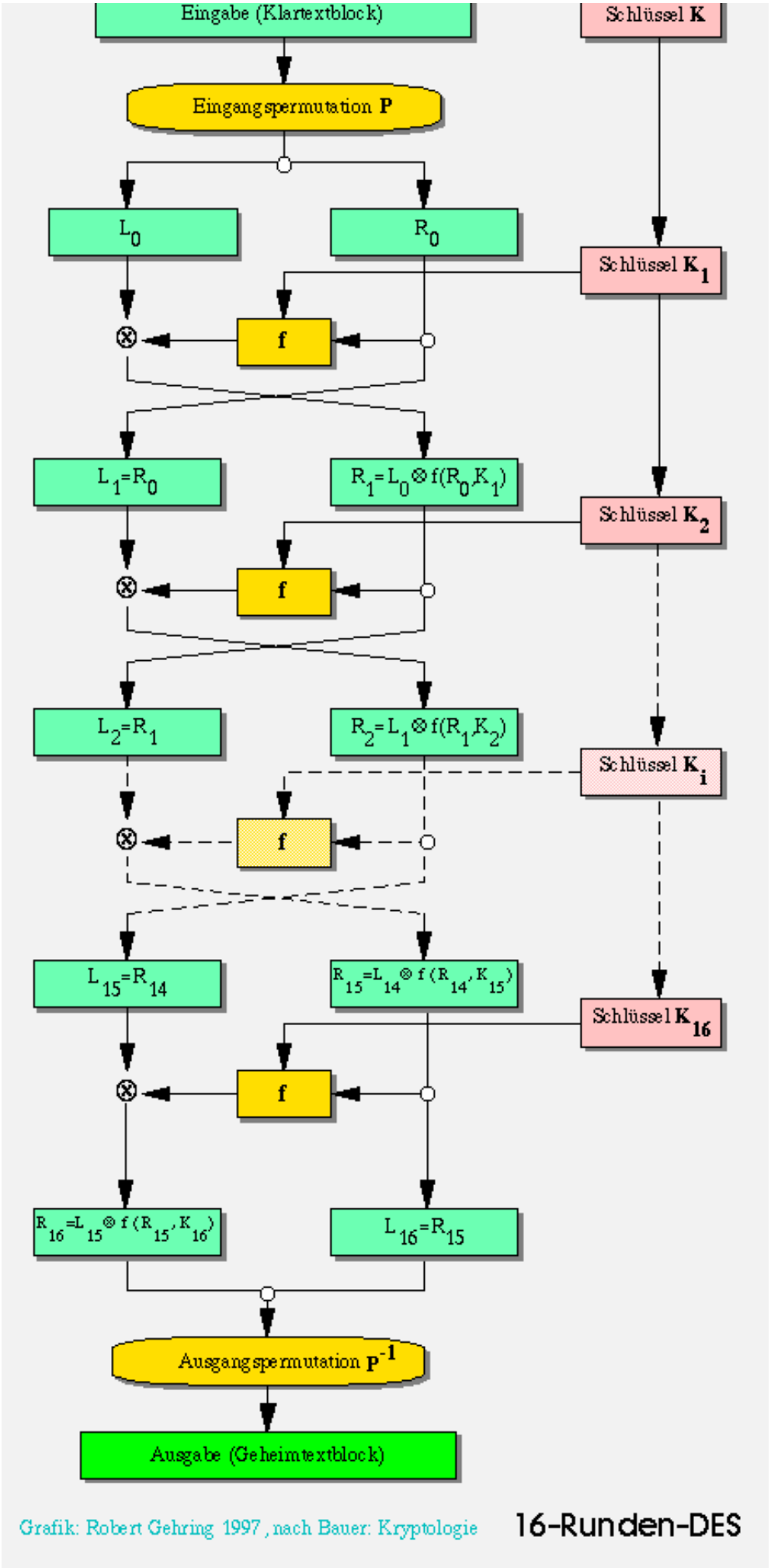
Ziel der Ausschreibung war es, eine Verschlüsselungstechnologie für (regierungsamtliche) Kommunikation und Dokumente zu standardisieren, um die Kompatibilität elektronischer Kommunikation bei gleichzeitiger Geheimhaltung sicherzustellen. Man beachte dabei, daß eine Software-Implementierung nicht zu den Ausschreibungskriterien gehörte!

Nachdem der Vorschlag von IBM, ein Algorithmus der iterativ mit Feistel-Netzwerken und einem 128-Bit-Schlüssel (inklusive Parität) arbeitet, bei der NBS vorlag, zog diese die NSA zu Rate. Wie groß der Einfluß der NSA auf die endgültige Gestaltung des Algorithmus' war, ist unbekannt. Bekannt ist nur, daß DES mit einem 56-Bit-Schlüssel und nicht, wie vorgeschlagen, mit einem 128-Bit-Schlüssel arbeitet. Die damit verbundene Verkleinerung des Schlüsselraumes erleichtert einen Brute-Force-Angriff erhblich.

Am 17. März 1975 wurde die detaillierte DES-Spezifikation im `Federal Register' der USA veröffentlicht, wobei gleichzeitig um Stellungnahme ersucht wurde. Im Resultat der Auswertung der Stellungnahmen und zweier abgehaltener Konferenzen wurde DES (mit 16 Runden) am 23. November 1976 als Standard anerkannt und am 15. Januar 1977 als FIPS PUB 46 veröffentlicht. Das ANSI akzeptierte DES ebenfalls als Standard (ANSI X3.92), unter dem Namen DEA (Data Encryption Algorithm). Für den Export wurde die Schlüssellänge auf 40 Bit beschränkt.

Arbeitsweise

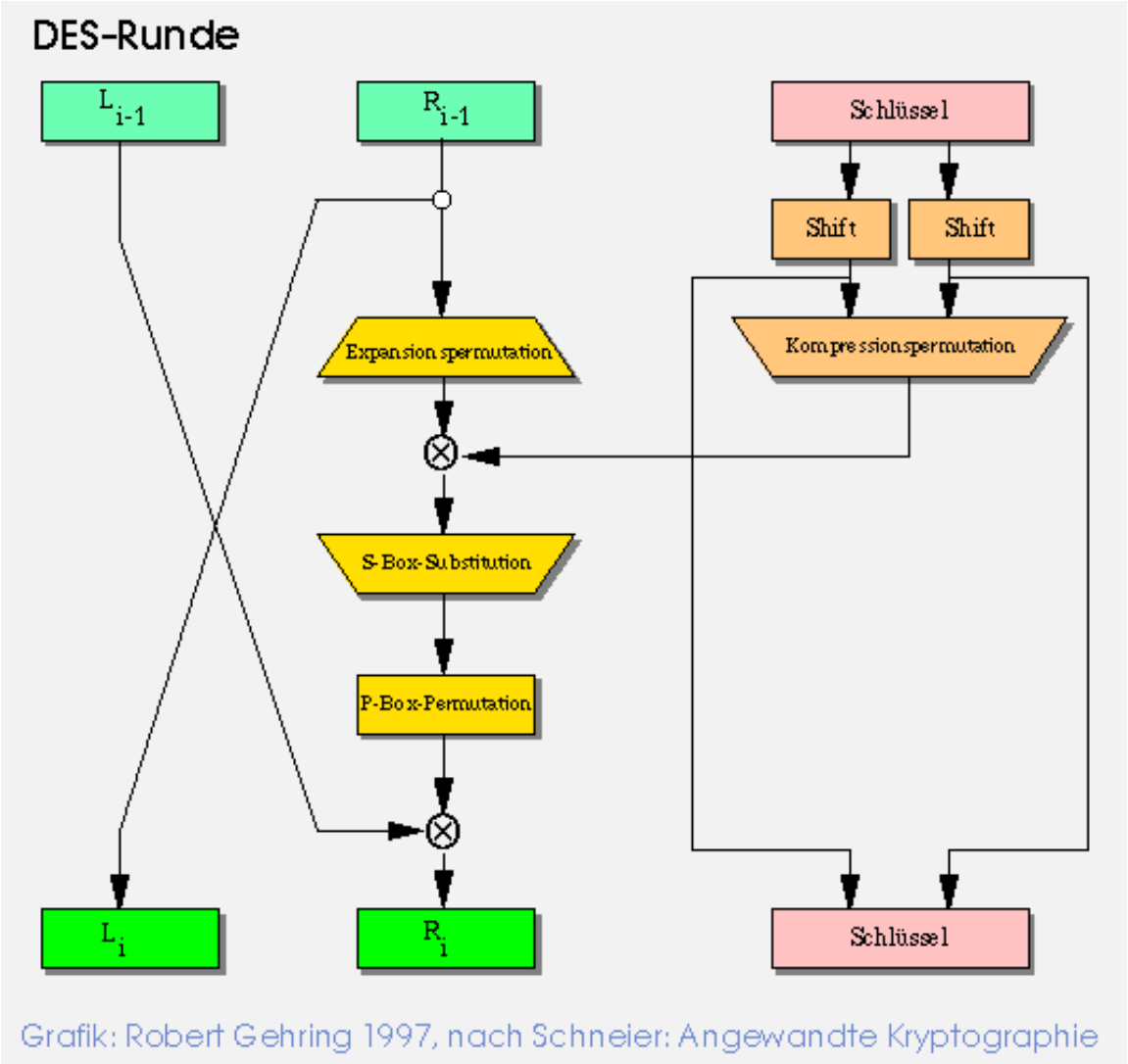
DES ist ein symmetrisches Verschlüsselungsverfahren und arbeitet mit Feistel-Netzwerken. Grafisch läßt sich DES folgendermaßen darstellen:


Eingabe (Klartextblock)
Schlüssel K
Eingangspermutation P
L0
R0
Schlüssel K1
f
L1=R0
R1=L0⊗f(R0,K1)
Schlüssel K2
f
L2=R1
R2=L1⊗f(R1,K2)
Schlüssel Ki
f
L15=R14
R15=L14⊗f(R14,K15)
Schlüssel K16
f
R16=L15⊗f(R15,K16)
L16=R15
Ausgangspermutation P-1
Ausgabe (Geheimtextblock)
Grafik: Robert Gehring 1997, nach Bauer: Kryptologie
16-Runden-DES

Grafik: Robert Gehring 1997, nach Bauer: Kryptologie 16-Runden-DES

Der Schlüssel K besteht aus 64 Bit (8 Byte), wobei 8 Bit für die Parität reserviert sind. Die bei Feistel-Netzwerken bedeutsame Transformationsfunktion f basiert auf sogenannten S-Boxen, an deren Gestaltung die NSA gearbeitet hat. Möglicherweise darin enthaltene Falltüren waren und sind ein wesentlicher Kritikpunkt an DES. Die Bedeutung der Eingangs- und der Ausgangspermutation ist in der Fachliteratur nicht genau erklärt und wird auf Charakteristika der damals verfügbaren Hardware zurückgeführt.

Eine einzelne Runde stellt sich folgendermaßen dar:



Kryptographische Sicherheit

DES muß alle fünf Jahre erneut zertifiziert und als Standard bestätigt werden. Im nächsten Jahr (1998) steht eine erneute Untersuchung und ggf. Bestätigung bevor.

Bis heute ist kein wirksamer Angriff auf den 16-Runden-DES bekannt. Dabei liegt die Betonung auf bekannt. Nahezu alle Experten sich einig, daß die NSA in der Lage ist, jede DES-Verschlüsselung in wenigen Stunden zu brechen. Der Kostenaufwand für einen Computer mit der notwendigen Rechenleistung wird auf etwa 1 Million US-$ geschätzt. In Anbetracht der Einsatzbreite von DES kann davon ausgegangen werden, daß dies kein Hindernis ist. Von Michael Wiener stamm der Entwurf eines 1 Million US-$ teuren Computers, der nur etwa 3,5 Stunden für einen `Brute-Force-Angriff' benötigt.

Im Zusammenhang mit der wachsenden Anzahl ungeklärter Betrugsfälle mit EC-Karten kann ebenfalls vermutet werden, daß der Algorithmus geknackt wurde. So heißt es in einer SPIEGEL-Meldung:

> "*Es sei offenbar gelungen, den der PIN-Berechnung zugrundeliegenden DES-Algorithmus zu entschlüsseln.*" [SPIEGEL 36/1997], S. 104

Bedeutung

DES ist der meistbenutzte Verschlüsselungsalgorithmus überhaupt. Die Kommunikation im Bankwesen wird mit DES verschlüsselt, ebenso die Daten der EC-Karte. Von letzterer wurden allein in Deutschland 40 Millionen ausgegeben.

IETF [*Internet Engineering Task Force*]

Internet Engineering Task Force (engl.) - ??? [*Anm.: Mir fällt keine `schöne' Übersetzung ein.*]

Die IETF ist eine Arbeitsgruppe des IAB (Internet Activities Board). Sie ist zuständig für Standardisierungsvorschläge für's Internet. Die andere Arbeitsgruppe bei IAB ist die IRTF (Internet Research Task Force).

IV [Initialisierungsvektor]

Initialisierungsvektor - (engl.) initial vector

Bei Verschlüsselungsverfahren, die einen Startwert benötigen (z.B. weil sie mit Rückkopplung arbeiten, wie im CBC- oder CFB-Modus), wird ein Initialisierungsvektor nach bestimmten Regeln mit dem Startwert gefüllt.

XOR [*Exclusive Or*]

exclusive Or (engl.) - exklusives Oder, Exklusiv-Oder, ExOR

XORist eine elementare logische Operation. Sprachlich läßt sie sich mit `*Entweder, oder*' beschreiben. Die mathematische Abbildung sieht folgendermaßen aus:

Wert	FALSE (0)	TRUE (1)
FALSE (0)	FALSE (0)	TRUE (1)
TRUE (1)	TRUE (1)	FALSE (0)

XORwird als eine elementare Verschlüsselungsoperation eingesetzt. Kommt sie in geeigneter Kombination mit anderen Operationen vor, ist sie sehr nützlich (siehe z.B. IDEA). Oft wird sie jedoch in simpelster Weise eingesetzt, indem der Klartext per XORmit dem Schlüsselverknüpft wird. Die Entschlüsselungerfolgt durch erneute XOR-Verknüpfung mit dem Schlüssel, denn es gilt: (a XORb) XORb = a. Eine solche ``Verschlüsselung'' ist für alle möglichen Arten von Angriffenbestens geeignet.

adaptive chosen-plaintext attack

adaptive chosen-plaintext attack (engl.) - Klartextangriff mit Anpassung des gewählten Klartextes

Siehe auch: chosen-plaintext attack, plaintext attack

kryptographische Einweg-Hashfunktion

kryptographische Einweg-Hashfunktion - (engl.) cryptographic one-way hash function

Kryptographische Einweg-Hashfunktionist ein Synonym für *kryptographische Hashfunktion*.

MEMEX

MEMEXist ein Programm, das mittels künstlicher Intelligenz automatisch elektronisch übermittelte Kommunikation auf für die NSAinteressante Inhalte hin untersucht. MEMEXwird im ECHELON-System eingesetzt, um die Kommunikation weltweit zu überwachen.

NSA [*National Security Agency*]

Die `National Security Agency' ist

> "*das offizielle kryptographische Organ Amerikas*"
>
> (Zitat: Whitfield Diffie im Vorwort zu [Schneier 1996]).

Genauer gesagt handelt es sich um den geheimsten aller US-amerikanischen Geheimdienste (von denen man weiß, daß sie existieren). Mancherort liest man die Bezeichnung "Supergeheimdienst". Die NSA wurde von Harry Truman im Jahre 1952 gegründet, ihre Existenz wurde aber lange Jahre von der Regierung bestritten.

Die NSA ist für alles zuständig, was mit geheimer Informationssicherung und -beschaffung, sprich Kryptographie und Kryptanalyse zu tun hat. Zu diesem Zwecke beschäftigt sie -gerüchteweise- ca. 20.000-40.000 Mathematiker. Diese arbeiten an der Entwicklung neuer Verschlüsselungstechniologie und an der `Brechung' von Verschlüsselungstechnologie anderer Länder (Firmen? Institutionen?).

Das Budget der NSA beträgt vermutlich ca. 10 Mrd. US-$ ([Wobst 1997 (I)], S. 329), mehr als der CIA ("Central Intelligence Agency") zur Verfügung steht. Die Ergebnisse der Tätigkeiten der NSA werden in der Regel nicht veröffentlicht. Experten wie z.B. Bruce Schneier gehen jedoch davon aus, daß die NSA in vielerlei Hinsicht kryptographische Erkenntnisse gewonnen hat, die über das hinausgehen, was in der zivilen kryptographischen Forschung erreicht wurde ([Schneier 1996], S.677).

Das deutsche Gegenstück zur NSA war das BSI (Bundesamt für Sicherheit in der Informationstechnik) - bevor es (per Gesetz) aufhörte, eine Dienststelle des BND ("Bundesnachrichtendienst") zu sein. Der Aufwand, den die NSA im Rahmen ihrer Tätigkeit treibt, war und ist allerdings deutlich größer, als der beim BSI. Zumindest stellt sich dies nach den öffentlich zugänglichen Informationen so dar.

Die NSA hat großen Einfluß auf wichtige Institutionen in den USA, z.B. das NIST (National Institute of Standards and Technologie). Wenn auf dem Gebiet der Verschlüsselungstechnologie in den USA offizielle Empfehlungen von solchen Institutionen ausgesprochen werden, sollte man deshalb schon mißtrauisch werden. An der Entwicklung des DES-Verfahrens, das vom NIST als Standard definiert wurde, war die NSA beteiligt. Wie weit, ist allerdings unbekannt.

Ein Resultat von NSA-Aktivitäten ist zum Beispiel das Scheitern der `Clipper-Chip'-Initiative der US-Regierung (1994).

Image

Die Vorstellungen der US-Öffentlichkeit von der NSA werden z.B. dadurch illustriert, daß die aus dem Nichts auftauchenden Gestalten in den zur Zeit sehr beliebten `Mystery'-Serien (z.B. "The X-Files") regelmäßig behaupten, daß sie für die NSA arbeiten.

Auch im Film "Sneakers" müssen ehemalige NSA-Mitarbeiter als Bösewichter herhalten. Bei diesem Film hat

übrigens Professor Leonard Adleman als Berater fungiert. (Adleman ist das `A' in RSA.)

Internet

Die NSA unterhält einen Web-Server (http://www.nsa.gov:8080).

BSI [*Bundesamt für Sicherheit in der Informationstechnik*]

Das BSIwar einmal -als Zentralstelle für Sicherheit in der Informationstechnik (ZSI)- eine Zweigstelle des Bundesnachrichtendienstes (BND). Mit dem BSI-Errichtungsgesetz wurde es zum 1.1.1991 in ein staatliches Institut umgewandelt. Aus der BND-Zeit übernommen wurde die Aufgabe, die

> "*Dienste der Inneren Sicherheit (Polizei, Staatsanwaltschaften und Verfassungsschutzämter) zu unterstützen*(§3 Abs. 1 Nr. 6 BSI-Errichtungsgesetz)" ([Bizer 1997]).

Heutzutage ist das BSIein staatliches Institut, dessen Aufgabenbereich sich wesentlich auf die Überprüfung von Sicherheitsarchitekturen und -systemen erstreckt. An der Erarbeitung des Signaturgesetzes (SigG) war das BSI maßgeblich beteiligt.

Internet:http://www.bsi.bund.de

BND [*Bundesnachrichtendienst*]

Bundesnachrichtendienst - (engl.) Federal Intelligence Service

Der BND ist der größte Geheimdienst der Bundesrepublik Deutschland.

NIST [*National Institute of Standards and Technology*]

National Institute of Standards and Technology (engl.) - Nationales Institut für Standards und Technologie

Das NIST (ehemals NBS), Gaithersburg, Maryland, ist in den USA auf Bundesebene zuständig für die technische Standardisierung von Sicherheitstechnologie und gibt die sogenannten FIPS-Standards heraus. Es arbeitet dem ANSI zu.

Beziehung NIST - NSA

Es gibt ein MOU (Memorandum of Understanding) zwischen dem NIST und der NSA, die Zusammenarbeit auf dem Gebiet der Kryptographie betreffend. Wegen dieses MOU ist das NIST heftig angegriffen worden, da Kritiker der Meinung sind, daß der NSA zuviel Einfluß eingeräumt werde.

So ist zum Beispiel eine Zusammenarbeit bei der Entwicklung von:

- security protocol standards
- digital signature standards
- key management standards
- encryption algorithm standards

vorgesehen. Wie groß der Einfluß der NSA tatsächlich ist, bleibt geheim.

Siehe auch: ANSI

Clipper chip

Die Clipper chip-Initiative (Clipper-Initiative) war der erste großangelegte Versuch der US-Regierung, Verschlüsselungzu reglementieren. Sie wurde nach mehreren Jahren der Vorbereitung 1993 gestartet und endete erfolglos. Die Wirtschaft zeigte ein deutliches Desinteresse an -staatlich sanktionierter- abhörbarer Kommunikation in der vorgesehenen Form des key escrow, d.h. der Verschlüsselung mit Schlüsselhinterlegung. Allerdings brechen die Fronten langsam auf, seit es einen neuen Namen für das Projekt gibt: Key Recovery.

Der Clipper-Chip

Der Clipper-Chipdient der Sprachverschlüsselung mit Schlüsselhinterlegung. Er wurde als `tamper resistant device' auf der Grundlage des SKIPJACK-Algorithmus' entwickelt.

Siehe auch: Capstone chip

Internet:http://www.cpsr.org/dox/clipper/clipper.html

ECHELON

ECHELONist ein von der NSAbetriebenes System zum automatischen Abhören des elektronisch vermittelten Kommunikationsverkehrs (Telefon, eMail, Telex) in der Welt. Mittels künstlicher Intelligenz (MEMEX-System) werden die belauschten Nachrichten automatisch auf interessierende Inhalte hin untersucht. Die Resultate werden dann via Satellit in die USA wietergeleitet. ECHELONist integraler Bestandteil des UKUSA-Systems und wurde speziell zum Abhören ziviler Kommunikation entwickelt.

Die Existenz des Systems wurde in einem internen Bericht an das Europäische Parlament (PE 166 499) offiziell bestätigt. Der Bericht wurde von Steve Wright für *Scientific and Technological Options Assessment* (STOA) angefertigt. Seine Existenz wurde von "The Daily Telegraph" am 16. Dezember 1997 in der Internetausgabe 936 bekanntgegeben. Inzwischen (5. Februar 1998) steht er auch der Redaktion von "Telepolis" zur Verfügung, die ihn in Auszügen veröffentlicht.

UKUSA

UKUSAist ... ein von der NSAbetriebenes Spionagenetz ??? Bestandteil des UKUSA-Systems ist ECHELON, mit dem automatisch der weltweite elektronische Kommunikationsverkehr abgehört wird.

MPQS [*Multiple Polynomial Quadratic Sieve*][*Multiples Polynomisches Quadratisches Sieb*]

Das MPQS stellt eine Weiterentwicklung des Polynomischen Quadratischen Siebes (PQS) und jenes wiederum eine Weiterentwicklung des Quadratischen Siebes (QS) dar. Alle Verfahren dienen der Faktorisierung.

abhören

abhören - (engl.) tap

Mit abhören bezeichnet man das Belauschen von (Telefon-) Gesprächen von Personen ohne deren Einverständnis. Man unterscheidet legales und illegales Abhören durch Staatsorgane und durch Personen, die nicht bei Staatsorganen angestellt sind.

Gesetzliche Regelungen

Es gibt verschiedene Gesetze, die das Abhören durch staatliche Organe regeln:

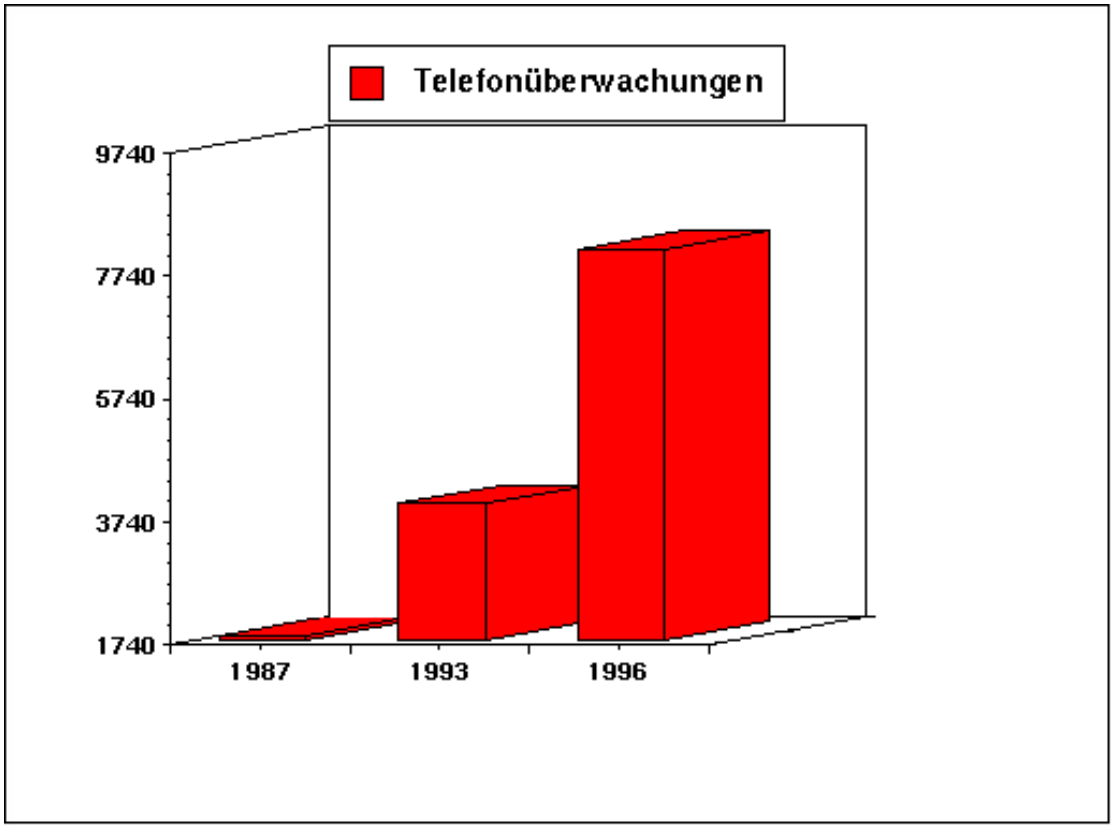
Gesetzliche Regelungen zum Abhören

Grafik: Robert Gehring, 1997

Abhörmaßnahmen, die nicht durch staatliche Organe vorgenommen werden sind illegal. Abhörmaßnahmen durch staatliche Organe sind nur unter bestimmten Umständen zulässig, somit legal. Bisher stehen sie unter einem richterlichen Vorbehalt. Im Entwurf zum Begleitgesetz zum neuen Telekommunikationsgesetz (TKG) wird dieser richterliche Vorbehalt teilweise abgeschafft, indem *abgeschlossene Telekommunikation* nicht mehr darunter fallen soll.

Abhörstatistik

Auf eine Anfrage der Grünen im Bundestag hin (1997) gab die Bundesregierung die Zahlen für die Abhöraktionen mit 6183 für Telefonanschlüsse, 1911 für Mobiltelefonanschlüsse und 18 für Funkrufanschlüsse an. Sucht man die wenigen veröffentlichten Zahlen zusammen, ergibt sich ungefähr folgendes Bild:



Die einzelnen Zahlen sind mit Vorsicht zu genießen. Die Tendenz dürfte aber relativ genau wiedergegeben werden.

Abhörgesetz

Abhörgesetz - (engl.) tap law

Abhörgesetz ist die umgangssprachliche Bezeichnung für das G-10-Gesetz (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimisses).

Siehe auch: abhören, Wanze

Alice

Alice ist die Kommunikationspartnerin von Bob. Sie bekommt häufig von diesem geheime Mitteilungen zugeschickt, die verschlüsselt sind. Alice und Bob sind raffiniert und verwenden jedes erdenkliche Verschlüsselungsverfahren. Wer Bücher über Kryptographie/Kryptologie liest, wird früher oder später über Alice und Bob stolpern.

allgemeines Zahlkörpersieb

allgemeines Zahlkörpersieb - (engl.) General Number Field Sieve (GNFS)

Das allgemeine Zahlkörpersieb ist ein Verfahren zur Faktorisierung und wurde aus dem Zahlkörpersieb entwickelt.

ANSI [*American National Standards Institute*]

Das ANSI hieß früher `American Standards Association' (ASA) und erfüllt Standardisierungsaufgaben, die in Deutschland z. T. durch das DIN erfüllt werden.

Siehe auch: NIST, NSA

ARPA [*Advanced Research Projects Agency*]

Advanced Research Projects Agency (engl.) - Agentur für Weiterführende Forschungsprojekte

Von der DARPA (Defense Advanced Research Projects Agency), einer US-amerikanischen Regierungsbehörde, wurde ab 1973 unter der Leitung von Dr. Robert Kahn das Internet - ursprünglich für militärische Zwecke unter dem Namen ARPAnet - entwickelt. Der Name wechselt mehrfach zwischen DARPA und ARPA, je nachdem, wofür die Finanzmittel vorwiegend zur Verfügung standen, für's Militär oder für ein ziviles Netz.

ARPAnet, ARPANET

ARPAnet (engl.) - Advanced Research Projects Agency Network

Das ARPAnet ist der Vorläufer des Internet, den die ARPA (DARPA) ab Ende der 60'er Jahre zu entwickeln begann.

Ziel der Entwicklung war eine Netzwerkstruktur, die sichere Informationsübertragungen über große Entfernungen auch bei Ausfall einzelner Teile des Netwerkes gestattete. Damit sollte die militärische Informationsübertragung auch im Falle eines Atomkrieges ermöglich werden.

Unter den ersten Teilnehmern am ARPAnet waren u.a.:

- die University of California, Los Angeles
- die University of California, Santa Barbara.

asymmetric cryptosystem

asymmetric cryptosystem (engl.) - asymmetrisches Verschlüsselungssystem, asymmetrisches Verschlüsselungsverfahren

asymmetric encryption

asymmetric encryption (engl.) - asymmetrische Verschlüsselung

asymmetric encryption algorithm

asymmetric encryption algorithm (engl.) - asymmetrischer Verschlüsselungsalgorithmus, asymmetrisches Verschlüsselungsverfahren

Siehe auch: symmetric encryption algorithm

asymmetric encryption scheme

asymmetric encryption scheme (engl.) - asymmetrisches Verschlüsselungsverfahren

Siehe auch: symmetrisches Verschlüsselungsverfahren

Glossar Digitale Signaturen

asymmetrischer Verschlüsselungsalgorithmus

asymmetrischer Verschlüsselungsalgorithmus - (engl.) asymmetric encryption algorithm, asymmetric encryption scheme

Asymmetrische Verschlüsselungsalgorithmen arbeiten mit unterschiedlichen Schlüsseln für Verschlüsselung und Entschlüsselung, mit Schlüsselpaaren.

Es ist bei asymmetrischen Verschlüsselungsverfahren nicht möglich, eine Nachricht, die mit einem Schlüssel des Paares verschlüsselt wurde, mit demselben Schlüssel wieder zu entschlüsseln. Zur Entschlüsselung kann nur der andere Schlüssel des Paares verwendet werden. Wegen dieser Eigenschaft kann man als asymmetrische Verschlüsselungsalgorithmen auch als public key-Algorithmen bezeichnen.

Asymmetrischen Verschlüsselungsalgorithmen liegt die folgende Idee zugrunde:

> Man konstruiere eine Funktion, deren einer Parameter eine spezifische Information, genannt Schlüssel, und deren anderer Parameter eine andere, unspezifische Information, genannt Nachricht oder Klartext, ist. In Abhängigkeit von Schlüssel und Nachricht wird ein Funktionswert, genannt Geheimtext, derart gebildet, daß bei Kenntnis von Schlüssel, Verfahren und Geheimtext eine Rekonstruktion des Klartextes nicht mit vertretbarem Aufwand in akzeptabler Zeit möglich ist.
>
> Insofern die Abbildung ohne Kompression erfolgt, d.h. im Funktionswert die gleiche Informationsmenge, wie in der Nachricht steckt, hat man einen Verschlüsselungsalgorithmus. Wurde die Information dagegen komprimiert, d.h. die Informationsmenge im Geheimtext ist geringer, als im Klartext, handelt es sich um eine Einweg-Hashfunktion.
>
> Gibt es jetzt eine zweite, spezifische Information, mit deren Hilfe bei Kenntnis von Verschlüsselungsverfahren und Geheimtext der Klartext, sprich: die Nachricht, wiederhergestellt, d.h. entschlüsselt werden kann, und zwar in akzeptabler Zeit und mit vertretbarem Aufwand, hat man ein asymmetrisches Verschlüsselungsverfahren konstruiert. Die Information, die zur Entschlüsselung nötig war, nennt man dann ebenfalls Schlüssel.
>
> Mathematisch formuliert:
>
> $A_{S1}(K)=G$, $A_{S2}(G)=K$, mit A ... Algorithmus, S1 ... Schlüssel, S2 ... Schlüssel, S1 ungleich S2

Die grundlegende Idee scheint bereits Ende des letzen Jahrhunderts entwickelt worden zu sein[*]. Publik und praktikabel machten sie jedoch erst Whitfield Diffie und Martin Hellman, Ende der 70'er Jahre. Die bedeutendste Realisierung der Idee ist der RSA-Algorithmus, der auf dem Faktorisierungsproblem aufgebaut ist. Ein neuerer Algorithmus ist der von ElGamal.

Siehe auch: symmetrischer Verschlüsselungsalgorithmus

---

[*] **Siehe:** Annotation zum RSA-Verfahren.

Eingangsseite Index Mail
digitale signaturen diplomarbeit · robert gehring

authentication

authentication (engl.) - Authentifizierung, Echtheitsprüfung, Beglaubigung

Das englische Wort authentication wird oft falsch übersetzt. Beliebt sind sowohl `*Authentizierung*', als auch -seltener- `*Authentikation*'. Der Blick in ein einigermaßen umfangreiches Wörterbuch liefert für das Verb *authenticate* allerdings die Übersetzung *authentifizieren*. Dementsprechend sollte das Substantiv *Authentifizierung* lauten.

AWG [*Außenwirtschaftsgesetz*]

Außenwirtschaftsgesetz - (engl.) Foreign Trade Act (???)

Das Außenwirtschaftsgesetz stellt den wesentlichen Teil des nationalen Außenwirtschaftsrechtes dar. Dieses wird durch Regelungen auf europäischer Ebene ergänzt.

Im AWG sind u.a. die Zuständigkeiten von Behörden und die notwendigen Ausfuhrgenehmigungsverfahren festgelegt.

Ebenfalls werden mit dem AWG Abhörbefugnisse für die Zollkriminalbehörden festgelegt.

BDSG [*Bundesdatenschutzgesetz*]

Bundesdatenschutzgesetz - (engl.) Federal Data Protection Law (?)

Das Bundesdatenschutzgesetz stellt die wichtigste Regelung zum Datenschutz in Deutschland dar. Seine Aufgabe ist folgendermaßen beschrieben:

> ``*Zweck dieses Gesetzes ist es, den einzelnen davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.*" [Paraggraph 1 Absatz 1 BDSG]

Gesetzestext

Begleitgesetz zum TKG (Entwurf)

Begleitgesetz zum TKG - (engl.) ???

Im Entwurf (1997) zu einem Begleitgesetz zum Telekommunikationsgesetz (TKG) werden ... geregelt.

Der Entwurf sieht eine Ausweitung der Befugnisse zum Abhören und Überwachen seitens staatlicher Organe vor.

Siehe auch: IuKDG, TKG, FÜV, FAG, abhören

Benutzerprofil

Benutzerprofil - (engl.) user profile

Ein Benutzerprofil, auch: Nutzerprofil, ist eine statistische Auswertung und Aufbereitung von Daten über die Aktivitäten eines Benutzers (eines Computers, des Internets, des Funktelefons, ...).

Im Internet ist das Benutzerprofil von Internetbenutzern insbesondere für Werbefirmen von Interesse, die ihre Werbung zielgruppengerecht plazieren wollen. Diese wollen möglichst viele Daten über die Nutzer sammeln und darin möglichst wenig beschränkt werden. Um die Interessen von Benutzern, Anbietern und Werbefirmen auszugleichen, gibt es mit OPS einen Vorschlag zur Standardisierung der Datensammelei.

birthday attack

birthday attack (engl.) - Geburtstagsangriff

Birthday attacks [Anm.: Geburtstagsangriff ist eher ungebräuchlich] nutzen statistische Eigenschaften von Hashfunktionen für einen kryptologischen Angriff aus, anstelle von Schwächen der Algorithmen. Auf diese Weise kann es gelingen, falsche Nachrichten unterzuschieben.

Blockchiffrieralgorithmus

Blockchiffrieralgorithmus - (engl.) block encryption algorithm

Siehe: Blockchiffrierung

block cipher

block cipher (engl.) - Blockchiffrierung, Blockverschlüsselungsverfahren, Blockverschlüsselungsalgorithmus

Siehe auch: stream cipher

block encryption

block encryption (engl.) - Blockverschlüsselung, Blockchiffrierung

Siehe auch: stream encryption, block cipher

block encryption algorithm

block encryption algorithm (engl.) - Blockchiffrieralgorithmus

Siehe: Blockchiffrierung

block encryption scheme

block encryption scheme (engl.) - Blockverschlüsselungsverfahren, Blockverschlüsselungsalgorithmus

Anmerkung: Der Ausdruck block encryption scheme ist in der Literatur selten zu finden. Statt dessen findet man eher block cipher.

Siehe auch: stream encryption scheme

Blockverschlüsselung

Blockverschlüsselung - (engl.) block cipher, block encryption

Bei einer Blockverschlüsselung wird eine Anzahl von Daten des Klartextes zusammengefaßt, zu einem Block, und dann verschlüsselt. Werden die Daten des Klartextes einzeln verschlüsselt, spicht man dagegen von einer Stromverschlüsselung.

Wichtige Blockverschlüsselungsalgorithmen sind:

- DES
- IDEA

Siehe auch: Stromverschlüsselung, Blockchiffrierung

Blockverschlüsselungsalgorithmus

Blockverschlüsselungsalgorithmus - (engl.) block encryption algorithm, block encryption scheme

Ein Blockverschlüsselungsalgorithmus ist der Kern eines Blockverschlüsselungsverfahrens. Beide Begriffe werden oft synonym verwandt.

Siehe auch: Stromverschlüsselungsalgorithmus

Blockverschlüsselungsverfahren

Blockverschlüsselungsverfahren - (engl.) block cipher, block encryption algorithm, block encryption scheme

Siehe auch: Stromverschlüsselungsverfahren, Stromchiffrierung

Bob

Bob ist der klassische Teilnehmer einer verschlüsselten Kommunikation. Er tauscht regelmäßig Nachrichten mit Alice, von deren Inhalt niemand Kenntnis erlangen soll. Dazu benutzt er alle möglichen Verschlüsselungsverfahren. Er geistert durch viele Bücher über Kryptographie und Kryptologie.

brute force

brute force (engl.) - rohe Gewalt

Siehe auch: brute force-attack, `brute force'-Angriff

Brute-Force-Angriff *(`brute force'-Angriff)*

Brute-Force-Angriff - (engl.) brute force attack

Ein Brute-Force-Angriffist ein kryptanalytischer Angriff, bei dem alle möglichen Schlüssel des Schlüsselraums durchprobiert werden, in der Hoffnung, möglichst schnell auf den richtigen Schlüssel zu treffen.

Vorgehen

Ein vorliegender Geheimtextwird mit einem gewählten Schlüssel entschlüsselt. Der entzifferte Text mußdann auf Plausibilität geprüft werden. Die meisten Schlüssel werden zu sinnlosen Lösungen führen. Das kann maschinell, z.B. mit Wörterbüchern überprüft werden. Der korrekte Klartext kann anhand seiner Semantik identifiziert werden, was in der Regel nicht maschinell durchführbar ist.

Erfolg

Die einzige Verschlüsselungsmethode die einem Brute-Force-Angriffbeweisbar widersteht, ist das onetimepad. Alle anderen kryptographischen Verfahren sind höchstens praktisch sicher, d.h. ein Brute-Force-Angrifffführt unter Einsatz `großer Rechenkapazitäten' nicht in `vernünftiger Zeit' zum Erfolg.

Je nach Bedeutung der verschlüsselten Information ist die `vernünftige Zeit' dabei unterschiedlich lang. Es kann sich um 24 Stunden (z.B.: Börsenkurs wird verschlüsselt) oder um 50 Jahre (z.B.: Unterlagen über die Entwicklung der Atombombe) handeln. Auch die `großen Rechenkapazitäten' sind ein weitgefaßter Begriff und müssen den jeweiligen Umständen entsprechend interpretiert werden.

Siehe auch:brute force

brute force attack

brute force attack (engl.) - Brute-Force-Angriff, Angriff mit roher Gewalt

bug

bug (engl.) - Wanze, Käfer, Fehler

Capstone-Chip

Der Capstone-Chipbildet das Herzstück der Fortezza-Karte. Er enthält als tamper proof device bzw. tamper resistant deviceden geheimen SKIPJACK-Algorithmus und dient der Datenverschlüsselung mit dem PC.

Der Capstone-Chipist wesentlich komplizierter aufgebaut, als der Clipper-Chip für die Sprachverschlüsselung. Er enthält u. a. Algorithmen für die Public-Key-Verschlüsselung und einen Zufallsgenerator. Ebenfalls wurden DSAund SHAimplementiert. [Menezes/Oorschot/Vanstone 1997]

Siehe auch: Capstone-Initiative

Capstone-Initiative

Für die Capstone-Initiative wird oft synonym der Begriff Clipper-Initiative verwandt.

CBC [*Cipher Block Chaining*]

cipher block chaining (engl.) - Geheimtextblockverkettung

CBC ist ein Verschlüsselungsmodus von Blockverschlüsselungsverfahren. Dabei werden die Geheimtextblöcke, die zu einem Zeitpunkt x erzeugt wurden, mit zur Verschlüsselung der Geheimtextblöcke zum Zeitpunkt x+1 herangezogen, indem der zu verschlüsselnde Klartextblock per XOR mit dem zuletzt erzeugten Geheimtextblock verknüpft wird - *Rückkopplung*.

Siehe auch: ECB

certificate

certificate (engl.) - Zertifikat

certification

certification (engl.) - Zertifizierung

certify

certify (engl.) - zertifizieren

cipher

cipher (engl.) - Verschlüsselungsverfahren, Chiffrierung

ciphertext only attack

ciphertext-only attack (engl.) - Angriff nur mittels Geheimtext, Geheimtextangriff

classified

classified (engl.) - geheim, klassifiziert

Amtliche Dokumente, die als geheim eingestuft werden, werden in den USA als `classified' bezeichnet. Es gibt mehrere Stufen der Klassifizierung.

Clipper

Unter dem Namen Clipper-Initiative versuchte die US-Regierung, das Verfahren des `key escrow' bei Verschlüsselung zu etablieren. Dazu wurde von der NSA u.a. ein Verschlüsselungschip namens `Clipper' entwickelt.

Der Verschlüsselungsalgorithmus der Clipper-Initiative -Skipjack- ist geheim.

Siehe auch: clipper chip, fortezza card

Clipper-Initiative

Clipper-Initiative - (engl.) Clipper initiative

Die Clipper-Initiative der US-Regierung (Start: 16. April 1993) versuchte unter Federführung der NSA, das key escrow-Verfahren, d.h. Verschlüsselung mit Schlüsselhinterlegung, in den USA zu etablieren. Der Begriff wird oft synonym mit Key Escrow Initiative verwandt. Andere, gebräuchliche Begriffe dafür sind: Capstone Initiative, Fortezza-Initiative.

Siehe auch: Clipper, Clipper-Chip

codieren

codieren - (engl.) encode

Codieren(*auch:* kodieren) ist ein älteres Synonym für verschlüsseln.

Siehe auch:decodieren

confusion

confusion (engl.) - Konfusion

Siehe auch: Diffusion

cookies

cookies (engl.) - Plätzchen, Kekse

Cookies sind Bestandteile eines einfachen Schemas, um in Netzwerken Benutzerprofile zu erstellen.

In der Praxis werden sie so eingesetzt, daß ein Server Informationen -cookies- auf dem Rechner ablegt, von dem der Client seine Dienste abgerufen hat. Diese Informationen können dann per Fernabruf abgefragt werden. So läßt sich eine Übersicht gewinnen, wann der Benutzer welche Dienste angefordert hat.

Daß dies auch ohne Zustimmung des Benutzers möglich ist, stellt einen wesentlichen Kritikpunkt aus der Sicht des Datenschutzes dar.

cryptanalysis

cryptanalysis (engl.) - Kryptanalyse

cryptography

cryptography (engl.) - Kryptographie

cryptology

cryptology (engl.) - Kryptologie

cryptosystem

cryptosystem (engl.) - Verschlüsselungssystem

CU [*See You*]

See You. (engl.) - Bis bald., Wir sehen uns.

CUist eine im Internet häufig gebrauchte Redewendung.

Mit derartigen Abkürzungen kann man die Bandbreite des Internets schonen, wie es z.B. bei Newsgroups angebracht ist.

DARPA [*Defense Advanced Research Projects Agency*]

Defense Advanced Research Projects Agency (engl.) - Agentur für Weiterführende Verteidigungsprojekte

DARPA ist ein anderer Name für die ARPA.

Datenschutz

Datenschutz - (engl.) data protection

Die wichtigste Vorschrift zum Datenschutz ist in Deutschland das Bundesdatenschutzgesetz (BDSG). Zusätzlich existieren noch Landesdatenschutzgesetzes.

DEA [*Data Encryption Algorithm*]

DEA ist die ANSI-Bezeichnung für den DES-Algorithmus "für private Zwecke". Für amtliche Zwecke ist DES als FIPS PUB 46 standardisiert.

decipher

decipher (engl.) - entschlüsseln

decode

decode (engl.) - decodieren, entschlüsseln

decodieren

decodieren - (engl.) decode

Decodieren(*auch:*dekodieren) ist ein älteres Synonym für entschlüsseln.

Siehe auch:codieren

decrypt

decrypt (engl.) - entschlüsseln

dekodieren

dekodieren - (engl.) decode

Siehe:decodieren

Diffusion

Diffusion - (engl.) diffusion

Unter Diffusion versteht man die Verteilung der redundanten Informationen des Klartextes über den Geheimtext. Transposition ist eine Form von Diffusion. Der Begriff Diffusion in diesem Zusammenhang geht auf Claude Shannon zurück.

Stromchiffrierungen arbeiten in der Regel mit Diffusion.

Siehe auch: Konfusion

digitales Wasserzeichen

digitales Wasserzeichen - (engl.) digital watermark

Ein digitales Wasserzeichenist eine Art versteckter digitaler Signaturin urheberrechtlich geschützten, digitalen Daten (Bildern, Musikstücken, etc.). Derartige Markierungen sollen der Durchsetzung urheberrechtlicher Ansprüche in Medien mit digitaler Kommunikation dienen, wie z.B. dem Internet.

Anforderungen

Die wichtigste Forderung an die Qualität digitaler Wasserzeichen ist die nach ihrer Dauerhaftigkeit.
...

digital watermark

digital watermark (engl.) - digitales Wasserzeichen

DIN [*Deutsche Industrie-Norm*]

Deutsche Industrie-Norm - (engl.) German Industrial Standard

Siehe auch: DIN-Institut, ANSI

DSA [*Digital Signature Algorithm*]

Digital Signature Algorithm (engl.) - Algorithmus für Digitale Signaturen

Der DSAwurde vom NIST1991 zusammen mit dem DSS(Digital Signature Standard) vorgestellt. DSAbasiert auf dem Verfahren von ElGamalund dient der Erzeugung und Verifikation von Digitalen Signaturen, sowie der Verteilung von Schlüsseln. Der Algorithmus wurde von der NSAentwickelt.

Sicherheit

DSAist öffentlich und konnte analysiert werden. Als Abkömmling von ElGamal, basiert die Sicherheit des DSAauf dem Problem der diskreten Logarithmen: Sie wird angenommen, ist aber nicht bewiesen (allerdings auch nicht widerlegt). Es wird SHA(Secure Hash Algorithm) als Hashfunktion eingesetzt. Die Sicherheit von DSAhängt also auch von der Sicherheit des SHA ab.

Patente

DSA wurde von Kravitz zur Patentierung angemeldet und ist unter Nr. 5.231.668 mit Datum vom 27. Juni 1993 patentiert.

Internet

FIZ Karlsruhe
Lecture Notes in Computer Science

US Patent Office
US Patents Database

Eingangsseite Index Mail

digitale signaturen diplomarbeit · robert gehring

DSS [*Digital Signature Standard*]

Digital Signature Standard (engl.) - Standard für Digitale Signaturen

DSS wurde als FIPS (Federal Information Processing Standard) Nr. 186 vom NIST 1991 veröffentlicht und basiert auf dem DSA (Digital Signature Algorithm). DSS repräsentiert *den* offiziellen Standard für Digitale Signaturen in den USA. Als FIPS ist er für den Einsatz in Behörden zugelassen und empfohlen.

Es gab viel Kritik an der Entscheidung des NIST, DSA statt RSA einzusetzen, nicht zuletzt von RSADSI, die lieber Lizenzgebühren kassiert hätten. Abgesehen davon wurde argumentiert, daß der de facto-Standard international RSA (ISO 9796) ist und im Sinne der Interoperabilität eine Entscheidung für diesen angebracht gewesen wäre.

ECB [*Electronic Codebook*]

electronic codebook (engl.) - elektronisches Codebook

ECB ist ein Verschlüsselungsmodus von Blockalgorithmen, bei dem ein Klartextblock zu einem Geheimtextblock codiert wird. Dabei wird keine Rückkopplung, wie bei CBC vorgenommen.

Siehe auch: CBC

EES [*Escrowed Encryption Standard*]

Escrowed Encryption Standard (engl.) - Standard für Verschlüsselung mit Schlüsselhinterlegung

EES (FIPS-185) wurde 1994 im Rahmen der Clipper-Initiative eingeführt und stellt eine Möglichkeit für US-Behörden dar, ihre Kommunikation zu verschlüsseln. Sie *können, müssen aber nicht* EES-verschlüsselt kommunizieren. Wenn sie es tun, können die Sicherheitsbehörden wegen der Schlüsselhinterlegung (key escrow) mithören.

EISS [*European Institute for Systems Security*]

Das EISSwurde vom Land Baden-Württemberg (!) am 29. Februar 1988 ins Leben gerufen. Seine Aufgabe besteht in der Forschung zum Thema der Sicherheit in:

- Computersystemen
- Telekommunikation
- Informationssystemen

Dazu gehört insbesondere auch die kryptologische Forschung.

ElGamal

ElGamal wurde, wie auch RSA, nach seinem Entwickler benannt - Taher ElGamal.

Ebenso, wie das RSA-Verfahren, basiert das Verfahren von ElGamal auf einem zahlentheoretischen Problem, in diesem Falle der Berechnung von diskreten Logarithmen modulo einer großen Primzahl.

encryption algorithm

encryption algorithm (engl.) - Verschlüsselungsalgorithmus, Verschlüsselungsverfahren

escrow agent

escrow agent (engl.) - Hinterlegungsagent, Treuhänder

Einen escrow agentbenötigt man für den key escrow, um dort den Schlüsselzu hinterlegen.

Die US-Regierung hat zwei escrow agentsvorgeschlagen: Das NISTund die Abteilung für automatisierte Systeme beim Schatzministerium (Department of the Treasury, Automated Systems Division).

FAG [*Fernmeldeanlagengesetz*]

Fernmeldeanlagengesetz - (engl.) ???

Das Fernmeldeanlagengesetz legte (in der Fassung vom 3.7.1989) fest, daß Fernmeldeanlagen ausschließlich vom Bund errichtet werden durften. Der Bund nahm dieses Recht durch Beauftragung der Deutschen Telekom wahr.

Im Zuge der Liberalisierung des Fernmeldewesens innerhalb der EU wurde das FAG stark überarbeitet und den neuen Bedingungen eines offenen Marktes angepaßt.

Die Sicherheitsdienste, die Polizei, der Bundesinnenminister, die meisten Innenminister der Länder, und ... sind sehr daran interessiert, auch die Überwachungsmöglichkeiten den neuen (gesetzlichen und technischen) Umständen anzupassen. Stichwort: Großer Lauschangriff.

Der umstrittene Pragraph 12 des FAG ermöglicht durch seine vage Formulierung eine weite Auslegung und somit teilweise eine Überwachung des Telekommunikationsverkehrs ohne richterliche Ermächtigung.

Das FAG ist bis zum 31.12.1997 gültig.

Siehe auch: TKG, FÜV, abhören

Falltür

Falltür (engl.) - trapdoor

Als Falltür bezeichnet man im kryptologischen Sinne die Eigenschaft einer schwer berechenbaren Funktion, bei Einbeziehung einer spezifischen Information, der Falltürinformation, deutlich leichter berechenbar zu sein. Solche schwer berechenbaren Funktionen treten in der Regel als Einweg-Funktionenauf.

Falltürinformation

Falltürinformation - (engl.) trapdoor information

Eine Falltürinformationist die Kenntnis davon, wie die inverse Funktion zu einer Einweg-Funktionzu bilden ist.

Siehe auch: Falltür

FBeitrV [*Frequenznutzungsbeitragsverordnung*]

Frequenznutzungsbeitragsverordnung - (engl.) ???

Eingangsseite Index Mail

FGebV [*Frequenzgebührenverordnung*]

Frequenzgebührenverordnung - (engl.) ???

Im Rahmen der Liberalisierung des Telekommunikationsmarktes trat zum ... die Frequenzgebührenverordnung in Kraft. Sie regelt, ...

Fortezza-Initiative

Bei der Fortezza-Initiative handelt es sich um die Clipper-Initiative. Der Begriff Fortezza-Initiative ist eher ungebräuchlich.

Siehe auch: Fortezza-Karte

Fortezza-Karte

Fortezza-Karte - (engl.) fortezza card

Die Fortezza-Karteentstand im Rahmen der Capstone/Fortezza-Initiative, alias Clipper-Initiative. Federführend war die NSA.

Aufbau

Es handelt sich um eine PC-Card(PCMCIA-Card), die einen Capstone-Chipenthält, d.h. die Verschlüsselung wird mit dem geheimen SKIPJACK-Algorithmus vorgenommen. Sie kann an jeden PC mit einem entsprechenden PC-Card-Steckplatz angeschlossen werden. Aktiviert wird die Karte erst nach der Eingabe einer PIN(Personal Identification Number). Voraussetzung ist natürlich die Installation entsprechender Software.

Einsatz

Die Fortezza-Kartekann eingesetzt werden für
- Benutzerauthentifizierung
- Verschlüsselung
- Integritätssicherung.

Das US-Verteidigungsministerium setzt die Karte zur Absicherung seiner Kommunikation ein.

Sicherheit

Eine Untersuchungskommission hat den SKIPJACK-Algorithmus für sicher erklärt. Überprüfen läßt sich dieses Resultat nicht, da der Algorithmus geheim (classified) ist.

Der Capstone-Chip der Fortezza-Karte gilt als `tamper proof device', d.h. ebenfalls als sicher. Es gibt aber Gerüchte in den entsprechenden Newsgroups, daß in den Sandia National Laboratories ein Exemplar bereits geknackt wurde. Belegt ist das nicht.

Daß die Verschlüsselung mittels key escrow den berechtigten Behörden -und allen anderen, die Zugriff sowohl auf den hinterlegten Schlüssel, als auch auf den Kommunikationskanal haben,- zugängig ist, sollte nicht vergessen werden.

Siehe auch: Tessera-Karte

FreqZutV [*Frequenzzuteilungsverordnung*]

Frequenzzuteilungsverordnung - (engl.) ???

FÜV [*Fernmeldeverkehrsüberwachungsverordnung*]

Fernmeldeverkehrsüberwachungsverordnung - (engl.) ???

Die FÜV regelt ... die (technischen) Umstände, unter denen die Sicherheitsdienste Zugriff auf die Daten der Telekommunikation erhalten sollen. ???

Dazu gehört z.B., daß der verschlüsselte Funktelefonverkehr (GSM-Netze, d.h. D1, D2, E-Plus) entschlüsselbar sein muß.

Siehe auch: TKG, FAG, G-10-Gesetz, abhören

Verordnungstext

FIPS [*Federal Information Processing Standard*]

Federal Information Processing Standard (engl.) - Bundesstandard für Informationsverarbeitung

Mit FIPS werden in den USA Normen gekennzeichnet, die vom NIST (National Institute of Standards and Technology) herausgegeben werden. Die FIPS-Normen stellen die Grundlage für alle weiteren Spezifikationen auf Bundesebene dar. Das NIST greift oft auf Vorschläge aus der Industrie oder des ANSI zurück, um den Erfolg der Normierungen sicherzustellen.

Bedeutung

Entscheidungen des NIST, eine industrielle Technologie zu einem FIPS zu erklären, sind oft von großer wirtschaftlicher Tragweite. Insbesondere der Einsatz in Bundesbehörden ist von der FIPS-Konformität abhängig. Die mangelnde Herstellerunabhängigkeit stellt einen Kritikpunkt dar.

Beispiele

- FIPS 185 - Escrowed Encryption Standard (EES)
- FIPS 186 - Digital Signature Standard (DSS)

fortezza card

fortezza card (engl.) - Fortezza-Karte

Die fortezza card wurde -ebenso, wie der clipper chip- von der NSA im Rahmen der Clipper-Initiative zur Schlüsselhinterlegung (key escrow) bei starker Verschlüsselung entwickelt.

G-10-Gesetz

G-10-Gesetz - (engl.) ???

Das Grundgesetz räumt in Paragraph 10 dem Brief-, dem Post- und dem Fernmeldegeheimnis einen hohen Stellenwert ein, indem diese als unverletzlich bezeichnet werden. Diese Unverletzlichkeit kann allerdings durch ein Gesetz eingeschränkt werden. Dazu dient das sogenannte G-10-Gesetz (Gesetz zu Artikel 10 GG vom 13. August 1968).

Im G-10-Gesetz (Creifelds: ``*Abhörgesetz*'') sind die Bedingungen für die heimliche Überwachung des Briefverkehrs und das Abhören des Telefonverkehrs von Personen geregelt. Die Betroffenen müssen nicht über die Aktion benachrichtigt werden, auch nicht nach deren Abschluß, und der Rechtsweg zur Überprüfung kann ausgeschlossen werden. Allerdings kann eine Benachrichtigung erfolgen.

Die Überwachung kann durch einen Richter oder, bei ``Gefahr im Verzug'', durch einen Staatsanwalt angeordnet werden.

Überwachung

Gründe, wegen denen eine Überwachung beantragt werden kann:

- begründeter Verdacht, daß jemand staatsgefährdende Straftaten begeht, begangen hat oder plant
- Erkennung und/oder Abwehr (internationaler) terroristischer Anschläge
- Abwehr eines bewaffneten Angriffs auf die Bundesrepublik Deutschland
- unerlaubter Kriegswaffenhandel
- unerlaubter Betäubungsmittelhandel

Personen, die Betroffen sein können:

- Personen, bei denen die oben genannten Gründe vorliegen (Verdächtige)
- Personen, die mit Personen, bei denen die oben genannten Gründe vorliegen (Verdächtige), kommunizieren

Vorgesehene Antragsteller:

- Bundesnachrichtendienst
- Bundesverfassungsschutz
- Landesverfassungschutz
- Amt für Sicherheit der Bundeswehr

Siehe auch: IuKDG, TKG, abhören

Eingangsseite Index Mail
digitale signaturen diplomarbeit · robert gehring

Geheimtextangriff

Geheimtextangriff - (engl.) ciphertext-only attack

Wenn zur Kryptanalyseausschließlich Geheimtexteverwendet werden (können), spricht man von einem Geheimtextangriff. Das Szenario sieht folgendermaßen aus:

Der Kryptananlytiker hat eine Anzahl von Geheimtexten (durch Abhören o.ä. erlangt) und nimmt an, daß sie mit demselben Verfahren verschlüsselt wurden. Dann stellen sich ihm drei Aufgaben mit unterschiedlichem Schwierigkeitsgrad:

1. Die Klartexte zu den Geheimtexten ermitteln.
2. Den Schlüssel der Verschlüsselung bestimmen.
3. Das Verschlüsselungsverfahren bestimmen.

Je nach Erfolg kann er weitere Geheimtexte entschlüsseln oder sogar selbst Klartexte verschlüsseln (wenn er Schlüssel und Verschlüsselungsverahren ermitteln konnte).

Effektivere Formen von Angriffen über den Geheimtext sind:

- Geheimtextangriff mit gewähltem Geheimtext
- Geheimtextangriff mit Anpassung des gewählten Geheimtextes

Geheimtextangriff mit Anpassung des gewählten Geheimtextes

Geheimtextangriff mit Anpassung des gewählten Geheimtextes - (engl.) adaptive chosen-ciphertext attack

Beim Geheimtextangriff mit Anpassung des gewählten Geheimtextes kann der Kryptanalytiker wiederholt einen Geheimtext auswählen, zu dem er den Klartext erhält. Durch geschickte Wahl der Geheimtexte bestimmt er charakteristische Eigenschaften des Verschlüsselungssystems. Hat er genug Erkenntnisse gesammelt, d.h. der Angriff war erfolgreich, kann er weitere Geheimtexte in Klartexte übersetzen.

Geheimtextangriff mit gewähltem Geheimtext

Geheimtextangriff mit gewähltem Geheimtext - (engl.) chosen-ciphertext attack

Dieser Angriffwird ausgeführt, indem der Angreiferzu einer Anzahl von ihm ausgewählter Geheimtextedie Klartexteerhält. Ziel ist es, aus der Analyse der Geheimtext/Klartext-Paare Erkentnisse über die Art und Weise der Verschlüsselungzu gewinnen.

Gelingt der Angriff, kann der Angreifer im Anschluß andere Geheimtexte ohne Zugriff auf die Verschlüsselungstechnik oder die Klartexte entschlüsseln.

Der Geheimtextangriff mit gewähltem Geheimtext ist eine effektivere Form des Geheimtextangriffes.

Siehe auch: Geheimtextangriff mit Anpassung des gewählten Geheimtextes

GIP [*Global Internet Project*]

Global Internat Project (engl.) - Globales Internet-Projekt

Das GIP ist ein Zusammenschluß großer Internet-Provider, der deren Interessen ggü. Regierungen und Industrie vertreten soll.

Siehe auch: http://www.gip.org

GNFS [*General Number Field Sieve*]

general number field sieve (engl.) - allgemeines Zahlkörpersieb

Hashwert

Hashwert - (engl.) hash value

Der Hashwertist das Ergebnis (Ausgabewert) der Anwendung einer Hashfunktionauf einen Eingabewert. Handelt es sich um eine kryptographische Hashfunktion, so bezeichnet man den Hashwertoft als *message digest*(MD).

Eingangsseite Index Mail

hash function

hash function (engl.) - Hashfunktion

hash value

hash value (engl.) - Hashwert

IAB [*Internet Activities Board*]

Internet Activities Board (engl.) - Kommission für Internetaktivitäten

Das IAB (ehemals: ICCB, Internet Control and Configuration Board) lenkt die Entwicklung des Internet. Dazu beschäftigt es zwei Arbeitsgruppen: IETF (Internet Engineering Task Force) und IRTF (Internet Research Task Force).

IP [Internet Protocol]

Internet Protocol (engl.) - Internetprotokoll

Damit Computer in einem Netzwerk miteinander kommunizieren können, sind sie darauf angewiesen, Aktionen und Reaktionen standardisiert auszuführen. Einen solchen Standard stellt das Internet Protocol (IP) zur Verfügung.

IP wurde im Rahmen des ARPA-Projektes entwickelt und stellt den defacto-Standard für die Rechnerkommunikation in offenen Netzen dar.

Bei einer Kommunikation nach IP werden die auszutauschenden Nachrichten in Teile einheitlicher Länge (Pakete, packets) zerlegt. Diese werden alle einzeln mit einer Adresse versehen (IP-Adresse) und an den Rechner, zu dem die Adresse gehört, geschickt. Sind die Pakete am Ziel angekommen, werden sie von ihrer Adresse befreit und wieder zur ursprünglichen Nachricht zusammengesetzt.

Der Weg durchs Internet, den die einzelnen Pakete nehmen, steht nicht vorher fest. Vielmehr werden sie an den nächsten erreichbaren, zur Paketübermittlung bestimmten Rechner geschickt. Der schickt sie je nach Adresse weiter. So werden die Pakete von Rechner zu Rechner geschickt, bis sie ihr Ziel erreichen.

Sollte ein Übertragungscomputer ausfallen, so werden die Pakete an den nächsten zuständigen Rechner geschickt. Für solche Fälle gibt es Listen, welche Übermittlungsrechner mit welcher Priorität zuständig sind.

Siehe auch: TCP/IP, UDP/IP

IP-Tunnel [*Internet Protocol Tunnel*]

Internet Protocol Tunnel (engl.) - Tunnel via Internetprotokoll

Siehe: IP-Tunneling

IP-Tunneling

IP-Tunneling (engl.) - IP-Untertunnelung

IP-Tunneling ist tunneling für IP (Internet Protocol).

Mittels IP-Tunneling lassen sich Kommunikationsprotokolle auf Basis des Internetstandardprotokolls IP abwickeln. Eingesetzt werden solche Verfahren z.B. in Virtuellen Privaten Netzwerken (Virtual Privat Network , VPN). Häufig verwenden die proprietären Protokolle Verschlüsselungstechniken, um die Kommunikation zu schützen.

Die proprietären Protokolle werden dabei z.B. auf Applikationsebende implementiert. Die Internet-/Intranetkommunikation zwischen den Applikationen erfolgt dann über die Mechanismen, die TCP/IP zur Verfügung stellt und die gut getestet sind.

Es ist also nicht nötig, sämtliche Kommunikationsvorgänge neu zu implementieren. Man kann sich auf applikationsspezifische Teile konzentrieren und gleichzeitig die Flexibilität des Internet ausnutzen.

IRTF [*Internet Research Task Force*]

Internet Research Task Force (engl.) - Arbeitsgruppe für Internetforschung und -entwicklung (???)

Die IRTF ist, neben der IETF (Internet Engineering Task Force), eine der beiden Arbeitsgruppen des IAB (Internet Activities Board).

ISAKMP [*Internet Security Association and Key Management Protocol*]

Internet Security Association and Key Management Protocol (engl.) - Internetsicherheitsverbund- und Schlüsselverwaltungsprotokoll

ISAKMP ist das von der IETF bevorzugte Modell zur Schlüsselverwaltung im Internet. Es liegt als Internet-Draft vor.

Siehe auch: SKIP

ISO [*International Standards Organisation*]

International Standards Organisation (engl.) - Organisation für Internationale Standards

Die ISO ist das internationale Gegenstück zu den nationalen Standardisierungs- und Normungsgremien, wie z.B. dem ANSI in den USA oder dem DIN - Institut in Deutschland.

IuKDG [*Informations- und Kommunikationsdienstegesetz*]

Informations- und Kommunikationsdienstegesetz - (engl.) Information and Communication Services Act (???)

Das IuKDG, umgangssprachlich: *Multimediagesetz*, wurde im Dezember 1996 beschlossen, trat zum 1. August 1997 in Kraft und soll die Weichen auf dem Weg in die Informationsgesellschaft stellen. Das meint jedenfalls die Bundesregierung und sieht sich in einer europäischen/internationalen Vorreiterrolle.

Siehe auch:TKG, G10-Gesetz

Gesetzestext

IW [*Information Warfare*]

Information Warfare (engl.) - *in etwa:* Kriegführung mit/durch/gegen Informationen und Informationstechnik

An dieser Stelle ein Zitat aus [CRISIS 1996], S.49:

> `` "Information warfare" (IW) is a term used in many different ways. Of most utility for this report is the definition of IW as *hostile action that targets the information systems and information infrastructure of an opponent*... "

insecure channel

insecure channel (engl.) - unsicherer Kanal

JCE [*Java Cryptography Engine*]

Java Cryptography Engine (engl.) - Verschlüsselungsmaschine für Java

JCE, eine SUN-Entwicklung, stellt kryptographische Routinen für die Java-Programmierung bereit.

JIS [*Japanese Industrial Standardisation Committee*]

Japanese Industrial Standardisation Committee(engl.) - Japanisches Komitee für Industriestandards

JIS ist die englische Abkürzung für das Japanische Komitee für Industriestandards. Das JIS ist das japanische Gegenstück zum amerikanischen ANSI oder dem deutschen DIN-Institut.

LOKI

LOKIist die Bezeichnung für ein Paar von Blockverschlüsselungsverfahren, die auf einem von Lawrence P. Brown, Josef Pieprzyk und Jennifer Seberry entwickelten Konzept basieren (LOKI'89).

Ursprünglich handelte es sich um einen einzigen Algorithmus, genannt LOKI. Nachdem dieser sich als unsicher herausgestellt hatte, wurde er umbenannt in LOKI'89 und weiterentwickelt zu LOKI'91.

Sicherheit

Beide Varianten sind anfällig gegen Angriffe mit verwandten Schlüsseln(related-key attacks). Sicherer werden sie bei einer Verbesserung der Schlüsselverwaltung. ([Schneier 1996], S. 363 ff; [Menezes/Oorschot/Vanstone 1997], S. 281)

Patente

LOKI'89und LOKI'91sind nicht patentiert.

LOKI'89

LOKI'89hießursprünglich nur LOKI. Nachdem aufgedeckt wurde, daßer nicht sicher ist, wurde er in LOKI'89 umbenannt und ein Nachfolger entwickelt - LOKI'91.

Siehe auch:LOKI

LOKI'91

LOKI'91ist der Nachfolger von LOKI'89.

Siehe auch:LOKI

LEAF [*Law Enforcement Access Field*]

Law Enforcement Access Field (engl.) - Zugriffsbereich zur Durchsetzung der Gesetze

Das LEAFwird bei der Verschlüsselung mit SKIPJACK-Algorithmus verwendet.

Praktisch gesehen handelt es sich beim LEAF um eine Bitfolge, in der u.a. der Sitzungsschlüssel und die UID (unique identifier) des jeweiligen Gerätes codiert sind. Das LEAF übernimmt dabei zwei Funktionen:

- Eine Entschlüsselung wird nur bei gültigem LEAF durchgeführt.
- Behörden können die Kommunikationsteilnehmer identifizieren und zu Zwecken des Abhörens den Sitzungsschlüssel rekonstruieren.

Siehe auch: Clipper-Initiative

Lucifer

Lucifer war der Name eines Projektes der IBM, das in der 70'er Jahren von einem Kryptographen-Team durchgeführt wurde. Zu dem Team gehörten unter anderem Don Coppersmith und Horst Feistel. Von Horst Feistel wurde dabei das sogenannte Feistel-Netzwerk entwickelt. Ziel des Projektes war die Entwicklung von Verschlüsselungstechnologie, die sich leicht in Hardware implementieren läßt und die außerdem effizient arbeitet.

Diese Kriterien setzen voraus, daß nur elementare Prozessoroperationen auszuführen sind und der Speicherbedarf gering ist. Um die Sicherheit zu gewähren, muß der Algorithmus gleichzeitig Schlüssel aus einem großen Schlüsselraum verwenden können. Die Sicherheit darf dabei nur von der Wahl des Schlüssels und nicht vom Algorithmus selbst abhängig sein, um das Problem der Geheimhaltung des Algorithmus zu vermeiden.

Lucifer war das Ergebnis des Entwicklungsprozesses. Er verwendete nur elementare Prozessoroperationen (XOR, ADD, ...) und verschlüsselte mit 128 Bit (inlusive Parität), d.h. es gibt 2^112 verschiedene Schlüssel. Da er auf Feistel-Netzwerken basierte, war auch der Speicherbedarf gering. Damit war diese Bedingung für eine effiziente Implementierung erfüllt.

IBM reichte Lucifer als Vorschlag auf eine Ausschreibung des NBS (National Bureau of Standards) hin ein. In dieser Ausschreibung wurde nach einer Verschlüsselungstechnologie gesucht, die man als offiziellen Standard einführen könnte.

An dieser Stelle kommt die NSA in's Spiel. Das NBS zog -nach offizieller Darstellung- die NSA bei der Evaluierung des Algorithmus zu Rate. Im Ergebnis wurde die Schlüssellänge auf 56 Bit (8 Byte inklusive Parität) reduziert und der Algorithmus unter der Bezeichnung "Data Encryption Standard" (DES) freigegeben (23. November 1976), allerdings nur für "nichtgeheime Regierungsvorgänge" (!). Ob die Veröffentlichung des Algorithmus dabei `*aus Versehen*' geschah (siehe [Schneier 1996], S.311) und eigentlich nicht vorgesehen war, bleibt umstritten.

Nutzerprofil

Nutzerprofil - (engl.) user profile

Nutzerprofil ist ein Synonym für Benutzerprofil.

NBS [*National Bureau of Standards*]

Das NBS war der Vorläufer des NIST.

INDEX - N

HAUPTINDEX

HOME

NDA [*Non-Disclosure Agreement*]

Non-Disclosure Agreement (engl.) - Abkommen über Nichtoffenlegung, Geheimhaltungsabkommen

Ein NDA ist ein beliebtes Mittel, um sich vor unerwünschten Mitbewerbern zu schützen. Der Unterzeichner stimmt dabei zu, ihm zugänglich gemachtes Knowhow (Technologie) geheim zu halten. So kann der Technologieinhaber sich auswählen, wen er in seine Geheimnisse einweiht und gleichzeitig durch Kooperation seine Technologie am Markt durchsetzen.

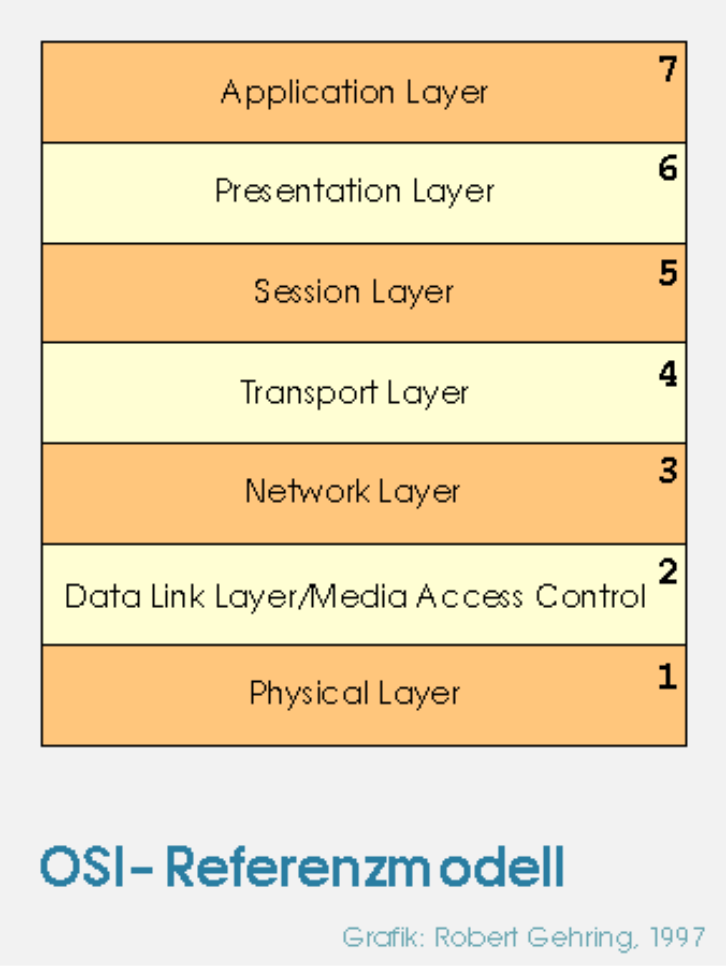
number theory

number theory (engl.) - Zahlentheorie

OSI - Referenzmodell

OSI - Referenzmodell - (engl.) OSI Reference Model

Das OSI - Referenzmodell stellt eine abstrakte Beschreibung vernetzter Computersysteme dar. Die Kommunikation zwischen den Computern wird in einem 7-Schichtenmodell repräsentiert.



Jede Schicht ist spezifischen Teilen der Netzwerkkommunikation zugeordnet. Von den meisten Netzwerktechnologien werden nicht alle Schichten einzeln implementiert. Oft werden die Schichten 5-7 zusammengefaßt.

Das OSI-Referenzmodell wurde von der ISO (International Standards Organisation) entwickelt und ist international für offene Netzwerke akzeptiert.

Funktion

Die Funktionen der einzelnen Schichten lassen sich folgendermaßen beschreiben:

Schicht 7: **Application Layer**	Schicht 7 repräsentiert die Ebene der Anwendungsprogramme, die so vielfältig, wie die Hersteller zahlreich sind. **Beispiel:** Die UNIX-Office-Suite Applix*ware* ist netzwerkfähig, arbeitet also auf Ebene 7.
Schicht 6: **Presentation Layer**	In Schicht 6 ... **Beispiel:**
Schicht 5: **Session Layer**	In Schicht 5 ... **Beispiel:**
Schicht 4: **Transport Layer**	In Schicht 4 ... **Beispiel:**
Schicht 3: **Network Layer**	In Schicht 3 ... **Beispiel:**
Schicht 2: **Data Link Layer/Media Access Control**	In Schicht 2 werden die Modi des Zugriffs auf die physikalische Netzwerkverbindung in Schicht 1 repräsentiert. **Beispiel:** Der Zugriffsmodus bei Ethernetverbindungen, wie sie in lokalen Netzwerken (LANs) üblich sind, heißt z.B. CSMA/CD (Carrier Sense Multiple Access with Collision Detection).
Schicht 1: **Physical Layer**	Schicht 1 repräsentiert die Ebene der Verkabelung bzw. der physikalischen Verbindung der Computer. **Beispiel:** Koaxialkabel, Richtfunk, Telefonkabel, ...

Siehe auch: OSIRM

OSIRM [*Open Systems Interconnection Reference Model*]

Open Systems Interconnection Reference Model (engl.) - Referenzmodell für die Zusammenschaltung offener Systeme

OSIRM ist die wenig gebräuchliche Abkürzung für *OSI Reference Model*, dt.: OSI-Referenzmodell.

OECD [*Organization for Economic Cooperation and Development*]

Organization for Economic Cooperation and Development (engl.) - Organisation für Wirtschaftliche Zusammenarbeit und Entwicklung

Die OECD ist als zwischenstaatliche Organisation zuständig für ...

Kryptographie

Die OECD hat kürzlich für die Mitgliedsstaaten Richtlinien zum Umgang mit Kryptographie veröffentlicht, die als *relativ liberal* angesehen werden. Dort heißt es u.a.:

`` ... "

Siehe auch: http://www.oecd.org

OID [*Object Identifier*]

Object Identifier (engl.) - Objektkennung

One-Time-Pad

Für One-Time-Padgibt es keinen deutschen Begriff, weshalb der englische Begriff kurzerhand übernommen wurde. Wörtlich übersetzt würde es `Einmal-Block' heißen.

Der Begriff leitet sich von der ersten praktikablen Implentierung des Verfahrens ab:

> Auf die Seiten eines Textblocks wurden Zufallszahlen gedruckt. Zur Verschlüsselung wurden die Zahlen der obersten Seite als Schlüssel benutzt. Anschließend wurde die Seite vernichtet. Für das Entschlüsseln stand ein identischer Schlüssel zur Verfügung. Dessen Schlüsselseite wurde nach der Entschlüsselung ebenfalls vernichtet. Gegebenenfalls mußten mehrere Schlüsselseiten benutzt werden, um eine Schlüsselwiederholung zu vermeiden.

Das One-Time-Padist das einzige wirklich sichere Verschlüsselungsverfahren, solange (a) wirkliche Zufallszahlen oder -buchstaben benutzt werden und (b) die Schlüssel wirklich nur einmal (one time) verwendet werden. Als Erfinder werden genannt: Werner Kunze und Erich Langlotz ([Kippenhahn 1997]); Kuntze, Schaufler und Langlotz ([Bauer 1994]) bzw. Joseph Mauborgne und Gilbert Vernam ([Schneier 1996]).

Sicherheit

Worauf basiert nun die Sicherheit des One-Time-Pad?

Der Schlüssel, der die gleiche Länge wie der Klartext haben muß, wird aus einer Menge von Zeichen (derselben Menge, wie sie für die Textbuchstaben verwendet wird) zufällig gewählt. Der Schlüssel hat dann eine unendliche Periode, da bei zufälliger Auswahl der Zeichen keine Periode (systematische Wiederholung) entstehen kann. Dann wird je ein Klartextzeichen mit je einem Schlüsselzeichen chiffriert. Vorausgesetzt, die Zeichen des Schlüssels sind tatsächlich zufällig gewählt, *kann ein Geheimtext dann mit gleicher Wahrscheinlichkeit zu jedem möglichen Klartext gleicher Länge gehören*. Damit sichergestellt ist, daß kein Schlüssel mehrfach verwendet wird, muß dieser nach der Chiffrierung bzw. Dechiffrierung vernichtet werden.

Das Problem dieses Verfahrens besteht darin, daß beiden Seiten (Chiffreur und Dechiffreur) der gleiche Schlüssel bekannt sein muß. Die Schlüsselübergabe muß demnach zu einem Zeitpunkt erfolgen, zu dem noch nicht feststeht, was zu chiffrieren ist. Andernfalls müßte der Schlüssel kurz vor dem Chiffriervorgang unbemerkt übermittelt werden. Da der Schlüssel die gleiche Länge, wie der Klartext hat, könnte man an dessen Stelle aber auch gleich die Nachricht übermitteln, da die Übermittlung ja ohnehin geheim erfolgen muß. Auch muß ein Schlüssel, der eine gewisse Zeit vorher übergeben wurde bis zum Zeitpunkt der Entschlüsselung sicher aufbewahrt werden.

Ein weiteres Problem besteht in der zufälligen Auswahl der Schlüsselzeichen. Computer sind dazu nicht geeignet, da sie nur Pseudo-Zufallswerte generieren können. Zufällige Natureinflüsse (z.B. Athmosphärenrauschen) stellen zwar eine Möglichkeit dar. Dann muß aber sichergestellt werden, daß diese Ereignisse nicht als solche identifiziert werden können, weil sonst unter Umständen Aufnahmen, die davon existieren, zur Entschlüsselung verwendet werden können.

Man sieht, die Einsatzmöglichkeiten des One-Time-Pad sind sehr begrenzt.

one-way function

one-way function (engl.) - Einweg-Funktion

OPS [*Open Profiling Standard*]

Open Profiling Standard (engl.) - offener Standard für die Erstellung von Profilen

OPS soll nach dem Willen verschiedener großer Anbieter von Internettechnologie (z.B. Netscape, VeriSign, IBM, HP, Sun) *der* Standard für die automatische Erstellung, Übermittlung und Auswertung von Benutzerprofilen werden und das bisher verwendete Schema mit Cookies ablösen.

Nach OPS soll der Benutzer wesentlich besseren Einblick in das erstellte Benutzerprofil erhalten. Auch soll er/sie selbst darüber entscheiden können, wer welche Daten abrufen darf. Vielen Werbefirmen geht der vorgesehene Datenschutz zu weit und sie versuchen, ihn abzuschwächen.

OSI [*Open Systems Interconnect, Open Systems Interconnection*]

Open System Interconnection (engl.) - Zusammenschaltung offener Systeme

Es gibt keinen entsprechenden deutschsprachigen Begriff, OSI ist etabliert.

Siehe auch: OSIRM, OSI-Referenzmodell

OSS [*Ong-Schnorr-Shamir*]

OSS(1984) wurde nach seinen Entwicklern -*H. Ong, Claus P. Schnorr*und *Adi Shamir*- benannt. Es handelt sich dabei um ein Verfahren für Digitale Signaturen, das auf quadratischen Gleichungen basiert.

Sicherheit

OSSwurde 1987 von J.M. Pollard und Claus Schnorr gebrochen.

OT [*Oblivious Transfer*]

Oblivious Transfer (engl.) - unbemerkte/nicht wahrnehmbare Übertragung

Eingangsseite Index Mail

OWF [*One-Way Function*]

One-Way Function (engl.) - Einwegfunktion

OWHF [*One-Way Hash Function*]

One-Way Hash Function (engl.) - Einweg-Hashfunktion

Quantenkryptographie

Quantenkryptographie - (engl.) quantum cryptography(QC)

Die Quantenkryptographieist eine relativ junges Gebiet der Kryptographie, das auf quantenmechanischen Effekten (Unschärferelation) aufbaut.

Erste Ideen dazu stammten von *S. Wiesner* (1970) und wurden 1983 veröffentlicht (S. Wiesner: Conjugate coding. SIGACT News, 15/1983). Andere Arbeiten stammen von C. Bennet und G. Brassard (1983, 1997). Ihren Sinn findet die Quantenkryptographie darin, wirklich abhörsichere Kanäle zu schaffen, in der Hinsicht, daß jedes Abhören bemerkt wird und in der Regel zur Zerstörung der verschlüsselten Nachricht führt.

QC [*Quantum Cryptography*]

Quantum Cryptography (engl.) - Quantenkryptographie

See:quantum cryptography

quantum cryptography

quantum cryptography (engl.) - Quantenkryptographie

See also:QC

Rucksack

Rucksack - (engl.) knapsack, backpack, rucksack

related-key attack

related-key attack (engl.) - Angriff mit verwandtem Schlüssel

replay attack

replay attack (engl.) - Angriff mit Aufzeichnungswiederholung

Dieser Angriff basiert darauf, zu einem Zeitpunkt Aufzeichnungen (*records*) einer Sitzung anzufertigen und diese zu einem späteren Zeitpunkt wieder ``abzuspielen'' (*replay*). Auf dieses Art und Weise kann es dem Angreifergelingen, einen korrekten Sitzungsablauf zu simulieren, wie z.B. eine login-Prozedur.

RC2 [*Rivest Cipher 2*]

RC2 wurde von Ron Rivest entwickelt. Der Algorithmus ist Firmengeheimnis von RSADSI und wurde von dieser nicht offengelegt. Bei RC2 handelt es sich um eine Blockchiffrierung.

Bedeutung

Produkte, die RC2 und RC4 implementieren unterliegen in den USA vereinfachten Ausfuhrverfahren, insofern die Schlüssellänge nicht mehr als 40 Bit beträgt.

Patente

RC2 ist nicht patentiert.

Siehe auch: RC4, RC5

RC4 [*Rivest Cipher 4*]

Rivest Cipher 4 (engl.) - Rivest-Chiffrierung 4

RC4 ist ein Blockchiffrieralgorithmus und wurde von Ron Rivest für die Firma RSADSI entwickelt (1987).

Geschichte

Der Algorithmus war ursprünglich geheim und nur bei Unterzeichnung eines NDA einzusehen. Im Internet wurde 1994 ein Algorithmus veröffentlicht, von dem behauptet wurde, daß er die RC4-Chiffrierung implementieren würde. Benutzer von RC4 erklärten, daß der Algorithmus kompatibel mit dem Original sei. Ob es sich um das Original oder bloß um eine funktional gleichwertige Implementierung handelt, ist bisher ungeklärt - wegen der NDA's.

Bedeutung

Produkte, die RC2 und RC4 implementieren unterliegen in den USA vereinfachten Ausfuhrzulassungsverfahren, insofern die Schlüssellänge nicht mehr als 40 Bit beträgt.

RC4 wird u.a. im Netscape Navigator und in Lotus Notes eingesetzt. Dabei ist die Schlüssellänge allerdings auf 40 Bit begrenzt, wodurch die Chiffrierung relativ leicht gebrochen werden kann. Auch zur Verschlüsselung der Mobilfunkkommunikation wird RC4 verwendet.

Bruce Schneier rät davon ab, RC4 ohne gültige Lizenz einzusetzen ([Schneier 1996], S.456).

Patente

RC4 ist nicht patentiert, wird allerdings als Firmengeheimnis behandelt.

Siehe auch: RC5, RC2

RC5 [*Rivest Cipher 5*]

Rivest Cipher 5 (engl.) - Rivest-Chiffrierung 5

RC5 ist ein Blockchiffrieralgorithmus und wurde von Ron Rivest entwickelt.

Bedeutung

RC5 ist noch relativ neu (vorgestellt 1994).

Im Internet wurde vor kurzem ein 56-Bit RC5-Geheimtext entschlüsselt. Das Resultat: ``*It is time to move to a longer key length*.", lautete der Klartext. Der Aufwand zum Brechen des Geheimtextes war beträchtlich: Im Internet beteiligten sich Computer mit 381.753 verschieden Internet-Adressen (nicht gleichzusetzen mit 831.753 Computern!) an der Brute-Force-Entschlüsselungsaktion. Diese dauerte 212 Tage und es wurden ca. 35 Billiarden Schlüssel ausprobiert (in Zahlen: 35.000.000.000.000.000).

Sicherheit

RC5 ist mit ausreichend langen Schlüsseln allem Anschein nach sehr sicher.

Patente

Das Verfahren ist von RSA Data Security zum Patent angemeldet, der Name RC5 ist geschützt.

Siehe auch: RC4, RC2

RFC [*Request For Comment*]

Request For Comment (engl.) - Bitte um Kommentar

Ein RFC ist ein Papier (im übertragenen Sinne), das von der Internet Engineering Task Force (IETF) mit der Bitte um Kommentar veröffentlicht wird. Ein solches Papier stellt Vorschläge für Standards vor, die im Internet verbindlich werden sollen. Je nach Inhalt der Reaktionen (Kommentare) werden die Vorschläge abgewandelt oder verbindlich erklärt.

RFC-1701 [*Request For Comment No. 1701*]

Request For Comment No. 1701 (engl.) - Bitte um Kommentar, Nr. 1701

In RFC-1701 geht es um ...

Siehe auch: RFC

ROTFL [*Rolling-On-The-Floor-Laughing*]

Rolling-On-The-Floor-Laughing (engl.) - sich vor Lachen auf dem Boden kugeln

ROTFL ist eine der vielen Abkürzungen für Redewendungen, die im Internet entwickelt wurden, um die Bandbreite zu schonen. Bei `ROTFL' werden 5 Bytes übertragen, anstelle von 29 Bytes für `Rolling-On-The-Floor-Laughing'.

RSADSI [*RSA Data Security Inc.*]

RSADSI ist eine amerikanische Firma und ein bedeutender Hersteller von Verschlüsselungssystemen. Die Firma besitzt Rechte an vielen wichtigen Verschlüsselungsalgorithmen, z.B. RC5.

Internet: http://www.rsa.com

Schlüsselgenerierung

Schlüsselgenerierung - (engl.) key generation

Siehe: Schlüsselerzeugung

Schlüsselhinterlegung

Schlüsselhinterlegung - (engl.) key escrow

Der Begriff der Schlüsselhinterlegung wurde vom englischen *key escrow* abgeleitet. Die Geschichte des Begriffes und das entsprechende Verfahren wird auch unter diesem Begriff erläutert.

Pro

Mit der Schlüsselhinterlegung wollen sich die "Dienste der inneren Sicherheit", d.h. Polizei und Geheimdienste, eine Möglichkeit verschaffen, die verschlüsselte Kommunikation von Bürgern und Unternehmen abzuhören. Als Hauptargument gilt ihnen dabei die "international operierende Organisierte Kriminalität" (OK), von der sie behaupten, daß sie das Internet benutzt, um Verbrechen zu organisieren. Damit sie dabei ungestört bleibt, verschlüsselt sie die gesamte Kommunikation.

Kontra

Kritiker wenden dagegen ein, daß eine solche Maßnahme unverhältnismäßig, weil wenig erfolgversprechend wäre: Die Kriminellen, die sich tatsächlich gegen Abhören wollen, lassen sich nicht auf Schlüsselhinterlegung ein. Oder sie verschlüsseln mehrfach, oder sie greifen zu Verfahren der Steganographie, oder ... Jedenfalls werden sie alles unternehmen, um keine Beweise zu hinterlassen, vermutlich erfolgreich.

Andererseits wäre die Kommunikation der Bürger nicht mehr gegen die Aktivitäten bestechlicher, ahnungsloser oder fahrlässiger Schlüsselverwalter gesichert. Sie hätten unter Umständen den Schaden zu tragen. Den Wirtschaftsspionen würde das Leben ebenfalls leichter gemacht. Keine schönen Aussichten.

Realität

In Deutschland gibt es zur Zeit noch keine gesetzlichen Beschränkungen für den Einsatz von Verschlüsselungstechnologie, damit auch keine Schlüsselhinterlegung. Es gibt einige Juristen, die eine solche Beschränkung für verfassungswidrig halten.

Im Signaturgesetz (SigG), dem ersten Gesetz, das sich mit Verschlüsselung auseinandersetzen muß, wurde weitgehend vermieden, von Verschlüsselung zu reden. Ja, der Begriff taucht noch nicht einmal auf. Der Gesetzgeber schweigt sich über das Zustandekommen einer digitalen Signatur aus. Allerdings ist von öffentlichen Schlüsseln und privaten Schlüsseln die Rede! In der amtlichen Begründung zum Signaturgesetz heißt es dann ganz offen:

> "*Die Funktionen Signatur und Verschlüsselung sind technisch wie rechtlich völlig eigenständig zu betrachten.*" [SigGB], Abschnitt V. - Wichtige Einzelaspekte, Wirksamer Informationsschutz

Während die zweite Aussage dieses Satzes streitbar ist, ist die erste offensichtlich falsch. Der Satz gibt insofern den -zweifelhaften- Stand der politischen Überlegungen gut wieder.

Schlüsselübergabe

Schlüsselübergabe - (engl.) key delivery, key transport

Die Schlüsselübergabeist ein notwendiger Vorgang, der vor der Aufnahme einer verschlüsselten Kommunikation vollzogen werden muß. Es lassen sich diverse Varianten vorstellen, wie der (die) Schlüsselübergeben werden. Wichtig ist dabei, daßder Weg, auf dem die Übergabe erfolgt und ggf. die Schlüsselweitergabe innerhalb der vertrauenswürdigen Instanz sicher ist.

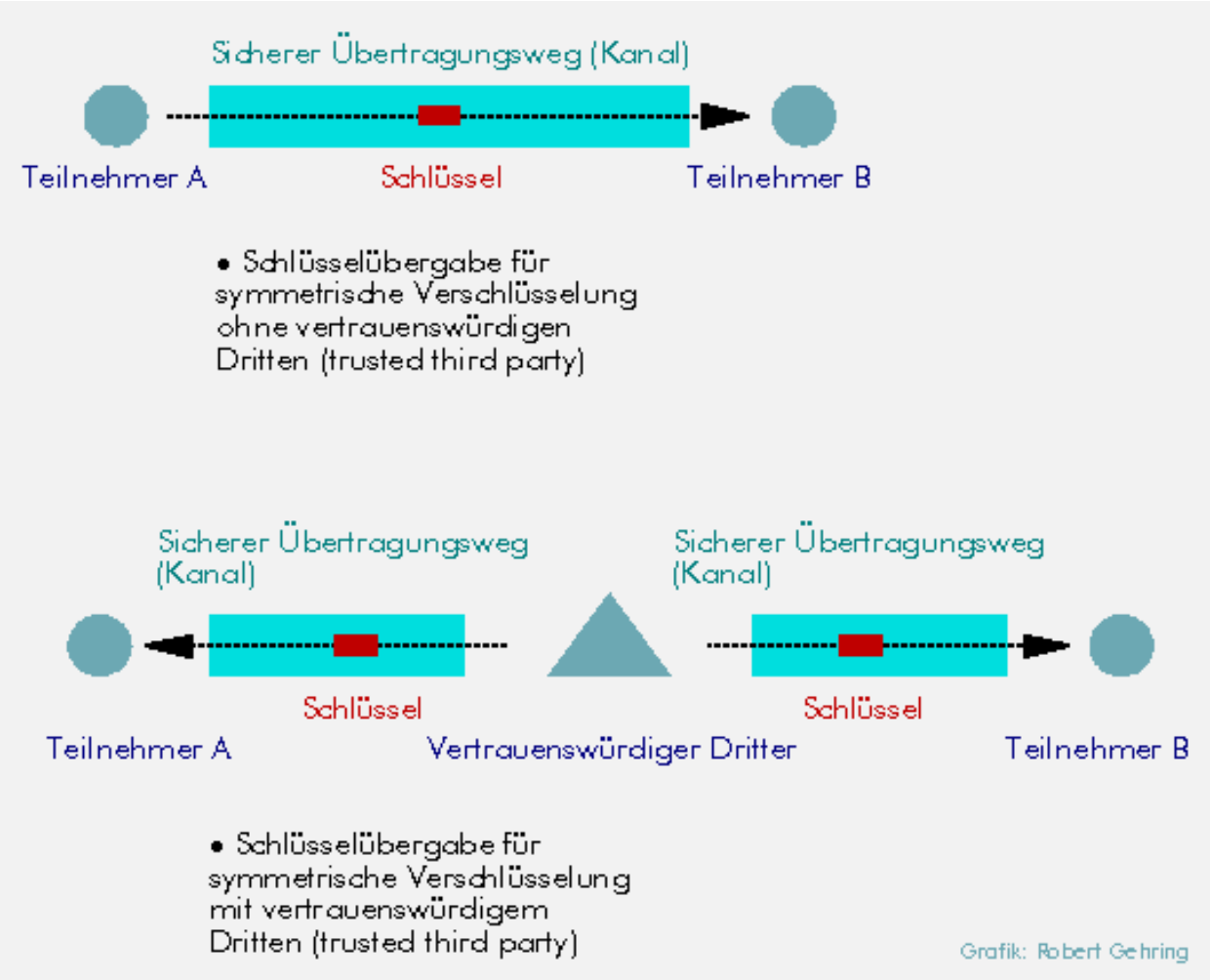
Grundsätzlich können zwei Szenarien unterschieden werden:

1. Schlüsselübergabe bei Kommunikation mit symmetrischer Verschlüsselung (symmetric encryption)
2. Schlüsselübergabe bei Kommunikation mit asymmetrischer Verschlüsselung (public key encryption)

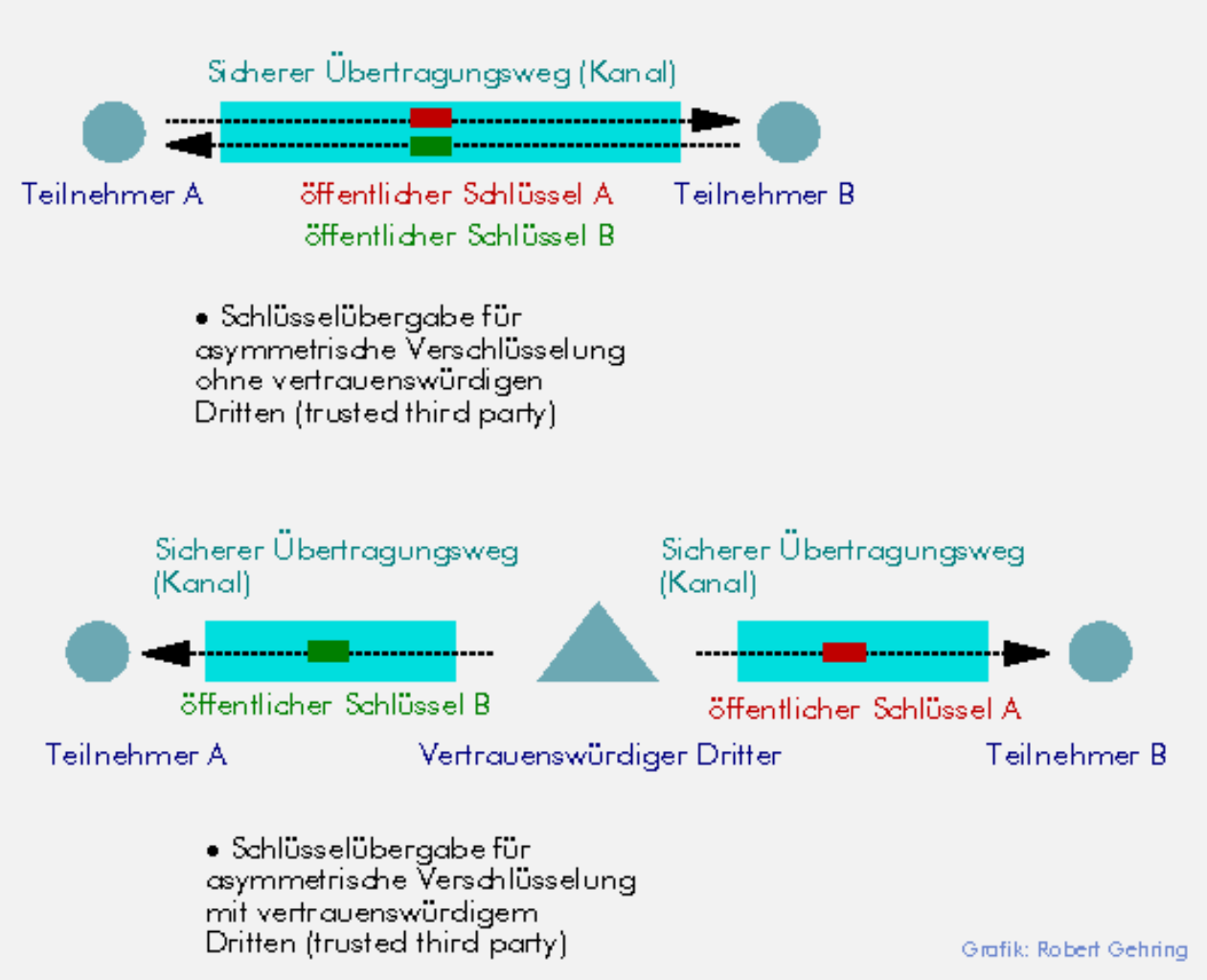
Beide Varianten sind sowohl mit, als auch ohne vertrauenswürdigen Dritten (trusted third party) realisierbar.

Struktur

(1) Schlüsselübergabefür symmetrische Verschlüsselung



(2) Schlüsselübergabefür asymmetrische Verschlüsselung



In diesem Falle wird angenommen, daßder vertrauenswürdige Dritte die öffentlichen Schlüssel lediglich verwaltet, nicht jedoch erzeugt. Auch sollen die geheimen Schlüssel nur den berechtigten Inhabern bekannt sein.

Soll er die Schlüssel nicht bloß verwalten, sondern auch erzeugen, so müßten die zugehörigen geheimen Schlüssel ebenfalls über den sichen Kanal ausgeliefert werden: A bekäme dann seinen eigenen geheimen Schlüssel, seinen öffentlichen Schlüssel und den öffentlichen Schlüssel von B. B erhielte den öffentlichen und den geheimen Schlüssel für B und den öffentlichen Schlüssel von A.

Mit wachsendem Aufwand für die Schlüsselübergabe wird ein darauf aufbauendes System verschlüsselter Kommunikation anfälliger für Fehler und Manipulation.

Siehe auch: Schlüsselverteilung

Schlüsselverteilung

Schlüsselverteilung - (engl.) key distribution, key delivery, key transport

Schlüsselverteilungist ein Synonym für Schlüsselübergabe.

Ist die Rede von größeren Systemen, so wird eher Schlüsselverteilungverwandt. Im kleineren Rahmen spricht man eher von Schlüsselübergabe.

Schlüsselverwaltung

Schlüsselverwaltung - (engl.) key management

Unter der Schlüsselverwaltungfaßt man die Menge aller Handlungen zusammen, die zwischen Schlüsselerzeugungund Schlüsselvernichtungverrichtet werden, um eine sichere verschlüsselte Kommunikation unter Verwendung der Schlüssel zu ermöglichen. Dazu gehören u.a.:

- Schlüsselspeicherung
- Schlüsselübergabe
- Verschlüsselung
- Schlüsselregistrierung
- ggf. Schlüsselwiederherstellung

Schlüsselerzeugungund Schlüsselvernichtunggehören nicht zur Schlüsselverwaltung, da ohne Schlüsselkeine verschlüsselte Kommunikation -auch keine Verwaltung der Schlüssel- möglich ist.

Die Handlungen, die im Rahmen der Schlüsselverwaltung vollzogen werden, lassen sich als Zyklus auffassen: Schlüsselverwaltungszyklus(key management cycle). Im Rahmen größerer Systeme, in denen verschlüsselt kommuniziert wird, werden oft ein oder mehrere Instanzen geschaffen, die große Teile der Schlüsselverwaltungübernehmen. Dazu zählen z.B. auch die sogenannten vertrauenswürdigen Drittenin Systemen mit Public Key-Verschlüsselung.

schwache Verschlüsselung

schwache Verschlüsselung - (engl.) weak encryption

Von schwacher Verschlüsselung spricht man in dem Fall, daß zur Verschlüsselung Verfahren zum Einsatz kommen, die mit *vertretbarem Aufwand* (an Rechenleistung) in *vertretbarer Zeit* ohne Kenntnis des Schlüssels gebrochen werden können.

Die Begriffe *vertretbarer Aufwand* und *vertretbare Zeit* sind sehr relativ und in Abhängigkeit vom jeweiligen Zweck zu deuten.

Siehe auch: starke Verschlüsselung

sicherer Kanal

sicherer Kanal - (engl.) secure channel

Ein sicherer Kanal ist ein Kommunikationsweg, bei dem die Kommunikationspartner sicher sein können, daß niemand außer ihnen Zugriff auf die ausgetauschten Nachrichten hat oder, besser noch, daß niemand von der Kommunikation überhaupt erfährt.

Gibt es noch sichere Kanäle? Wie sich in diesem Jahr zeigte, gibt es jedenfalls genug Politiker, Polizisten, Polemiker und Geheimdienstler, die -aus welchem Grunde auch immer- etwas gegen sichere Kanäle haben. Das `Unter-vier-Augen-Gespräch' kann kaum noch als sicherer Kanal gelten, seit Wanze, Richtmikrofon und großem Lauschangriff ...

Sichere Kanäle können zum offenen Schlüsselaustausch für die Schlüssel zur symmetrischen Verschlüsselung benutzt werden.

Siehe auch: unsicherer Kanal, verdeckter Kanal

SigG [*Signaturgesetz*]

Das Signaturgesetz (SigG, Gesetz zur digitalen Signatur) trat als Artikel 3 des Multimediagesetzes (IuKDG) zum 1. August 1997 in Kraft.

> ``*Zweck des Gesetzes ist es, Rahmenbedingungen für digitale Signaturen zu schaffen, unter denen diese als sicher gelten und Fälschungen digitaler Signaturen oder Verfälschungen von signierten Daten zuverlässig festgestellt werden können.*'' [SigG §1 Abs. 1]

Siehe auch: Verordnung zum Signaturgesetz (SigV)

§§ **Gesetzestext**

SigV [*Verordnung zum Signaturgesetz*]

Siehe auch: Signaturgesetz (SigG)

starke Verschlüsselung

starke Verschlüsselung - (engl.) strong encryption

Unter starker Verschlüsselung versteht man die Verschlüsselungmit kryptographischen Verfahren derart, daßeine Entschlüsselungohne Kenntnis des Schlüssels*praktisch undurchführbar*ist, auch nicht mit sehr schnellen Computern.

Praktisch undurchführbar meint dabei, daß eine Entschlüsselung mit *vertretbarem* technischen und finanziellem Aufwand in *vertretbarer* Zeit nicht möglich ist.

Siehe auch:schwache Verschlüsselung

Steganographie

Steganographie - (engl.) steganography

Steganographie bedeutet soviel, wie verdecktes oder verstecktes Schreiben.

Gemeint ist damit das Verstecken von Informationen in Nachrichten derart, daß niemand, der nicht über zusätzliche Informationen -Schlüsselinformationen- verfügt, Zugang zu den versteckten Informationen erhält, ja diese noch nicht einmal wahrnehmen kann.

Der Begriff der Steganographie ist in letzter Zeit häufiger aufgetaucht. Die zwei wichtigsten Zusammenhänge sind dabei:

- ein mögliches Kryptographieverbot
- die Anbringung von Urheberinformationen an elektronischen Werken.

SECC [*Secret Error Correction Code*]

Seccret Error Correction Code (engl.) - geheimer Code zur Fehlerkorrektur

SECCstammt vom Error Correction Code (ECC) ab und wird zur Fehlerkorrektur bei der Übertragung verschlüsselter Daten über fehleranfällige Leitung verwendet.

secure channel

secure channel (engl.) - sicherer Kanal

SKIP [*Simple Key Management for Internet Protocol*]

Simple Key Management for Internet Protocol (engl.) - Einfache Schlüsselverwaltung für das Internet Protokoll

SKIP wurde von Sunsoft (http://www.sunsoft.com) entwickelt und liegt der IETF als Internet-Draft vor. Es konkurriert als Vorschlag zur Schlüsselverwaltung im Internet direkt mit ISAKMP.

Siehe auch: IP (Internet Protocol)

Skipjack

Skipjack(auch: SKIPJACK) ist der Name des geheimen Verschlüsselungsalgorithmus', der von der NSAin der Clipper-Initiativeentwickelt und in Clipper-Chip(zur Sprachverschlüsselung) und Capstone-Chip(zur Datenverschlüsselung) implementiert wurde.

Geschichte

Die Forschungen, deren Resultat SKIPJACK darstellt, begannen etwa Anfang der 80'er Jahre. 1987 wurde ein erstes Design erstellt, 1993 war der Algorithmus spätestens fertig und getestet.

Sicherheit

Skipjack ist ein `classified' Algorithmus, der von der NSAin Zusammenarbeit mit dem NISTentwickelt wurde. Da er `classified', d.h. nicht öffentlich zugänglich ist, hat eine öffentliche Diskussion zur Sicherheit des Algorithmus bisher nicht stattfinden können. Einer Kommission von Fachleuten, bestehend aus: E. F. Brickell, D. E. Denning, S. T. Kent, D. P. Maher und W. Tuchman, wurde die Möglichkeit gegeben, sich etwa sieben Tage lang mit dem Algorithmus vertraut zu machen und ihn zu testen. Im Ergebnis kamen sie zu dem Schluß, daßder Algorithmus sicher sei:

> *"... there is no significant risk that SKIPJACK will be broken by exhaustive search in the next 30-40 years. There is no significant risk that SKIPJACK can be broken through a shortcut method of attack. ... the strength of SKIPJACK against a cryptanalytic attack does not depend on the secrecy of the algorithm."*[SKIPJACK Review, 28. Juli 1993]

SKIPJACK darf nur in `tamper resistant devices' implementiert werden. Die Schlüsselvergabe der Familienschlüssel, die zur Verschlüsselung des LEAF(Law Enforcement Access Field) verwendet werden, erfolgt zentral durch die Firma "Mykotronx Corporation".

SSL *[Secure Socket Layer]*

secure socket layer (engl.) - sichere Socketschicht

Mit dem `secure socket layer' soll die Kommunikation in TCP/IP-Netzwerken abgesichert werden. SSL ist eine Entwicklung der Firma Netscape, die ursprünglich dafür gedacht war, die Kommunikation von Web-Browsern und Web-Servern im WWW sicherer zu machen.

Einsatz

SSL ist auf Ebene 4 des OSI-Refenzmodelles angesiedelt (Transportschicht) und verschlüsselt somit unabhängig von der konkreten Applikation. SSL wird zwischen TCP (transport control program) und Anwenderprogramm geschaltet, um den Datenfluß ins Netz zu verschlüsseln und den Datenfluß aus dem Netz zu entschlüsseln. Aufgrund der Transparenz der Verschlüsselung, kann SSL im Prinzip mit beliebigen Applikationen eingesetzt werden.

Nachteile

Da die Verschlüsselung unterhalb des Anwenderprogrammes angesiedelt wird, ist es möglich, die Daten zu manipulieren. Wenn zum Beispiel Daten durch Programme, die auf der Ebene 7 des OSI-Modelles arbeiten (Anwendungsschicht), ausgewertet werden müssen, liegen sie entschlüsselt vor und sind somit ungeschützt.

Emails durchlaufen beispielsweise Gateways, die für ihre Verteilung zuständig sind. Ein Gateway, das auf OSI-Ebene 7 arbeitet, bekommt die Email im Klartext, stellt somit einen Angriffspunkt dar. Daten können dort gelesen und ggf. verfälscht werden.

Wirklich sichere Kommunikation mit SSL ist also nur durch zusätzliche Verschlüsselung vor dem Übergang von der Anwendungsschicht zur Transportschicht möglich. Bei Email könnte dazu z.B. PGP eingesetzt werden.

steganography

steganography (engl.) - Steganographie

stream cipher

stream cipher (engl.) - Stromchiffrierung

stream encryption scheme

stream encryption scheme (engl.) - Stromverschlüsselungsverfahren, Stromverschlüsselung

Anmerkung: Der Ausdruck stream encryption scheme ist in der Literatur sehr ungebräuchlich. Häufig findet man statt dessen stream cipher.

Siehe auch: block encryption scheme

strong encryption

strong encryption (engl.) - starke Verschlüsselung

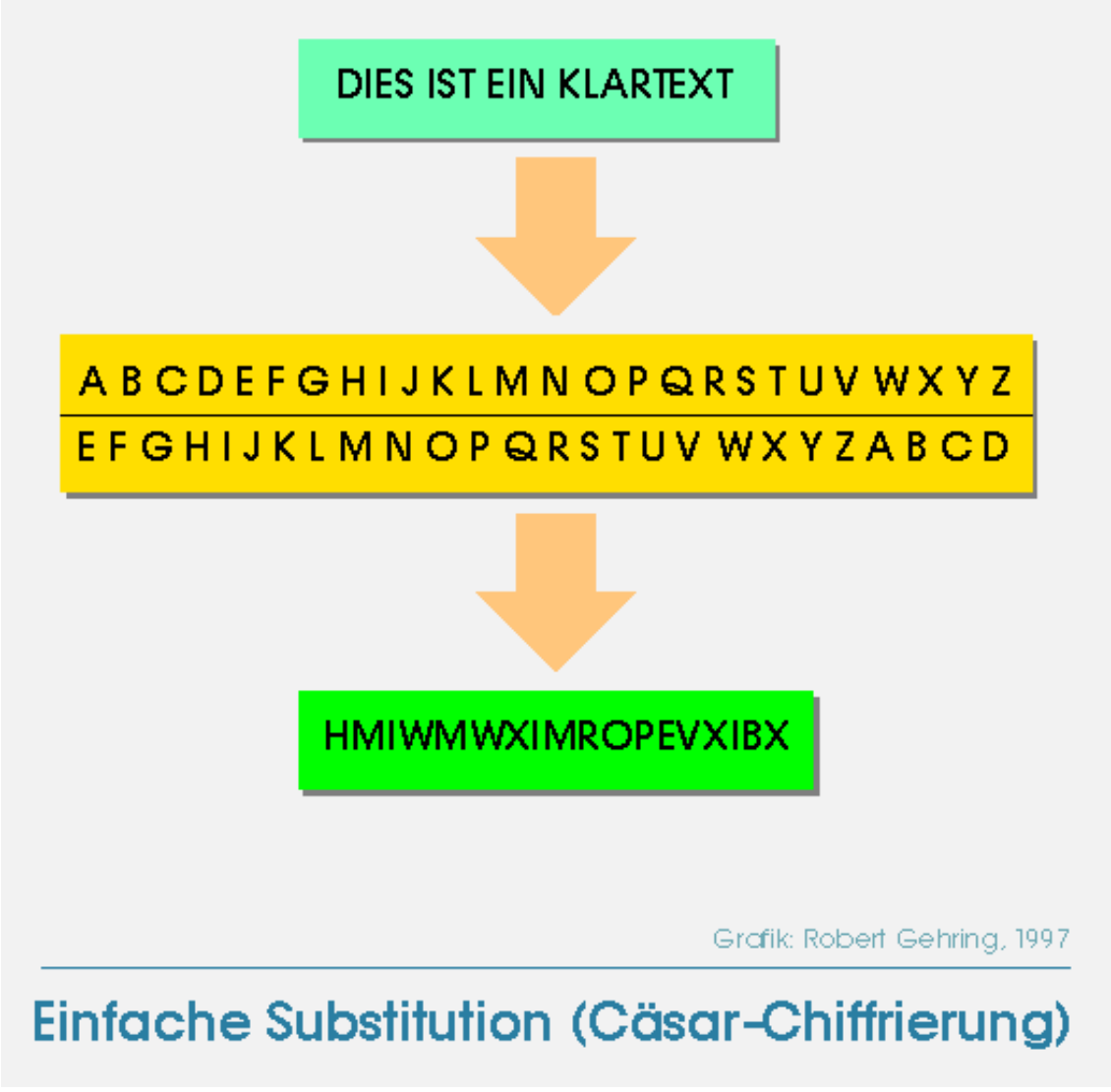
Siehe auch: schwache Verschlüsselung

Substitution

Substitution - (engl.) substitution

Substitution bedeutet Ersetzung. Im Falle der Kryptographie ist die nichtwillkürliche Ersetzung von Zeichen des Klartextes durch andere Zeichen gemeint, wodurch ein Geheimtext entsteht. Ist das Substitutionsverfahren bekannt, kann aus dem Geheimtext der Klartext rekonstruiert werden.

Eine einfache Substition hat folgendes Schema:



Im Falle der sogenannten Cäsar-Chiffrierung (benannt nach Julius Cäsar) wird jeder Buchstabe durch einen anderen Buchstaben im Alphabet ersetzt. Der Abstand zwischen diesen Buchstaben wird als Schrittweite bezeichnet. Im Falle der Grafik ist die Schrittweite 4, d.h. jeder Buchstabe des Klartextes wird durch den Buchstaben ersetzt, der im Alphabet vier Stellen weiter zu finden ist. Die Stellung der Zeichen im Geheimtext bleibt unverändert, allerdings werden in der Regel Wortzwischenräume und Interpunktionen unterdrückt.

Substitutionen allein sind nicht sehr sicher, da anhand statistischer Untersuchungen leicht herauszufinden ist, welche Zeichen im Geheimtext mit welchen Zeichen einer Sprache korrespondieren.

Siehe auch: Transposition

Eingangsseite Index Mail
digitale signaturen diplomarbeit · robert gehring

symmetric cipher

symmetric cipher (engl.) - symmetrische Verschlüsselung

symmetric cryptosystem

symmetric cryptosystem (engl.) - symmetrisches Verschlüsselungssystem, symmetrisches Verschlüsselungsverfahren

symmetric encryption

symmetric encryption (engl.) - symmetrische Verschlüsselung

symmetric encryption algorithm

symmetric encryption algorithm (engl.) - symmetrisches Verschlüsselungsverfahren, symmetrischer Verschlüsselungsalgorithmus

StPO [*Strafprozeßordnung*]

Strafprozeßordnung - (engl.) Code of Criminal Procedure

Die Strafprozeßordnung (vom 1. Februar 1877, in der Fassung vom 7. April 1987) enthält die wesentlichenTeile des Strafprozeßrechtes.

Sie legt fest, wie *Ermittlungsverfahren*, *Eröffnungsverfahren*, *Hauptverfahren*, *Rechtsmittelverfahren* und *Vollstreckungsverfahren* formell abzulaufen haben.

In der StPO sind die Abhörbefugnisse der Ermittlungsbehörden und der Strafverfolgungsbehörden festgeschrieben.

Stromverschlüsselung

Stromverschlüsselung - (engl.) stream cipher, stream encryption

Unter Stromverschlüsselung versteht man die Verschlüsselung eines Klartextes mittels eines Stromverschlüsselungsverfahrens. Im Gegensatz zur Blockverschlüsselung werden die Daten des Klartextes (Buchstaben, Bits) bei einer Stromverschlüsselung einzeln verschlüsselt.

Siehe auch: Blockverschlüsselung, Stromchiffrierung

Stromverschlüsselungsalgorithmus

Stromverschlüsselungsalgorithmus - (engl.) block encryption algorithm, block cipher

Ein Stromverschlüsselungsalgorithmus ist mathematisch gesehen eine Funktion, die einzelne Daten (Zeichen, Bits) eines Klartextes auf einzelne Daten eines Geheimtextes abbildet. Der Klartext stellt das Urbild dar und der Geheimtext das Abbild.

Die besondere Qualität der Funktion besteht darin, daß aus dem Abbild nicht ohne weiteres auf das Urbild geschlossen werden kann, d.h. dem Geheimtext ist nicht anzusehen, von welchem Klartext er abstammt.

Die Informationsmenge, die im Geheimtext enthalten ist, muß dabei der Informationsmenge des Klartextes entsprechen. Ist die Informationsmenge des Geheimtextes geringer, so wurde der Klartext komprimiert und man spricht von einer Einweg-Hashfunktion.

Werden nicht einzelne Daten, sondern Blöcke von Daten abgebildet, spricht man von einem Blockverschlüsselungsalgorithmus.

Siehe auch: Blockverschlüsselungsalgorithmus

Stromverschlüsselungsverfahren

Stromverschlüsselungsverfahren - (engl.) stream cipher, stream encryption scheme

Bei einem Stromverschlüsselungsverfahrenwird die zu verschlüsselnde Nachrichtals Strom einzelner Zeichen aufgefaßt, die kontinuierlich verschlüsselt werden. Bei einem Text wird dann jeder Buchstabe einzeln verschlüsselt.

Siehe auch: Blockverschlüsselungsverfahren

symmetric encryption scheme

symmetric encryption scheme (engl.) - symmetrisches Verschlüsselungsverfahren

Tessera-Karte

Die Fortezza-Karteheißzuerst Tessera-Karte. Da dieser Name aber geschützt ist, wie sich herausstellte, wurde sie umbenannt.

Siehe auch: Tessera

Transposition

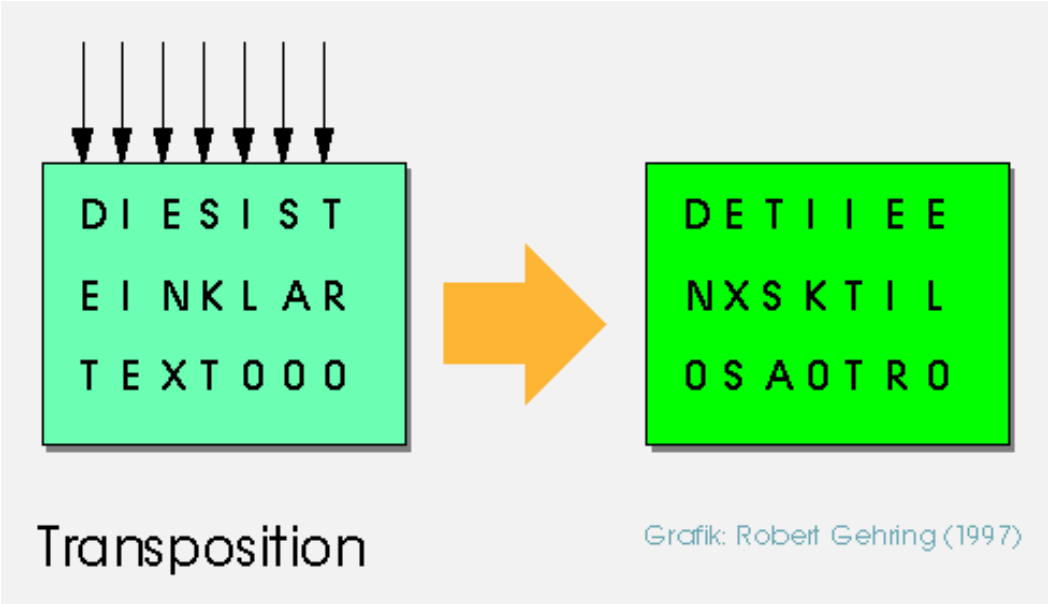
Transposition - (engl.) transposition

Transposition bedeutet Stellentausch. Dabei werden die Zeichen des Klartextes an eine andere Stelle umgesetzt, bleiben aber ansonsten unverändert.

Beispiel

Der Klartext wird mit definierter Breite fortlaufend untereinandergeschrieben. Leerzeichen werden weggelassen, Punkte und Kommata ebenso. Fehlende Zeichen werden durch eine 0 ersetzt. Anschließend wird er von oben nach unten gelesen und das Resultat aufgeschrieben, ebenfalls mit definierter Breite.

Damit wird z.B. aus dem Klartext "DIES IST EIN KLARTEXT" der Geheimtext "DETIIEENXSKTIL0SA0TR0" (von links nach rechts, von oben nach unten gelesen).



Zur Entschlüsselung muß in umgekehrter Reihenfolge vorgegangen werden. Die Methode wurde historisch gesehen oft verwendet, ist aber nicht besonders sicher.

Siehe auch: Substitution

TWG [*Telegrafenwegegesetz*]

Telegrafenwegegesetz - (engl.) ???

Im Telegrafenwegegesetz wurde zu Zeiten der Monopolstellung der Bundespost im Telekommunikationssektor deren Recht, Leitungen auf öffentlichen Wegen zu verlegen, geregelt. Mit der Vollständigen Liberalisierung des Telekommunikationsmarktes zum 1. Januer 1998 wird das TWG ungültig.

Siehe auch: TKG

tamper

tamper (engl.) - an *etwas* herumbasteln, rumspielen mit *etwas*, sich an *etwas* zu schaffen machen

Siehe auch: tamper resistance, tamper-proof

tamper-proof

tamper-proof (engl.) - vor [*unerlaubtem*] Zugriff gesichert, einbruchssicher

Siehe auch: tamper, tamper resistance

tamper proof device

tamper proof device (engl.) - gegen (unerlaubten) Zugriff gesichertes Gerät

Als tamper proof device(tamper resistant device) werden Geräte, auch Bauteile u.ä., bezeichnet, die in dem Falle zerstört werden, daßjemand versucht, ihr `Innenleben' zu erkunden. Gelingt es, solch ein Gerät, z.B. den Capstone-Chip, zu öffnen, soll dabei wenigstens die relevante Information -im Capstone-Fall: der Algorithmus (SKIPJACK)- verloren gehen.

In den vergangenen Jahren hat sich immer wieder gezeigt, daß das Attribut `tamper proof' mit Vorsicht zu genießen ist. Viele Systeme, die damit bezeichnet wurden, wurden trotzdem geknackt. Oft ist es nur eine Frage der Investitionen an Zeit, Geld und Knowhow. So wurden alle bisher eingeführten Ver-/Entschlüsselungskarten für's digitale Fernsehen in -vom Standpunkt des Kryptologen aus betrachtet- kurzer Zeit überwunden. Gerüchteweise wurde in den USA auch ein Exemplar des Capstone-Chips bereits geknackt, allerdings in den militärischen Sandia-Laboratories.

tamper resistance

tamper resistance (engl.) - Widerstandsfähigkeit gegen unerlaubte Eingriffe

Siehe auch: tamper, tamper proof

tamper resistant device

tamper resistant device (engl.) - Gegen (unerlaubte) Eingriffe gesichertes Gerät

Siehe auch:tamper, tamper proof, tamper resistant, tamper proof device

tap

tap (engl.) - abhören

Tessera

Tesserawar der alte Name für die PC-Card, die jetzt Fortezza cardheißt.

Siehe auch: Tessera-Karte

Tessera card

Tessera card (engl.) - Tessera-Karte

trusted third instance

trusted third instance (engl.) - glaubwürdige dritte Instanz, glaubwürdiger Dritter

Siehe auch:trusted third party(TTP)

tunneling

tunneling (engl.) - untertunneln

Eine glückliche Übersetzung für tunneling läßt sich nicht finden. Gemeint ist mit dem Wort die Einkapselung eines Kommunikationsprotokolles in ein anderes. So lassen sich proprietäre Protokolle mit verfügbarer Technologie abwickeln.

Eine bekannte Variante des tunneling ist das IP-Tunneling.

unsicherer Kanal

unsicherer Kanal - (engl.) insecure channel

Ein unsicherer Kanal ist ein unsicherer Kommunikationsweg, d.h. ein Kommunikationsweg, bei dem nicht sichergestellt werden kann, daß nur die Kommunikationspartner Kenntnis von der Kommunikation erhalten, bzw. Zugriff auf den Kommunikationsinhalt haben.

Beispiele

- Der Postweg ist unsicher, da nicht feststeht, wer eine Postsendung in die Hand bekommt. Per Gesetz und ggf. richterlicher Ermächtigung haben auch Geheimdienste und Polizei Zugriff auf Postsendungen.
- Telefonleitungen sind unsicher, da sie gesetzlich und somit berechtigt, wie auch ungesetzlich und unberechtigt angezapft werden können.
- Gespräche unter vier Augen sind spätestens seit dem Gesetz für den "Großen Lauschangriff" unsicher. Wanzen zum Abhören gab es allerdings schon vorher. Nur durften sie nicht rechtmäßig in Wohnungen eingesetz werden.
- Das Internet ist unsicher, da aller Daten, die übermittelt werden, irgendwo zwischengespeichert werden. Und wie soll man wissen, wer dabei "lauscht"?

Folgende Risiken existieren bei der Kommunikation über unsichere Kanäle:

Abhören	Nachrichten, die über unsichere Kanäle ausgetauscht werden, können abgehört werden. Der oder die Lauscher können so an Informationen gelangen, mit denen sie den Kommunikationspartnern schaden können, bzw. aus denen sie einen Vorteil schlagen können. Viele große Konzerne wären wohl wenig erfreut, wenn die Konstruktionspläne für die neueste Produktreihe in die Hände der Konkurrenz gelangen würden.
Zurückhalten	Nachrichten können abgefangen werden und später oder gar nicht weitergeleitet werden. Wie wäre es beispielsweise mit den Überweisungsaufträgen für Gehaltszahlungen der BFA?

Fälschen	Nachrichteninhalte können verfälscht oder komplett gefälscht werden. Der Empfänger kann so zu bestimmten Aktionen provoziert werden. Eine solche Aktion könnte beispielsweise die Amputation der falschen Hand sein, wenn eine Patientenakte gefälscht wird.
Stören	Die Weiterleitung der Nachrichten kann gestört werden. Man stelle sich vor, was geschieht, wenn der Funkverkehr der Luftüberwachung gestört wird.
Offenlegung	Geheime Informationen können veröffentlicht und somit im besten Falle wertlos gemacht werden. Im schlimmsten Falle werden viele Menschen großen Gefahren ausgesetzt. Es wird viel von sogenannten `Cyberterroristen' geredet und geschrieben. Angenommen, eine Handvoll von diesen gelangt an die Pläne der Installationen zentraler Schaltanlagen der Bundesbahn, wiel diese von einem frustrierten ehemaligen Bahnangestellten im Internet veröffentlicht wurden. Und angenommen, ein paar Signale werden falsch gestellt ...

Siehe auch: sicherer Kanal

UDSA [*Utah Digital Signature Act*]

Der US-Bundesstaat Utah verabschiedete unter der Bezeichnung `Utah Digital Signature Act' (UDSA) ein Gesetz zu Digitalen Signaturen, das am 1. Mai 1995 in Kraft trat. Weitere Bundestaaten sind diesem Beispiel bereits gefolgt (Kalifornien, Georgia, ...).

Bestimmung

Ziel des Gesetzes ist es (Zitat):

> "46-3-102 Purposes and construction.
>
> - to minimize the incidence of forged digital signatures and enable the reliable authentication of computer-based information;
> - to minimize the incidence of forged digital signatures and enable the reliable authentication of computer-based information;
> - to enable and foster the verification of digital signatures on computer-based documents;
> - to facilitate commerce by means of computerized communications; and
> - to give legal effect to the general import of the following and other similar standards ... "

Im Gegensatz zum deutschen Signaturgesetz (SigG) wird nicht versucht, eine künstliche Unterscheidung zwischen digitalen Signaturen auf der einen und Verschlüsselung auf der anderen Seite zu ziehen. Es wird im Gegenteil ganz klar ausgesprochen, daß es bei Digitalen Signaturen um Verschlüsselung geht:

> "46-3-103 Definitions.
>
> 2. `Asymmetric Cryptosystem' means a computer algorithm or a series of algorithms which utilize two different keys with the following characteristics:
>
> (a) one key encrypts a given message;
> (b) one key decrypts a given message; and
> (c) the keys have the property that, knowing one key, it is computationally infeasible to discover the other key."

Inhalt

Der UDSA enthält konkrete Begriffsdefinitionen (siehe oben), Anwendungsregeln, Aussagen über die Risikoverteilung, Zertifizierungsrichtlinien u.a.m.

user profile

user profile (engl.) - Benutzerprofil, Nutzerprofil

verdeckter Kanal

verdeckter Kanal - (engl.) subliminal channel

Ein verdeckter Kanalist ein Kommunikationsweg, dessen Existenz nicht offensichtlich ist. Dabei gibt es die Einschränkung, daßdie übertragbare Informationsmenge sehr gering ist.

Die verdeckten Kanäle, sind nur bei Kenntnis spezifischer Schlüsselinformationen zugänglich. Insofern funktionieren verdeckte Kanäle ähnlich wie Steganographie.

Verdeckte Kanäle lassen sich bei digitalen Signaturen in den Signaturen einrichten. Das ist insofern gefährlich, als sich darüber Teile des geheimen Schlüssels (private key) stückweise übertragen lassen, ohne daß es der Benutzer erfährt.

Siehe auch:geheimer Kanal(secret channel)

Verschlüsselungsalgorithmus

Verschlüsselungsalgorithmus - (engl.) encryption algorithm, cipher, encryption scheme

Ein Verschlüsselungsalgorithmusist das Kernstück jedes Verschlüsselungsverfahrens. Oft werden die Begriffe synonym verwendet, was aber eigentlich nicht ganz korrekt ist.

Typen

Man unterscheidet:

- Blockverschlüsselungsalgorithmen
- Stromverschlüsselungsalgorithmen

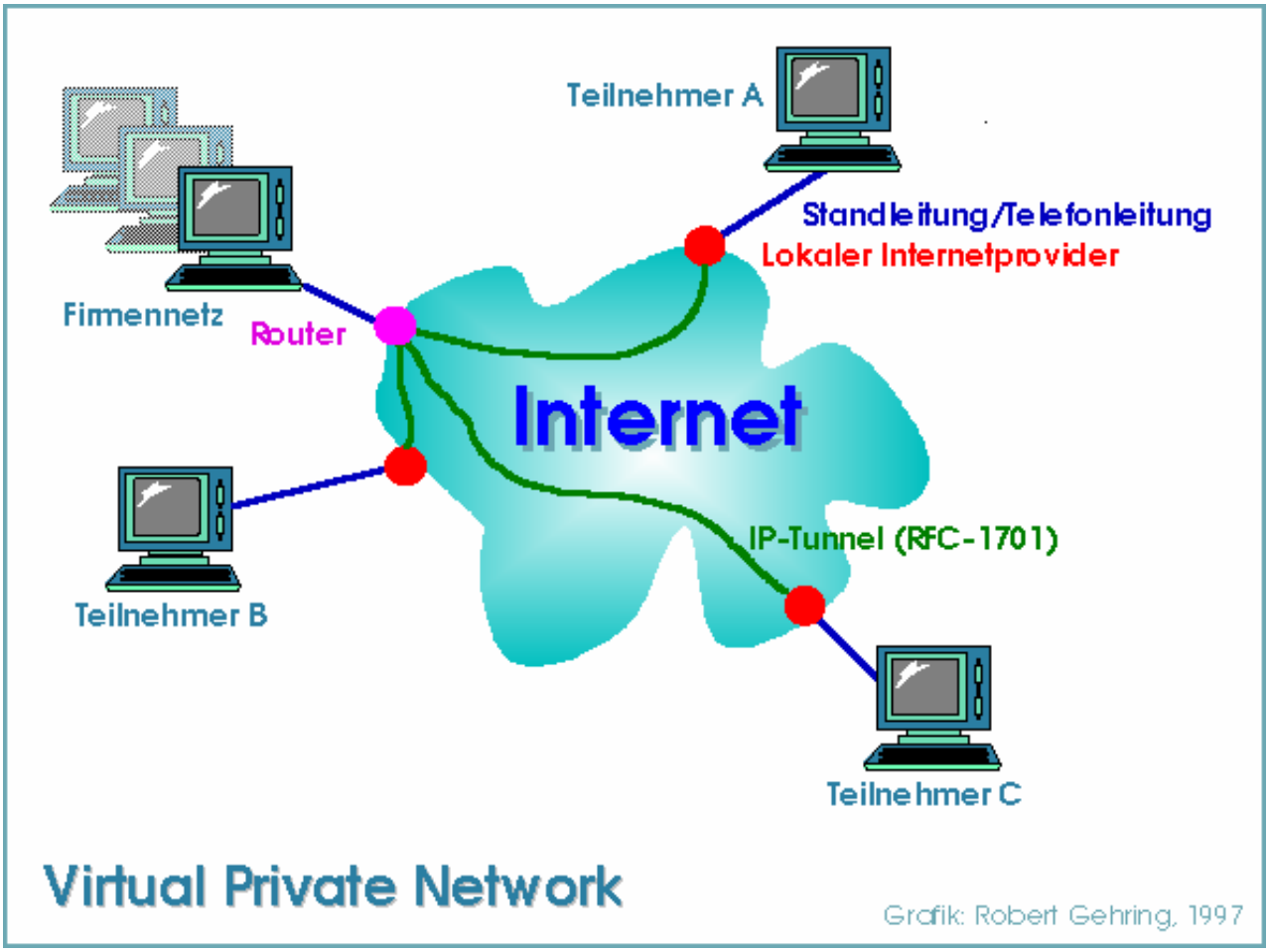
Man beachte, daßnicht zwischen symmetrischen oder asymmetrischen *Verschlüsselungsalgorithmen*zu unterscheiden ist, sondern zwischen symmetrischen oder asymmetrischen *Verschlüsselungsverfahren*. Zu einem *Verschlüsselungsverfahren* gehören die Algorithmen sowohl für die Verschlüsselung, als auch für die Entschlüsselung.

Virtuelles Privates Netzwerk

Virtuelles Privates Netzwerk - (engl.) Virtual Private Network (VPN)

Virtuelle Private Netzwerke wurden zur Vereinfachung der Datenverarbeitung in Unternehmen mit einer großen Anzahl dezentraler Computerarbeitsplätze entwickelt (Telearbeit, Außendienst, Zweigstellen).

Schema eines Virtuellen Privaten Netzwerkes



Die externen Computerarbeitsplätze und das Firmennetz werden mittels bewährter Internettechnologie an einen lokalen Internetprovider angeschlossen. Das Firmennetz und der Prvider sind in der Regel mit Routern ans Internet angebunden.

Je nach Datenaufkommen, bedient man sich einer Standleitung oder der Datenübertragung mit dem Modem. Zunehmend werden auch Richtfunkverbindungen interessant. Der liberalisierte Markt für Telekommunikationsdienstleistungen macht's

möglich.

Der Datenverkehr wird durch die TCP/IP-Protokolle gesteuert. Für nahezu jedes Betriebssystem gibt es inzwischen entsprechende Implementierungen. Die Standardisierung durch die IETF (Internet Engineering Task Force) garantiert Kompatibilität.

Zwischen dem lokalen Provider und dem Übergang ins firmeninterne Netz wird die IP-Tunneling-Technik eingesetzt. Damit wird der Datenverkehr gegen das Internet als Transportmedium abgeschottet. Die Teilnehmer am Virtuellen Privaten Netzwerk erhalten keinen Zugriff auf das Internet, die Internet-Teilnehmer bekommen keinen Einblick in die Firmendatenverarbeitung. Die Sicherheit der Kommunikation kannn dabei durch Verschlüsselung erhöht werden.

Die Auswahl der IP-Adressen erfolgt aus der Menge derjenigen Adressen, die speziell für solche Zwecke vorgesehen sind (RFC-1597, RFC-1918). Diese Adressen werden nicht an Provider vergeben und können deshalb in lokalen Netzen beliebig eingesetzt werden.

Gegenüber dem lokalen Provider identifizieren sich die VPN-Teilnehmer mit einem Paßwort und einer Benutzerkennung. So wird sichergestellt, daß nur autorisierte Personen ins Virtuelle Private Netz gelangen. Dies ist bei allen Providern möglich, die am Aufbau des VPN beteiligt sind. Die Teilnehmer sind deshalb nicht an einen bestimmten Provider gebunden, was ein großer Vorteil für Außendienstmitarbeiter ist.

Vorteile

1. Die eingesetzte Internettechnologie ist preiswert, bewährt und systemunabhängig.
2. Die Datenübertragung in das und aus dem Internet kann zum Ortstarif erfolgen. Innerhalb des Internets lassen sich Daten deutlich kostengünstiger übertragen, als über teure Mietleitungen.
3. Internetzugänge sind fast überall verfügbar, insofern eine Telefonleitung existiert.
4. Die Datenverarbeit wird auf eine einheitliche Basis gestellt.

VPN [*Virtual Private Network*]

Virtual Private Network (engl.) - scheinbar privates Netzwerk

Der Begriff Virtual Private Network ist noch ziemlich neu. Ein allgemein akzeptiertes, deutsches Pendant existiert bisher noch nicht, man findet jedoch zunehmend die einfache Übersetzung Virtuelles Privates Netzwerk.

Glossar Digitale Signaturen

Wanze

Wanze - (engl.) bug

Wanze ist die umgangssprachliche Bezeichnung für ein Abhörmikrofon kleiner Bauart, das unbemerkt in der Nähe von Personen plaziert wird, die abgehört werden sollen.

Es gibt verschiedene Möglichkeiten, das Abhören mittels Wanzen zu unterbinden:

Zerstören

Wenn man die Wanze ausfindig machen kann, tritt man einfach drauf. Oder man nimmt Hammer, Schraubstock, Zange, ...

Orte, an denen Wanzen (tatsächlich, sowie in Filmen und Romanen) gerne versteckt werden:

- Steckdosen (wegen der problemlosen Energieversorgung)
- Unterseite von Tischplatten
- Stehlampen, Lampen überhaupt
- Radios, Recorder, Lautsprecher, ... (wo sie schwer zu identifizieren sind)
- Zimmerpflanzen
- Gardinen, Vorhänge

Diese Methode dürfte legal sein, selbst wenn es sich um eine `offizielle' Wanze handelt. Wer Illegales tut könnte jedoch, wenn er dabei erwischt wird, unter Umständen eine Rechnung für die zerstörte Wanze zugestellt bekommen.

[**Frage:** *Weiß jemand von einem solchen Fall zu berichten?*]

Stören

Man verwendet während der Unterhaltung einen Sender, der mit hoher Leistung auf vielen Frequenzen (insbesondere im Kurzwellen- und Ultrakurzwellenbereich) sendet und die Übertragung der Funksignale der Wanze (leider auch Nachbars Radio) stört.

Solche Störsender sind allerdings illegal und man hat damit zu rechnen, daß die Telekom mit Peilwagen auf Suche nach dem Störer geht.

(**Siehe:** Fernmeldeanlagengesetz §19 Absatz 2)

Schweigen	Eine alte, auch alte kryptographische Weisheit lautet: *Reden ist Silber, Schweigen ist Gold.* Wo nicht geredet wird, kann nicht abgehört werden.
Spazierengehen	Man kann sich an einer einsamen, übersichtlichen Stelle verabreden. Dort hat man Ruhe vor Wanzen. (Nicht unbedingt vor Richtmikrofonen!)

Politik

Aktualität gewinnt das Thema durch den im Winter 1998 von der CDU/CSU/FDP/SPD-Buntagsmehrheit beschlossenen ``*großen Lauschangriff*''. Gegen diese Einschränkung des Grundgesetzes votierten (als Parteien) lediglich die Grünen/Bündnis 90 und die PDS.

Im Ergebnis dessen wurde das Grundgesetz geändert, das bisher die Unverletzlichkeit der Wohnung als ein Bürgerrecht garantierte. Von nun an ist es per (Grund-)Gesetz zulässig, die Wohnungen von Bürgern mit Wanzen auszustatten, insofern diese im Verdacht stehen, ein Verbrechen verübt zu haben oder verüben zu wollen. Es darf ebenfalls verwanzt werden, wenn vermutet werden kann, daß sich in den Räumen in Zukunft jemand aufhalten könnte, der verdächtig ist, ein Verbrechen verübt zu haben oder solches zu planen. Für welche Verbrechen das gilt, wird in einem Gesetz geregelt, über das der Bundestag mit einfacher Mehrheit beschließt und das mit einfacher Mehrheit der jeweiligen Regierungskoalition geändert werden kann.

Die Entscheidung über die Anordnung eines ``*großen Lauschangriffes*'' trifft in der Regel ein Gremium von drei Richtern.

Ausdrücklich vom ``*großen Lauschangriff*'' verschont bleiben allein die Abgeordneten, haben sie beschlossen.

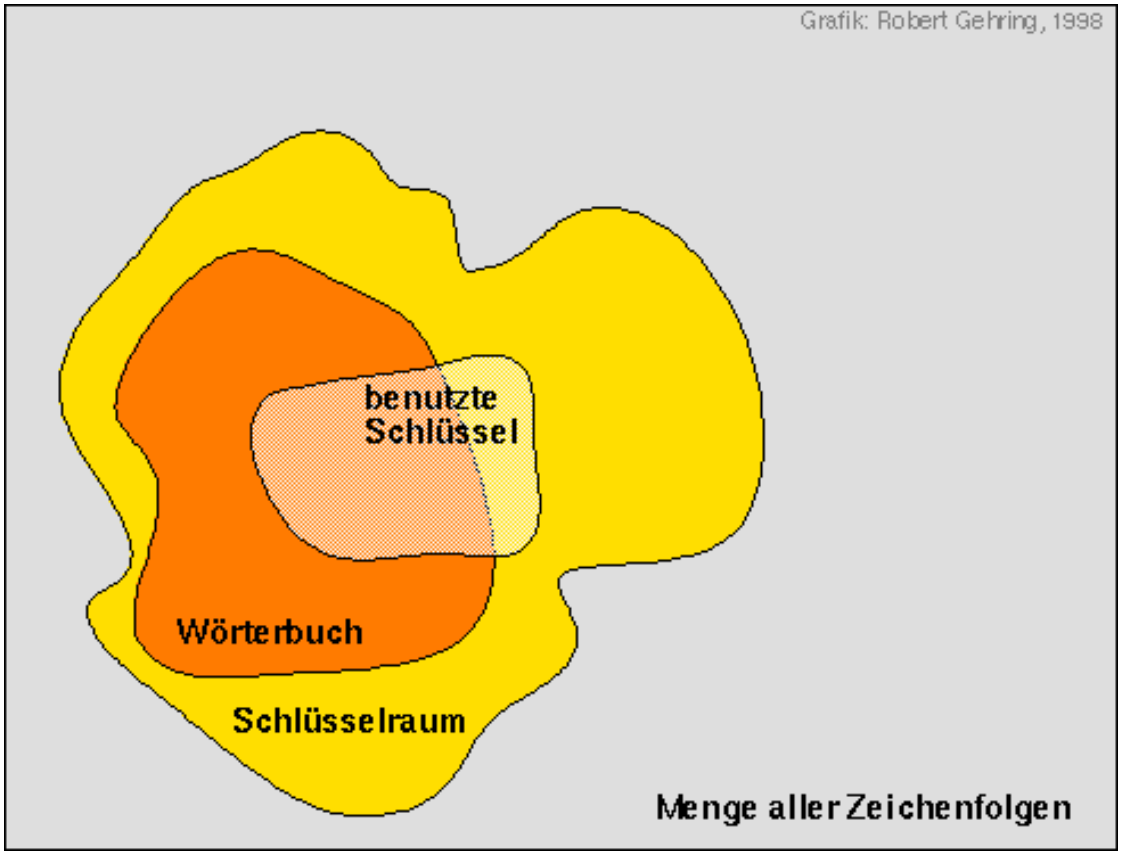
Inwiefern Pfarrer, Ärzte, Anwälte und Journalisten ebenfalls vor einem Belauschen sicher sein können, ist noch umstritten und gesetzlich noch nicht eindeutig geregelt.

Wörterbuchangriff

Wörterbuchangriff - (engl.) dictionary attack

Ein Wörterbuchangriffist eine simpler, aber in manchen Fälle sehr effektiver kryptographischer Angriff. Gegenüber einem Brute Force-Angriff(exhaustive Suche) wird der Schlüsselraumzur Suche eingeschränkt. Dazu benötigt man Kenntnisse über die Qualität der Schlüssel.

Sehr wirkungsvoll ist ein Wörterbuchangriff bei Verfahren mit Paßwörtern. Da nur wenige Leute in der Lage sind, sich kryptische Zeichenfolgen zu merken, wählen sie in der Regel Wörter, die sie sich gut merken können. In etwa zwei Dritteln aller Fälle gelangt man durch Ausprobieren von Wörtern aus umfangreichen Wörterbüchern und Variieren an das Paßwort.



weak encryption

weak encryption (engl.) - schwache Verschlüsselung

Siehe auch: starke Verschlüsselung

Yuval's birthday attack

Yuval's birthday attack (engl.) - Yuvals Geburtstagsangriff

Yuval's birthday attack ist ein Spezialfall einer birthday attack.

Ziel dieses Angriffs ist es, eine falsche Nachricht mit korrekter digitaler Signatur unterzuschieben. Dazu nimmt man die richtige Nachricht sowie die falsche und modifiziert sie ein wenig. Anschließend ermittelt man den Ausgabewert der verwendeten Einweghashfunktion. Die Hashwerte werden verglichen und ein gleicher Hashwert gesucht. Anstelle der richtigen Nachricht kann dann die falsche übermittelt werden.

Auf Grund statistischer Eigenschaften wird man irgendwann einen Treffer landen. Es kann aber unter Umständen sehr lange dauern, so daß die untergeschobene Nachricht dann bereits uninteressant ist.

Zahlentheorie

Zahlentheorie - (engl.) number theory

Die Zahlentheorie ist ein Gebiet der Mathematik, daß sich speziell mit den Eigenschaften der ganzen Zahlen beschäftigt.

Das Interesse daran hat im Zusammenhang mit asymmetrischen Verschlüsselungsverfahren stark zugenommen, da diese in der Regl auf zahlentheoretischen Überlegungen basieren. So ist die Sicherheit von RSA auf dem Faktorisierungsproblem aufgebaut.

Zahlkörpersieb

Zahlkörpersieb - (engl.) Number Field Sieve (NFS)

Das Zahlkörpersieb ist das schnellste Verfahren zur Faktorisierung von Zahlen mit mehr als 110 Dezimalstellen.

zertifizieren

zertifizieren - (engl.) certify

...

Zertifizierungsinstanz

Zertifizierungsinstanz - (engl.) certification instance

Siehe auch: Zertifizierungsstelle

Zertifizierungsstelle

Zertifizierungsstelle - (engl.) certification authority

Siehe auch: Zertifizierungsinstanz

Zertifizierungsstruktur

Zertifizierungsstruktur - (engl.) certification structure

chosen-ciphertext attack

chosen-ciphertext attack (engl.) - Geheimtextangriff mit gewähltem Geheimtext

Enigma

enigma (lat.) - Geheimnis

Enigmawar der Name der wichtigsten deutschen Verschlüsselungsmaschine im zweiten Weltkrieg.

Das Brechen der Enigma-Verschlüsselung wird von manchen Experten als besonders wichtig für den Sieg der Alliierten über Hitler-Deutschland angesehen. Maßgeblich daran beteiligt waren die polnischen Mathematiker *Marian Rejewski*, *Hendrik Zygalski* und *Jerzy Roczycki*, sowie der englische Mathematiker (und Informatiker) *Alan Turing*. [Kippenhahn 1997] Die Brechnung der Enigma erfolgte im Rahmen des Projektes ``ULTRA" in Bletchley Park, nördlich von London.

ULTRA

ULTRAwar der Codename des Projektes zur Brechnung des Codes der deutschen Verschlüsselungsamaschine ``Enigma'' im zweiten Weltkrieg.

Dechiffrierung

Dechiffrierung - (engl.) deciphering, decryption

Dechiffrierungist ein Synonym für Entschlüsselung.

kryptologische Annahme

kryptologische Annahme - (engl.) cryptological assumption

Der Terminus kryptologische Annahmewird verwendet, um bestimmte kryptologische Probleme zu charakterisieren. So gibt es das Faktorisierungsproblem, von dem angenommen wird, daßes praktisch unlösbar (*computationally infeasible*) ist. Allerdings gibt es keinen Beweis dafür, daßdiese Annahme richtig ist. Wenn aber eine hinreichend große Anzahl von Fachleuten nach vielen Versuchen, das Problem zu lösen, erfolglos war, so nimmt man an, daßes tatsächlich unlösbar ist. Eine solche Annahme, die auf Expertise beruht, heißt dann kryptologische Annahme. Auf solchen kryptologischen Annahmenberuht die Sicherheit der modernen, asymmetrischen Kryptographie.

encode

encode (engl.) - codieren, verschlüsseln

collision

collision (engl.) - Kollision

collision-free

collision-free (engl.) - kollisionsfrei

Siehe: Kollisionsfreiheit

Siehe auch:collision-resistant, collision-intractable

collision-resistant

collision-resistant (engl.) - kollisionsresistent

Siehe auch:collision-free, collision-intractable

verschlüsseln

verschlüsseln - (engl.) - encrypt, encipher, encode

Verschlüsselnist die Tätigkeit der Verschlüsselung. Ein älterer Begriff dafür ist codieren.

Siehe auch:entschlüsseln

Kryptanalytiker

Kryptanalytiker - (engl.) cryptanalyst (???)

Der Kryptanalytikerwidemt sich (beruflich) dem Entschlüsselnverschlüsselter Nachrichten.

Siehe auch: Kryptologe, Kryptograph

cryptographic hash function

cryptographic hash function (engl.) - kryptographische Hashfunktion

See also:cryptographic one-way hash function, one-way function

key delivery

key delivery (engl.) - Schlüsselverteilung, Schlüsselübergabe

Siehe auch:key distribution, key transport

entschlüsseln

entschlüsseln - (engl.) decrypt, decipher, decode

Entschlüsselnist die Tätigkeit der Entschlüsselung. Früher sprach man oft auch von decodieren.

Siehe auch:verschlüsseln

deciphering

deciphering (engl.) - Dechiffrierung

Decipheringist ein seltener gebrauchtes Synonym für decryption.

key space

key space (engl.) - Schlüsselraum

exhaustive Suche

exhaustive Suche - (engl.) exhaustive search

Unter der exhaustiven Sucheversteht man das Ausprobieren aller Schlüsselaus dem Schlüsselraum.

Die exhaustiven Suche kann so erfolgen, daß ein Schlüssel gewählt wird, und ein Geheimtext damit entschlüsselt wird. Ist das Resultat, d.h. der gewonnene Klartext, sinnvoll, so kann man vermuten, den Schlüssel gefunden zu haben. Ansonsten beginnt man von vorn und fährt fort, bis man erfolgreich war.

Eine andere Variante setzt voraus, daß man über mehrere Geheimtexte verfügt und vermutet, was diese bedeuten, d. h. welchen Klartexten sie entsprechen. Dann wählt man einen Schlüssel und verschlüsselt den Klartext. Zeigt ein Vergleich mit dem Geheimtext, daß die Verschlüsselung erfolgreich war, hat man vermutlich den Schlüssel gefunden.

Zur Überprüfung wählt man ein anderes Klartext/Geheimtext-Paar und probiert den Schlüssel aus.

symmetrischer Verschlüsselungsalgorithmus

symmetrischer Verschlüsselungsalgorithmus - (engl.) symmetric encryption algorithm, symmetric encryption scheme

Siehe auch: asymmetrischer Verschlüsselungsalgorithmus

geheimer Kanal

geheimer Kanal - (engl.) secret channel

...

secret channel

secret channel (engl.) - geheimer Kanal

encrypt

encrypt (engl.) - verschlüsseln

encipher

encipher - (engl.) verschlüsseln

universelle Hashfunktion

universelle Hashfunktion - (engl.) universal hashfunction

An eine universelle Hashfunktionwerden folgende Anforderungen gestellt: Wenn man aus der Menge der Argumente eine feste Anzahl Elemente wählt und deren Hashwertebestimmt, ist die Wahrscheinlichkeit einer Kollision für diese Elemente höchstens so groß, wie die Wahrscheinlichkeit, bei der Auswahl ein bestimmtes Argument zu wählen.

Um die Definition etwas zu veranschaulichen:

> Man nehme ein Buch, zerschneide es und mische die Seiten. Dann gebe man sich eine Funktion vor, die eine Anzahl von Buchstaben als Argument hat und eine Zahl als Resultat. Die Menge aller möglichen Zahlen (Funktionswerte) soll kleiner sein, als die Seitenzahl des Buches (sonst ist das Kriterium einer Hashfunktionnicht erfüllt).
>
> Man wähle zwei Seiten aus dem Haufen und wende auf die Buchstaben jeder Seite die Funktion an. Dadurch erhält man zwei Zahlen. Die Wahrscheinlichkeit, aus dem Stapel der Seiten eine bestimmte Seite herauszugreifen ist 1/Seitenzahl, insofern man nicht schummelt. Die gewählte Funktion wäre dann eine universelle Hashfunktion, wenn die Wahrscheinlichkeit, daßdie ermittelten Hashwerte -unsere zwei Zahlen- gleich sind (Kollision), nicht größer als 1/Seitenzahl ist.

collision-intractable

collision-intractable (engl.) - kollisionswiderspenstig

Der Begriff ist ziemlich ungebräuchlich. Gebräuchlicher sind statt dessen collision-freeund collision-resistant.

cryptographic one-way hash function

cryptographic one-way hash function (engl.) - kryptographische Einweg-Hashfunktion

See also:cryptographic hash function, one-way function, hash function

schwacher Schlüssel

schwacher Schlüssel - (engl.) weak key

Als schwache Schlüsseleines Verschlüsselungsverfahrenswerden diejenigen bezeichnet, die eine schwächere Verschlüsselung nach sich ziehen, z.B. indem einzelne Verfahrensschritte unwirksam gemacht werden. Meistens sind nur wenige Schlüssel eines Schlüsselraumsals schwach zu bezeichnen. Diese sollten durch ein gutes Verfahren zur Schlüsselgenerierungaussortiert werden.

vertrauenswürdiger Dritter

vertrauenswürdiger Dritter - (engl.) trusted third party

Vertrauenswürdiger Dritter steht synonym für glaubwürdiger Dritter.

weak key

weak key (engl.) - schwacher Schlüssel

TTP ["Trusted Third Party"]

Trusted Third Party (engl.) - Vertrauenswürdiger Dritter

Siehe auch: Trusted Third Instance

Gesetz über Fernmeldeanlagen (FAG) *

Inhaltsverzeichnis

---

§1 Rechte des Bundes; Begriff der Funkanlage; Telekommunikationsdienstleistungen durch andere

(1) - (3) (*aufgehoben*)

(4) Das Bundesministerium für Post und Telekommunikation verleiht hiermit der Deutschen Telekom AG bis zum 31. Dezember 1997 das ausschließliche Recht, Sprachtelefondienst nach §6 Abs. 1 Nr. 2 des Telekommunikationsgesetzes vom 25. Juli 1996 (BGBl. I S. 1120) zu erbringen.

(5) Das Bundesministerium für Post und Telekommunikation kann Änderungen an Inhalt und Umfang der ausschließlichen Rechte nach den Absatz 4 mit Beteiligung des Regulierungsrates nach §13 Abs. 3 Nr. 3 des Gesetzes über die Regulierung der Telekommunikation und des Postwesens bestimmen.

(6) Für Anlagen, die zur Verteidigung des Bundesgebietes bestimmt sind, hat der Bund die in den Absätzen 1, 2 und 4 bezeichneten Rechte inne. Diese Rechte werden durch den Bundesminister der Verteidigung ausgeübt.

§1a (*aufgehoben*)

§2 Verleihung der Betriebsbefugnis für einzelne Fernmeldeanlagen; Festsetzung der Bedingung und Kosten

(1) Soweit dem Nachfolgeunternehmen der Deutschen Bundespost TELEKOM ein ausschließliches Recht nach §1 Abs. 2 oder §1 Abs. 4 zusteht, kann der Bundesminister für Post und Telekommunikation die Befugnis zur Errichtung und zum Betrieb einzelner Fernmeldeanlagen auch an andere verleihen. Die Verleihung kann für bestimmte Strecken oder Bezirke erteilt werden. Die Verleihung sowie die Festsetzung der Bedingungen und Auflagen für die Verleihung und Ausübung der zugewiesenen Rechte stehen dem Bundesminister für Post und Telekommunikation oder den von ihm hierzu ermächtigten Behörde zu. Verleihungen werden gegen Gebühr erteilt.

(2) Der Bundesminister für Post und Telekommunikation erläßt durch Rechtsverordnung mit Beteiligung des Regulierungsrates gemäß §13 Abs. 2 Nr. 3 des Gesetzes über die Regulierung der Telekommunikation und des Postwesens für die Verleihung der Befugnisse nach Absatz 1

- Entscheidungen über die beabsichtigte Öffnung von Märkten für Telekommunikationsdienstleistungen,
- Regelungen zu Inhalt, Umfang und Verfahren der Verleihung.

(3) Der Bundesminister für Post und Telekommunikation wird ermächtigt, durch Rechtsverordnung, die der Zustimmung des Bundesrates bedarf, nach Maßgabe des Verwaltungskostengesetzes die gebührenpflichtigen Tatbestände

- nach Absatz 1 Satz 1 und
- der Frequenzzuteilung gemäß §3 Abs. 2 des Gesetzes über die Regulierung der Telekommunikation und des Postwesens,

die Höhe der Gebühr und die Erstattung von Auslagen zu regeln. Die Höhe der Gebühr und die Erstattung von Auslagen richtet sich nach dem mit den Amthandlungen verbundenen angemessenen Verwaltungsaufwand. Für die Tatbestände gemäß Satz 1 ist die rückwirkende Erhebung von Gebühren und Auslagen ab 1. Juli 1989 zulässig.

(4) Die Verleihung muß für Fernmeldeanlagen, die von Elektrizitätsunternehmen zur öffentlichen Versorgung mit Licht und Kraft, die der allgemeinen Versorgung von Gemeinden oder größerer Gebietsteile zu dienen bestimmt sind, zum Zwecke ihres Betriebes verwendet werden sollen, erteilt werden, soweit nicht Betriebsinteressen des Nachfolgeunternehmens der Deutschen Bundespost TELEKOM entgegenstehen; dies gilt nicht für Funkanlagen. Ferner muß sie für Satellitenfunkanlagen, die zur Übermittlung von Daten niedriger Bitraten bestimmt sind, erteilt werden, soweit Gründe des Funkverkehrs nicht entgegenstehen; für sonstige Satellitenfunkanlagen kann die Verleihung nach Absatz 1 erteilt werden.

§§2a bis §6 (*aufgehoben*)

§7 Öffentlicher Fernmelde- und Telegrammverkehr

(1) Jedermann hat gegen Zahlung der Gebühren das Recht auf Beförderung von ordnungsmäßigen Telegrammen und auf Zulassung zu einem ordnungsmäßigen Gespräch auf den für den öffentlichen Fernmeldeverkehr bestimmten Anlagen.

(2) (*aufgehoben*)

§8 Anschluß an das Lokalnetz

Sind an einem Ort Fernmeldeanlagen für den Ortsverkehr, sei es vom Nachfolgeunternehmen der

Deutschen Bundespost TELEKOM, sei es von der Gemeindeverwaltung oder von einem anderen Unternehmer, zur Benutzung gegen Entgelt errichtet, so kann jeder Eigentümer eines Grundstücks gegen Erfüllung der von jenen zu erlassenden und öffentlich bekanntzumachenden Bedingungen den Anschluß an das Lokalnetz verlangen.

§§9 - 11 (*aufgehoben*)

§12 Auskunft im Strafverfahren

In strafgerichtlichen Untersuchungen kann der Richter und bei Gefahr im Verzug auch die Staatsanwaltschaft Auskunft über die Telekommunikation verlangen, wenn die Mitteilungen an den Beschuldigten gerichtet waren oder wenn Tatsachen vorliegen, aus denen zu schließen ist, daß die Mitteilungen von dem Beschuldigten herrührten oder für ihn bestimmt waren und daß die Auskunft für die Untersuchung Bedeutung hat. Das Grundrecht des Artikels 10 des Grundgesetzes wird insoweit eingeschränkt.

§§13 - 18 (*aufgehoben*)

§19 [*Störung des Funkverkehrs*]

(1) Wer absichtlich den Betrieb einer öffentlichen Zwecken dienenden Funkanlage dadurch verhindert oder stört, daß er elektrische Energie verwendet, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Wer absichtlich den Betrieb einer sonstigen Funkanlage dadurch verhindert oder stört, daß er elektrische Energie verwendet oder für die Anlage bestimmte elektrische Energie entzieht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Die Tat wird nur auf Antrag verfolgt.

§§20 - 27 (*aufgehoben*)

§28 Außerkrafttreten

Dieses Gesetz tritt mit Ablauf des 31. Dezember 1997 außer Kraft.

** In der Fassung vom 3. Juli 1989; (BGBl. I S. 1455), geändert durch Artikel 5 Postneuordnungsgesetz (PTNeuOG) vom 14. September 1994 (BGBl. I S. 2325) und Artikel 47 Markenrechtsreformgesetz vom 25. Oktober 1994 (BGBl. I S. 3082), zuletzt geändert durch §99 Abs. 1 TKG vom 25. Juli 1996 (BGBl. I S. 1120)*

---

tamper resistant

tamper resistant (engl.) - einbruchsgeschützt, vor (unerlaubtem) Zugriff gesichert

UID [*User Identifier, Unique Identifier*]

1. User Identifier (engl.) - Benutzerkennung
2. Unique Identifier (engl.) - Eindeutige Kennung

1. Der User Identifier dient der Unterscheidung der Benutzer in einem Mehrbenutzerbetriebssystem, wie z.B. Linux.
2. Der Unique Identifier dient der eindeutigen Identifizierung von Personen und/oder Geräten bei der verschlüsselten Kommunikation in der Clipper-Initiative.

exhaustive search

exhaustive search (engl.) - exhaustive Suche

dictionary attack

dictionary attack (engl.) - Wörterbuchangriff

adaptive chosen-ciphertext attack

adaptive chosen-ciphertext attack (engl.) - Geheimtextangriff mit Anpassung des gewählten Geheimtextes

Eingangsseite Index Mail

Angriff

Angriff - (engl.) attack

Im Zusammenhang mit Kryptologieist mit der Bezeichnung Angriffder Versuch des unbefugten Zugriffes auf oder der unbefugten Teilnahme an einer verschlüsselten Kommunikation, oder deren Verhinderung gemeint. Die Wahl der Mittel und die möglichen Ziele des Angreiferssind sehr vielgestaltig.

Die Kryptologie hat sich zu einem großen Teil im Umfeld von Militär und Geheimdiensten entwickelt und drückt sich deshalb oft auch in deren Terminologie aus. So findet man die Einstufung von kryptographischen Angriffen (attacks) als ``*information warfare*" (IW) ([CRISIS 1996]).

Klassifizierung

Kryptographische Angriffelassen sich zwei Klassen zuordnen.

Die erste Klasse umfaßt Angriffe, bei denen der Angreifer unbemerkt mithören, d.h. abhören will. Da er nicht aktiv ins Kommunikationsgeschehen eingreift, werden solche Angriffe als *passiv* bezeichnet. Angriffe aus dieser Klasse stellen Verletzungen der Geheimhaltung dar.

Die zweite Klasse umfaßt diejenigen Angriffe, die auf eine aktive Beeinflussung der Kommunikation abzielen. Dazu gehören alle Arten der *aktiven* Manipulation von Inhalten und Formen des Nachrichtenaustausches. Dadurch werden sowohl die Geheimhaltung, als auch Authentizität und Integrität der Nachrichten und/oder Schlüssel verletzt. Der Grad möglicher Verletzungen ist in dieser Klasse höher, als bei passiven Angriffen.

Typisierung

Es werden eine Vielzahl unterschiedlicher Angriffeunterschieden, von denen einige *typisch*sind. Viele von ihnen lassen sich kombinieren und können als passiver oder aktiver Angriffausgeführt werden.

`Klassisch' sind diejenigen Angriffe, die eine Entschlüsselung des Geheimtextes zum Ziel haben. Dazu gehören:

- ciphertext-only attack

- chosen-ciphertext attack
- adaptive-chosen ciphertext attack
- known-plaintext attack
- chosen-plaintext attack
- adaptive-chosen plaintext attack

Dazu kommen eine Anzahl von Angriffen, die Schwachpunkte im kryptographischen Protokoll ausnutzen (u.a. nach [Menezes/Oorschot/Vanstone 1997], S. 42):

- known-key attack
- replay attack
- impersonation attack
- dictionary attack
- forward search
- interleaving attack

Weitere Angriffe sind u.a.:

- MAC forgery attack
- key recovery attack
- low exponent attack
- Berlekamp-Massey attack
- Round-off attack
- Nearest-Plane attack
- low density attack
- message-resend attack

Angreifer

Angreifer - (engl.) adversary, *selten:*attacker

Als Angreiferwird diejenige Person bezeichnet, die versucht, unbefugt (aus der Perspektive von Senderund Empfänger) Erkenntnisse über eine verschlüsselte Kommunikation zu gewinnen, indem sie einen kryptographischen Angriff(*attack*) startet.

Die Zielstellungen eines Angreifers können sehr unterschiedlich sein. Es lassen sich passive und aktive Formen des Angriffs unterscheiden.

Passive Angriffe, z.B.:

- Identität von Sender und/oder Empfänger ermitteln
- Inhalt der Nachricht bestimmen
- In den Besitz von Schlüsseln gelangen

Aktive Angriffe, z.B.:

- Vortäuschung, ein Kommunikationspartner zu sein
- Fälschen von Nachrichten (Verfälschen, Ankunft verhindern, falsche Nachrichten unterschieben)
- Fälschen von Schlüsseln

trapdoor

trapdoor (engl.) - Falltür

See also:trapdoor information

Einweg-Funktion

Einweg-Funktion - (engl.) one-way function (OWF)

Informell lassen sich Einweg-Funktionenfolgendermaßen beschreiben: Sie sind relativ leicht zu berechnen und die inverse Funktion läßt sich für nahezu alle Funktionswerte nicht in vertretbarer Zeit, mit vertretbarem Aufwand berechnen. Allerdings gibt es immer einige Funktionswerte, zu denen sich das Argument relativ leicht finden läßt. Die erste Definition für Einweg-Funktionenlieferte L. Berman (nach [Kurtz/Mahaney/Royer 1988]).

Anwendung

Die Idee der Einweg-Funktionwird z.B. bei Einweg-Hashfunktionenund bei der Public Key-Kryptographieaufgegriffen.

Sicherheit

Die Existenz von Einweg-Funktionenwird angenommen, ist jedoch unbewiesen. Könnte man beweisen, daßeine Funktion das Einweg-Kriterium erfüllt, so hätte man in diesem Falle eine *echte*Einweg-Funktion. Bisher ist das nicht gelungen. Die Sicherheit aller Einweg-Funktionenist somit eine angenommene, keine bewiesene! [Menezes/Oorschot/Vanstone 1997]

Siehe auch: Einweg-Funktion mit Falltür

trapdoor information

trapdoor information (engl.) - Falltürinformation

See also:trapdoor

Fernmeldeverkehrüberwachungsverordnung (FÜV*)

Inhaltsverzeichnis

Auf Grund des §10b Satz 2 des Gesetzes über Fernmeldeanlagen in der Fassung der Bekanntmachung vom 3. Juli 1989 (BGBl. I S. 1455), der durch Artikel 5 Nr. 11 des Gesetzes zur Neuordnung des Postwesens und der Telekommunikation vom 14. September 1994 (BGBl. I S. 2325) eingefügt wurde, verordnet die Bundesregierung:

Abschnitt 1: Allgemeine Vorschriften

§1 Zweck

Diese Verordnung regelt die Anforderungen und das Verfahren zur technischen Umsetzung von Überwachungsmaßnahmen nach dem Gesetz zu Artikel 10 Grundgesetz, §100a der Strafprozeßordnung und §39 des Außenwirtschaftsgesetzes in Fernmeldeanlagen, die für den öffentlichen Verkehr bestimmt sind.

§2 Begriffsbestimmungen

Im Sinne dieser Verordnung ist

1. Betreiber: jeder, der eine Fernmeldeanlage, die für den öffentlichen Verkehr bestimmt ist, betreibt;
2. Überwachungsmaßnahme: die technische Maßnahme zur Überwachung des Fernmeldeverkehrs nach dem Gesetz zu Artikel 10 Grundgesetz, §100a der Strafprozeßordnung oder §39 des Außenwirtschaftsgesetzes ;
3. Bedarfsträger: die berechtigten Stellen nach Art. 1 §1 Abs. 1 des Gesetzes zu Artikel 10 Grundgesetz, §1OOb Abs. 3 der Strafprozeßordnung oder §39 Abs. 1 des Außenwirtschaftsgesetzes ;
4. Anschluß: diejenige technische Einrichtung, die Ursprung oder Ziel des Fernmeldeverkehrs ist und in der Regel durch eine Rufnummer eindeutig gekennzeichnet wird (physikalischer Anschluß) oder die Rufnummer, die der Teilnehmer einem physikalischen Anschluß fallweise zuordnen kann;
5. Funkzelle: der kleinste durch seine geographische Lage bestimmbare funktechnische Versorgungsbereich in einem Mobilfunknetz;
6. Kunde: eine Person, die mit dem Betreiber Vertragsbeziehungen über die Bereitstellung und Nutzung der Fernmeldeanlage für eigene Telekommunikationszwecke unterhält;
7. Anordnung: die Anordnung zur Beschränkung des Fernmeldegeheimnisses nach dem Gesetz zu Artikel 10 Grundgesetz , den §§100a und 100b der Strafprozeßordnung oder den §§39 und 40 desAußenwirtschaftsgesetzes .

Abschnitt 2: Anforderungen an die Umsetzung von Überwachungsmaßnahmen

§3 Bereitzustellende Informationen

(1) Der Betreiber hat im Rahmen der räumlichen Abgrenzung nach §5 Abs. 1 zu gewährleisten,

daß innerhalb des durch die Anordnung bestimmten Zeitraums die Überwachung und Aufzeichnung des gesamten Fernmeldeverkehrs ermöglicht wird, der von dem zu überwachenden Anschluß ausgeht oder für diesen bestimmt ist oder der statt dessen zu technischen Speichereinrichtungen geleitet wird oder der aus solchen Speichereinrichtungen abgerufen wird.

(2) Neben den Nachrichten hat der Betreiber dem Bedarfsträger Informationen über die mit dem Fernmeldevorgang zusammenhängenden näheren Umstände bereitzustellen, und zwar:

1. die vom überwachten Anschluß gewählten Rufnummern und Zusatzdienste, auch wenn keine Verbindung zustande kommt,
2. die Rufnummern der Anschlüsse, die den überwachten Anschluß angewählt haben, auch wenn keine Verbindung zustande kommt,
3. bei Leistungsmerkmalen, welche den Fernmeldeverkehr um- oder weiterleiten (Rufumleitung oder Rufweiterschaltung) das Umlenkziel, bei virtuellen Anschlüssen die jeweils zugeordneten physikalischen Anschlüsse,
4. bei überwachten Mobilanschlüssen die Funkzellen, über die die Verbindung abgewickelt wird,
5. Informationen zu dem jeweils in Anspruch genommenen Telekommunikationsdienst und
6. mindestens zwei der folgenden drei Angaben: Beginn und Ende der Verbindung oder des Verbindungsversuchs (jeweils mit Datum und Uhrzeit), Dauer der Verbindung.

(3) Jeder an der Schnittstelle bereitgestellte Fernmeldeverkehr ist durch ein eindeutiges Merkmal der jeweiligen Überwachungsmaßnahme zu kennzeichnen; das Merkmal darf nicht identisch sein mit Daten zum überwachten Anschluß.

(4) Die in den Absätzen 1 bis 3 genannten Bedingungen gelten entsprechend auch für Konferenzgespräche, soweit und solange der überwachte Anschluß an einem solchen Gespräch teilnimmt.

§4 Zeitliche Umsetzung

(1) Der Betreiber muß die notwendigen Vorkehrungen treffen, um seine Verpflichtung, die Überwachung und Aufzeichnung des Fernmeldeverkehrs zu ermöglichen, ab dem Zeitpunkt, zu dem die Fernmeldeanlage den Kundenbetrieb aufnimmt, entsprechend den Vorschriften der §§3 bis 14 erfüllen zu können. Dies gilt entsprechend für die Einführung von Änderungen der Fernmeldeanlage oder für neue Betriebsmöglichkeiten bestehender Telekommunikationsdienste, soweit diese Einfluß auf bestehende Überwachungsmöglichkeiten haben.

(2) Die in einer Fernmeldeanlage zur Umsetzung von Überwachungsmaßnahmen erforderlichen

Vorkehrungen sind so zu gestalten, daß der Betreiber eine im Einzelfall angeordnete Überwachung sofort nach Vorlage der Anordnung ermöglichen kann.

(3) Die Überwachung des Fernmeldeverkehrs eines Anschlusses erfolgt nach der ergangenen Anordnung zeitgleich mit diesem Verkehr.

(4) Dem Bedarfsträger ist auf Antrag ein Anschluß zu den üblichen Geschäftsbedingungen des jeweiligen Betreibers zu dem Zweck zu überlassen, die technische Umsetzung der Überwachungsmaßnahmen unter sämtlichen Betriebsbedingungen zu erproben. Die Erprobung umfaßt die Bereitstellung des von diesem Anschluß herrührenden oder für ihn bestimmten Fernmeldeverkehrs gemäß den §§3 , 8 und 9, die Übertragung zum Bedarfsträger sowie die ordnungsgemäße Funktion der Aufzeichnungseinrichtungen des Bedarfsträgers. Der Bedarfsträger hat sicherzustellen, daß über diesen Anschluß ausschließlich der von ihm selbst zu Probezwecken erzeugte Fernmeldeverkehr ohne Beteiligung Dritter abgewickelt wird.

§5 Örtliche Umsetzung

(1) Die Verpflichtung des Betreibers besteht für solchen Fernmeldeverkehr, der mittels des überwachten Anschlusses über Fernmeldeanlagen im Geltungsbereich des Gesetzes zu Artikel 10 Grundgesetz, der Strafprozeßordnung und des Außenwirtschaftsgesetzes abgewickelt wird.

(2) Zum Zwecke einer eindeutigen Abgrenzung der Zuständigkeiten und Verantwortlichkeiten und der Gewährleistung des Fernmeldegeheimnisses unbeteiligter Dritter sind die Überwachung und Aufzeichnung des Fernmeldeverkehrs nicht in den Betriebsräumen des Betreibers durchzuführen. Die Bedarfsträger haben hierfür eigene Überwachungsstellen einzurichten. In Ausnahmefällen kann die Nutzung sonstiger Räume des Betreibers für diesen Zweck erfolgen, wenn diese Räume ausschließlich vom Bedarfsträger genutzt werden und dem Bedarfsträger ein Zugang zu den Betriebsräumen nicht möglich ist.

§6 Häufung von Überwachungsmaßnahmen

(1) Der Betreiber muß sicherstellen, daß gleichzeitig mehr als eine Überwachungsmaßnahme in Bezug auf ein und denselben Anschluß durchgeführt werden kann.

(2) Die in einer Fernmeldeanlage zu treffenden Vorkehrungen zur technischen Umsetzung von Überwachungsmaßnahmen sind anforderungsgerecht auszubauen und so zu gestalten, daß Engpässe, die in einem regional oder funktional begrenzten Teil einer Fernmeldeanlage bei

gleichzeitiger Durchführung mehrerer Überwachungsmaßnahmen auftreten können, unverzüglich beseitigt werden können.

(3) Das Bundesministerium für Post und Telekommunikation kann in Technischen Richtlinien nach §13 Richtwerte und Mindestwerte für die Anzahl der in einer Fernmeldeanlage oder Teilen einer Fernmeldeanlage gleichzeitig umsetzbaren Überwachungsmaßnahmen festlegen.

§7 Benennung des zu überwachenden Anschlusses

(1) Der Betreiber hat eine Überwachungsmaßnahme gegen eine Person, die sein Kunde ist, aufgrund der in der Anordnung enthaltenen Angaben zu Name und Anschrift des Kunden umzusetzen.

(2) Richtet sich eine angeordnete Überwachungsmaßnahme gegen eine Person, die nicht Kunde des Betreibers ist, muß der Betreiber die Überwachung auf der Grundlage eines ihm gleichzeitig mit der Anordnung zu benennenden eindeutigen technischen Kennzeichnungsmerkmals des zu überwachenden Anschlusses, insbesondere der Rufnummer, ermöglichen.

(3) Soweit die besonderen Eigenschaften einer bestimmten Fernmeldeanlage und die berechtigten Anforderungen der Bedarfsträger es erfordern, an einer Fernmeldeanlage verschiedenartige Kennzeichnungsmerkmale für die Bestimmung des zu überwachenden Fernmeldeverkehrs anzuwenden, hat der Betreiber sicherzustellen, daß der Fernmeldeverkehr auf Grund dieser Kennzeichnungsmerkmale überwacht werden kann. Die Kennzeichnungsmerkmale müssen im Einzelfall mit vertretbarem Aufwand zu ermitteln und geeignet sein, den zu überwachenden Fernmeldeverkehr eindeutig zu bestimmen.

§8 Technische Schnittstellen

(1) Der Betreiber hat den zu überwachenden Fernmeldeverkehr für die gesamte Dauer der Überwachungsmaßnahme an einer festgelegten technischen Schnittstelle bereitzustellen. Die Schnittstelle muß technisch so gestaltet sein, daß insbesondere

1. an ihr ausschließlich Fernmeldeverkehr bereitgestellt wird, der von dem überwachten Anschluß herrührt oder für diesen bestimmt ist,
2. die Qualität des an ihr bereitgestellten Fernmeldeverkehrs nicht schlechter ist als die, die dem überwachten Teilnehmer bei der jeweiligen Verbindung geboten wird,
3. die Übertragung des an ihr bereitgestellten Fernmeldeverkehrs zum Bedarfsträger mittels

genormter, allgemein verfügbarer Übertragungswege und Protokolle erfolgen kann und

4. der im Rahmen einer Überwachungsmaßnahme anfallende Fernmeldeverkehr im Falle der Übertragung über Festverbindungen über einen einzigen Übertragungsweg zum Bedarfsträger oder im Falle der Übertragung über Wählverbindungen zu einem einzigen Anschluß beim Bedarfsträger übermittelt werden kann.

Die Schnittstelle kann mit dem Ziel der Vereinheitlichung in Technischen Richtlinien nach §13 festgelegt werden.

(2) Für die Übertragung des an der Schnittstelle bereitgestellten zu überwachenden Fernmeldeverkehrs zum Bedarfsträger sind grundsätzlich Festverbindungen oder ISDN-Wählverbindungen oder ähnlich schnell aufbaubare Wählverbindungen zu nutzen. Soll die Übertragung zum Bedarfsträger mittels Wählverbindungen erfolgen, muß die Schnittstelle auch die Fähigkeit zum automatischen Verbindungsaufbau zu dem vom Bedarfsträger zu benennenden Anschluß beinhalten, an den die Aufzeichnungseinrichtung angeschlossen ist. Wählverbindungen zum Bedarfsträger sind zu Beginn eines jeden für den überwachten Anschluß bestimmten oder von diesem herrührenden Fernmeldeverkehrs aufzubauen und nach dessen Ende wieder auszulösen. Die erforderlichen Zugänge zum Wählnetz sind Bestandteil der Schnittstelle.

(3) Der Betreiber hat unter Berücksichtigung der praxisorientierten Erfordernisse, insbesondere der Anforderungen nach §4 Abs. 2 und 3 , festzulegen, von welcher der in Absatz 2 Satz 1 genannten Möglichkeiten er in einer bestimmten Fernmeldeanlage Gebrauch macht. Für den Fall, daß der zu überwachende Fernmeldeverkehr nicht an einer einzelnen Schnittstelle bereitgestellt werden kann, müssen die Schnittstellen so gestaltet sein, daß Wählverbindungen zum Bedarfsträger realisiert werden können.

(4) Wenn der Betreiber die ihm zur Übermittlung anvertrauten Nachrichten durch technische Maßnahmen gegen die unbefugte Kenntnisnahme durch Dritte schützt, hat er an der Schnittstelle nach Absatz 1 bis 3 die ungeschützten Nachrichten bereitzustellen. Falls der Betreiber dem Teilnehmer Verschlüsselungsmöglichkeiten für die Nachrichten bereitstellt, hat er an der Schnittstelle nach Absatz 1 bis 3 die entschlüsselten Nachrichten bereitzustellen oder dem Bedarfsträger die für eine Entschlüsselung erforderlicher Informationen zeitgerecht zur Verfügung zu stellen.

§9 Zeitweilige Übermittlungshindernisse

Falls in Ausnahmefällen die Übermittlung eines zu überwachenden Fernmeldeverkehrs an den Bedarfsträger nicht möglich ist, müssen ihm die Informationen über die näheren Umstände des Fernmeldeverkehrs in dem Umfang, in dem sie der Betreiber gemäß den geltenden Datenschutzbestimmungen speichert, unverzüglich nachträglich übermittelt werden. Eine

Verhinderung des zu überwachenden Fernmeldeverkehrs ist nicht zulässig. Zu einer Aufzeichnung oder zeitweiser Speicherung des zu überwachenden Fernmeldeverkehrs oder von Teilen desselben über den nach den Datenschutzbestimmungen zulässigen Umfang hinaus, insbesondere der Nachrichten, ist der Betreiber nicht befugt.

§10 Selbständigkeit des Betreibers

Der Betreiber hat seine Fernmeldeanlage technisch so zu gestalten, daß er eine angeordnete Überwachungsmaßnahme ohne Mitwirkung anderer umsetzen kann.

§11 Unveränderthеit des überwachten Anschlusses

Die Umsetzung einer Überwachungsmaßnahme muß so erfolgen, daß die Überwachung von den am Fernmeldeverkehr Beteiligten nicht feststellbar ist. Insbesondere dürfen die Betriebsmöglichkeiten des überwachten Anschlusses durch die Überwachungsmaßnahme nicht verändert werden.

§12 Schutzanforderungen

(1) Die Umsetzung der innerhalb der Fernmeldeanlage erforderlichen technischen Vorkehrungen, auf deren Grundlage die Durchführung von Überwachungsmaßnahmen ermöglicht wird, erfolgt unter Beachtung der beim Betreiben von Fernmeldeanlagen üblichen Sorgfalt, insbesondere hinsichtlich

1. der Schutzbedürftigkeit der Informationen, welche und wieviele Rufnummern einer Überwachung unterliegen oder unterlegen haben und in welchen Zeiträumen Überwachungsmaßnahmen durchgeführt wurden und
2. der Einbeziehung von möglichst wenig Personal für die Umsetzung von Überwachungsmaßnahmen

(2) Ein Zugriff auf die Schnittstelle nach §8 darf nur den dazu berechtigten Personen ermöglicht werden. Die Schnittstelle ist aus diesem Grund durch physikalische und organisatorische Maßnahmen vor Mißbrauch zu schützen.

(3) Der Fernmeldeverkehr darf an die Aufzeichnungseinrichtung des Bedarfsträgers nur

übermittelt werden, nachdem die Empfangsberechtigung der Aufzeichnungseinrichtung und die Sendeberechtigung der Schnittstelle nach §8 nachgewiesen ist. Im Falle der Nutzung von Wählverbindungen zum Bedarfsträger ist dieser Nachweis bei jedem Verbindungsaufbau zu erbringen.

(4) Informationen über die Art und Weise, wie Überwachungsmaßnahmen in einer bestimmten Fernmeldeanlage durchgeführt werden, dürfen Unbefugten nicht zugänglich gemacht werden. Der Betreiber hat auch mit den Herstellern seiner technischen Einrichtungen zur Umsetzung von Überwachungsmaßnahmen entsprechende Vertraulichkeit zu vereinbaren.

(5) Zur Verhinderung oder Verfolgung eines Mißbrauchs der in den Fernmeldeanlagen enthaltenen Funktionen, mit denen die Überwachung technisch ermöglicht wird, ist der Einsatz dieser Funktionen in Bezug auf einen konkreten Anschluß lückenlos zu protokollieren. Darunter fallen auch solche Einsätze, die durch fehlerhafte oder mißbräuchliche Bedienung verursacht wurden. Es sind zu protokollieren:

1. die Rufnummer bzw. das entsprechende Kennzeichnungsmerkmal des betroffenen Anschlusses,
2. Beginn und Ende des Einsatzes,
3. das Ziel, an das der zu überwachende Fernmeldeverkehr geleitet wird und
4. ein Merkmal, welches zur Erkennung des Bedienungspersonals geeignet ist (einschließlich Datum und Uhrzeit der Eingabe).

(6) Der Betreiber hat sicherzustellen, daß die Protokolle nur seinem mit der organisatorischen Durchführung der Überwachungsmaßnahme betrauten Personal oder bei VS-Angelegenheiten nur dem Personal zugänglich gemacht werden, das die Voraussetzungen nach dem Sicherheitsüberprüfungsgesetz erfüllt. Diese Personen prüfen die Protokolle regelmäßig, spätestens alle drei Monate. Das Ergebnis der Prüfung ist schriftlich festzuhalten. Wenn die Protokolle nicht beanstandet werden, sind die Daten unverzüglich durch den vorher genannten Personenkreis zu löschen. Andernfalls sind nur die nicht beanstandeten Datensätze zu löschen, die beanstandeten Datensätze hingegen erst unverzüglich nach Abschluß der zur Klärung der Beanstandung einzuleitenden Maßnahmen. Von Beanstandungen, insbesondere von fehlerhaften oder unzulässigen Eingaben, ist unverzüglich das Bundesamt für Post und Telekommunikation zu unterrichten. In Fällen, in denen es zu Beanstandungen im Rahmen einer angeordneten Überwachungsmaßnahme kommt, ist außerdem unverzüglich der betroffene Bedarfsträger zu informieren.

(7) Das Bundesamt für Post und Telekommunikation ist befugt, Einsicht in die Protokolle und die zugehörigen Unterlagen durch Bedienstete zu verlangen, die die Voraussetzungen nach dem Sicherheitsüberprüfungsgesetz erfüllen.

§13 Technische Richtlinien

Die nähere technische Ausgestaltung der Anforderungen nach den §§3 bis 12 kann in Technischen Richtlinien festgelegt werden. Diese sind vom Bundesministerium für Post und Telekommunikation zu erlassen. Ihre Herausgabe ist im Amtsblatt des Bundesministeriums für Post und Telekommunikation bekanntzumachen.

§14 Geheimschutz

Der Betreiber hat die in seiner Fernmeldeanlage zu treffenden technischen Vorkehrungen so zu gestalten, daß er auch die Überwachung auf Grund einer Anordnung ermöglichen kann, die Verschlußsache im Sinne des §1 Abs. 2 Nr. 1 des Sicherheitsüberprüfungsgesetzes ist. Der Betreiber ist verpflichtet, mit der zuständigen amtlichen Stelle Vereinbarungen über den Schutz amtlich geheim zu haltender Verschlußsachen (§4 Sicherheitsüberprüfungsgesetz) zu treffen.

Abschnitt 3: Zuständigkeiten und Verfahren

§15 Zuständige Behörde

Das Bundesamt für Post und Telekommunikation wird mit den Arbeiten zur Vorbereitung der Entscheidung über die Erteilung des Einvernehmens des Bundesministeriums für Post und Telekommunikation nach §10b Satz 1 des Gesetzes über Fernmeldeanlagen beauftragt. Diese Beauftragung schließt eine Wahrnehmung der Aufgaben nach Satz 1 durch das Bundesministerium für Post und Telekommunikation im Einzelfall nicht aus.

§16 Verfahren zur Erzielung des Einvernehmens

(1) Jeder Betreiber hat vor der erstmaligen Inbetriebnahme von Fernmeldeanlagen und vor der

Durchführung von Änderungen, die Einfluß auf die Ausführung von Überwachungsmaßnahmen haben können, dem Bundesamt für Post und Telekommunikation ein schriftliches Konzept zur Gestaltung der technischen Einrichtungen zur Umsetzung von Überwachungsmaßnahmen des Fernmeldeverkehrs vorzulegen.

(2) Aus dem Konzept muß hervorgehen

1. die technische Beschreibung der Fernmeldeanlage,
2. die über diese Fernmeldeanlage angebotenen Telekommunikationsdienstleistungen,
3. die in bezug auf diese Fernmeldeanlage nach§3 bereitzustellenden Informationen,
4. die Beschreibung der technischen Einrichtungen, die der Bereitstellung des zu überwachenden Fernmeldeverkehrs nach§3 dienen,
5. die Beschreibung der technischen Schnittstelle nach§8 und
6. die Beschreibung der Vorkehrungen zur technischen Umsetzung der Anforderungen nach den§§4bis13 .

(3) Entspricht das vorgelegte Konzept den Anforderungen der §§3 bis 13 und 17, teilt das Bundesministerium für Post und Telekommunikation dem Betreiber schriftlich mit, daß für den Fall der tatsächlichen Umsetzung des Konzeptes und des Vorliegens der Voraussetzungen nach den Absätzen 4 und 5 das Einvernehmen im Sinne von §10b Satz 1 des Gesetzes über Fernmeldeanlagen erteilt wird. Anderenfalls fordert das Bundesamt für Post und Telekommunikation den Betreiber unter Angabe der festgestellten Mängel zur Vorlage eines verbesserten Konzeptes auf.

(4) Der Betreiber hat die tatsächliche Umsetzung des Konzeptes dem Bundesamt für Post und Telekommunikation durch schriftliche Erklärung anzuzeigen. Etwaige Abweichungen von dem vorgelegten Konzept müssen den geltenden Rechtsvorschriften, insbesondere den Anforderungen der §§3 bis 14 und 17, entsprechen. Solche Abweichungen sind in der Erklärung darzulegen und zu begründen.

(5) Auf Ersuchen des Bundesamtes für Post und Telekommunikation hat der Betreiber ihm die Umsetzung des Konzeptes in geeigneter Form nachzuweisen. Dieser Nachweis kann insbesondere dadurch geführt werden, daß der Betreiber den Bediensteten des Bundesamtes für Post und Telekommunikation die Besichtigung sowie die Durchführung von Messungen und Prüfungen einschließlich des hierfür erforderlichen Betretens der Geschäfts- oder Betriebsräume gestattet oder die ordnungsgemäße Betriebsbereitschaft vorführt.

Abschnitt 4: Übergangs- und Schlußvorschriften

§17 Übergangs- und Ausnahmeregelung

(1) Vorbehaltlich anderweitiger Regelungen sind die technischen Vorkehrungen für Überwachungsmaßnahmen in Fernmeldeanlagen, die sich zum Zeitpunkt des Inkrafttretens dieser Verordnung bereits Kundenbetrieb befinden oder die bis zum 29. Februar 1996 den Kundenbetrieb aufnehmen, abweichend von §4 Abs. 1 Satz 1 bis zum 31. Mai 1996 entsprechend den Vorschriften der §§3 bis 14 zu treffen.

(2) Bei den technischen Vorkehrungen für Überwachungsmaßnahmen im bestehenden Funktelefonnetz C sind Abweichungen von den Vorschriften des §3 Abs. 2 Nr. 2, 3 und 5, des §3 Abs. 3, des §4 Abs. 3, des §5 Abs. 2, des §7 Abs. 3, des §9 und des §12 Abs. 2, 3 und 5 im Rahmen des am 1. Januar 1995 verfügbaren technischen Verfahrens zulässig.

(3) Für einen Anschluß, der über eine herkömmliche, mit analoger Übertragungstechnik betriebene Anschlußleitung an die Vermittlungsstelle geschaltet ist, kann die Bereitstellung der Überwachungsmöglichkeit noch so lange nach dem am 1. Januar 1995 bestehenden, ausschließlich auf die Anschlußleitung bezogenen technischen Verfahren erfolgen, wie auf Grund der Leistungsmerkmale, die mit dieser Vermittlungsstelle angeboten werden, oder auf Grund der von dem Netzbetreiber auf der Anschlußleitung eingesetzten Übertragungstechnik eine vollständige und zeitgerechte Überwachung mit den bei den Bedarfsträgern vorhandenen überwachungstechnischen Einrichtungen gewährleistet ist.

(4) Die Bereitstellung der Daten gemäß §3 Abs. 2 Nr. 2 kann unterbleiben, wenn der überwachte Anschluß

a. von einem analogen Anschluß angewählt wird oder
b. aus der Fernmeldeanlage eines anderen Betreibers angewählt wird und die Rufnummer nicht an die Fernmeldeanlage übergeben wird, in der die Überwachungsmaßnahme durchgeführt wird.

(5) Im Rahmen des Einvernehmens nach §10b Satz 1 des Gesetzes über Fernmeldeanlagen kann das Bundesministerium für Post und Telekommunikation mit Zustimmung der zuständigen Bundesministerien zulassen, daß in Fällen objektiver Unmöglichkeit von der Erfüllung einzelner Bestimmungen des §3 Abs. 2 abgesehen werden kann. Die Gründe für die objektive Unmöglichkeit sind von dem Betreiber in den Unterlagen nach §16 darzulegen.

§18 Inkrafttreten

Diese Verordnung tritt am Tage nach der Verkündung in Kraft.

** Verordnung über die technische Umsetzung von Überwachungsmaßnahmen des Fernmeldeverkehrs in Fernmeldeanlagen, die für den öffentlichen Verkehr bestimmt sind (18. Mai 1995, BGBl. I S. 722)*

Stand: 12.11.1997

Angriff mit verwandtem Schlüssel

Angriff mit verwandtem Schlüssel - (engl.) related-key attack

???

exklusives Oder

exclusives Oder - (engl.) exclusive or (*abbrev.*XOR)

Siehe:XOR

electronic document

electronic document (engl.) - elektronisches Dokument

cryptological assumption

cryptological assumption (engl.) - kryptologische Annahme

Entschlüsselungsalgorithmus

Entschlüsselungsalgorithmus - (engl.) decryption algorithm

Ein Entschlüsselungsalgorithmusist das Gegenstück zu einem Verschlüsselungsalgorithmus.

Es handelt sich dabei um eine Beschreibung, wie ein Geheimtext in den zugehörigen Klartext zu überführen ist. Verschlüsselungsalgorithmus und Entschlüsselungsalgorithmus treten immer paarweise auf, da einer ohne den anderen sinnlos. Beide können gleich sein und sich nur in der Reihenfolge ihrer Abarbeitung unterscheiden. Sie können aber auch völlig unterschiedlich sein.

Normalerweise arbeitet ein Verschlüsselungsalgorithmus mit zwei Eingaben: einem Geheimtext und einem Schlüssel. Heraus kommt dann der zugehörige Klartext.

decryption algorithm

decryption algorithm (engl.) - Entschlüsselungsalgorithmus

universal hashfunction

universal hashfunction (engl.) - universelle Hashfunktion

RACE [*Research and Development in Advanced Communication Technologies*]

Research and Development in Advanced Communication Technologies (engl.) - Foschung und Entwicklung im Bereich moderner Kommunikationstechnologie

RACEist ein Projekt der Europäischen Union. Darin geht es unter anderem um die Entwicklung und Bewertung von Verschlüsselungstechnologie. Im Rahmen von RACEwurde (wird) das RIPE-Projekt abgewickelt.

attack

attack (engl.) - Angriff

Einweg-Funktion mit Falltür

Einweg-Funktion mit Falltür - (engl.) trapdoor one-way function

Eine Einweg-Funktion mit Falltürist eine Einweg-Funktion, die zusätzlich die Bedingung erfüllt, daßbei Kenntnis einer zusätzlichen Information, der sogenannten Falltürinformation (trapdoor information), das Inverse relativ leicht gebildet werden kann. Ohne Kenntnis der Falltürinformationist es dagegen nahezu unmöglich, das Inverse zu einem Funktionswert zu ermitteln.

Anwendung

Der RSA-Algorithmus stellt eine Einweg-Funktion mit Falltürdar.

adversary

adversary (engl.) - *hier:*Angreifer; *auch:*Widersacher, Kontrahent

attacker

attacker (engl.) - Angreifer

Attackerist ein weniger gebräuchliches Synonym für *adversary*.

Benutzerkennung

Benutzerkennung - (engl.) user identifier (UID)

Die Benutzerkennung dient in Mehrbenutzersystemen (z.B. Linux) der eindeutigen Zuordnung von Ressourcen zu Benutzern.

trapdoor one-way function

trapdoor one-way function (engl.) - Einweg-Funktion mit Falltür

Datenschutz

Bundesdatenschutzgesetz - BDSG

``Neue Medien''

Multimediagesetz - IuKDG

Teledienstegesetz - TDG

Teledienstedatenschutzgesetz - TDDSG

Signaturgesetz - SigG

Signaturverordnung - SigV

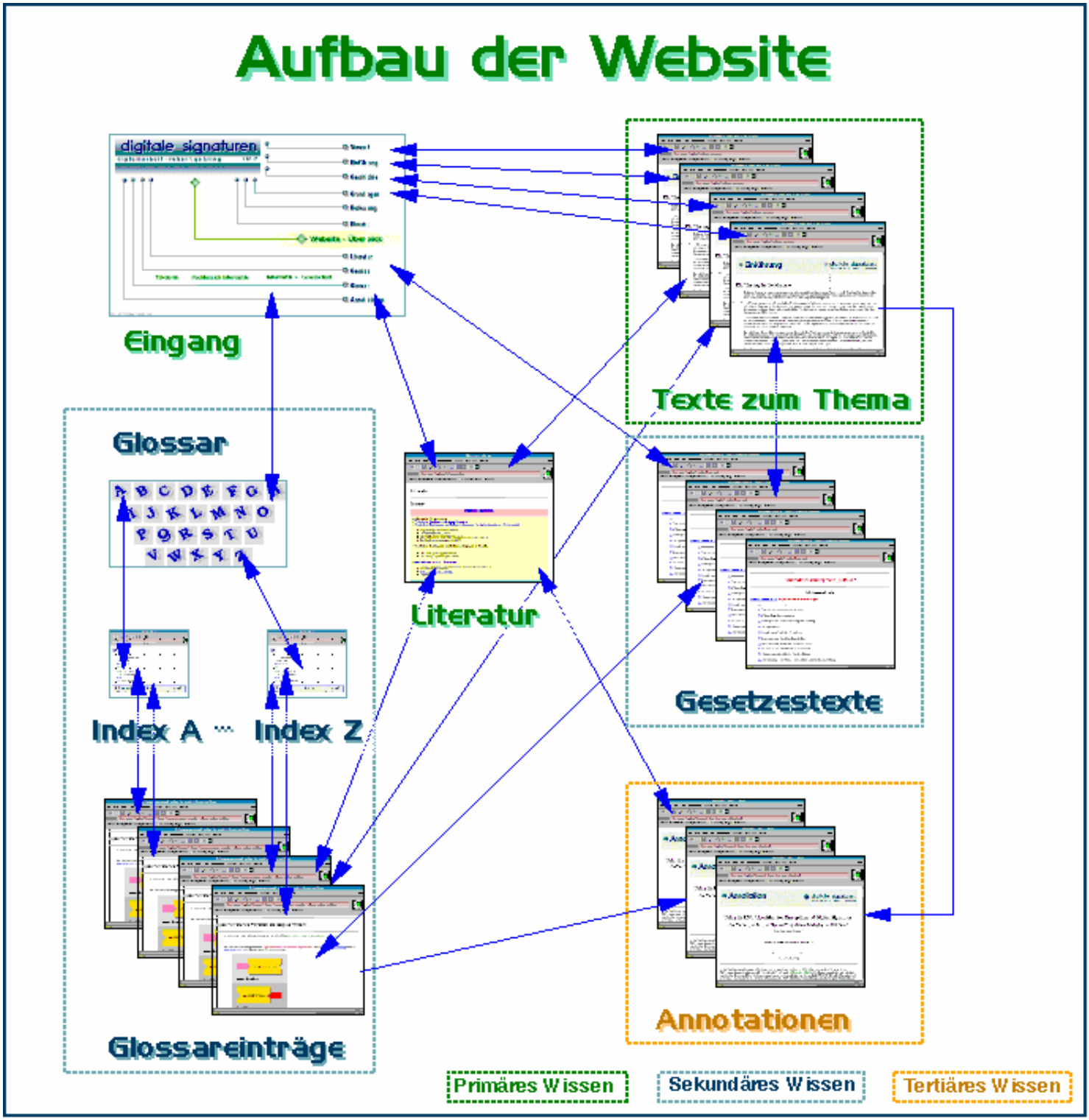
Telekommunikationsgesetz - TKG

Abhören

Fernmeldeverkehrüberwachungsverordnung - FÜV

Fernmeldeanlagengesetz - FAG

G10-Gesetz - G10G



Erläuterungen

Das ``Wissen", das auf dieser Website vorliegt, wurde so aufbereitet, daß es in mehrere, relativ eigenständige Bereiche zerfällt.

Da finden sich erstens die Texte, die sich unmittelbar dem Thema ``Digitale Signaturen" widmen. Diesen Bereich möchte ich als

`primäres Wissen' bezeichnen.

Erläuterungen zu einzelnen Begriffen, die dort Verwendung finden, würden für gewöhnlich in Fußnoten landen. Ich möchte solche Erläuterungen, die sich nicht nur auf das Thema `Digitale Signaturen' beziehen, als sekundäres Wissen bezeichnen. Sie wurden in einem Glossar zusammengefaßt und so strukturiert, daß das Glossar auch anderweitig verwendet werden kann. Ebenfalls in den Bereich `sekundäres Wissen' ordne ich Gesetzestexte ein, die speziell für den Einsatz in Hypertexten aufbereitet wurden. Auch diese sind vielfältig zu gebrauchen.

Zuletzt bleibt noch das übrig, was in obenstehender Grafik als `tertiäres Wissen' ausgewiesen ist. Dabei handelt es sich um einige Texte, die über den Rahmen des unmittelbar oder mittelbar notwendigen hinausgehen. Sie sollen den Zweck erfüllen, einen größeren Kontext zu illustrieren und so dem Leser helfen, das spezifische Thema im größeren Zusammenhang zu sehen. Auch finden sich hier Überlegungen mehr spekulativer oder prognostischer Natur. Man könnte sie als Anregungen zum Nach- und Weiterdenken auffassen.

Den Zusammenhalt zwischen primärem, sekundärem und tertiären Bereich stellen viele Hyperlinks her. Sollte der Leser einmal den Überblick verlieren, so gelangt er über einen Link am Ende jeder einzelnen Seite wieder zur Eingangsseite.

Einsatz Digitale Signaturen

Inhaltsverzeichnis

PGP

Einer der ältesten Einsatzzwecke digitaler Signaturen ist die Absicherung der Nachrichtenübermittlung im Internet: *email*, *news*und *ftp*. Der Zweck der Absicherung war und ist primär Qualitätssicherung durch Unterbindung versehentlicher oder absichtlicher Datenmanipulation. Überlegungen zur Beweissicherung für juristische Zwecke spielen dabei praktisch keine Rolle.

PGP (ausgeschrieben ``pretty good privacy'') ist ein Programm, das von Phil Zimmerman in den USA entwickelt wurde. Damit können digitale Signaturen erstellt werden, emails oder Dateien verschlüsselt werden. PGP arbeitet mit einem hybriden Verfahren.

Für die symmetrische Verschlüsselung der emails kommt IDEA zum Einsatz. Die IDEA-Sitzungsschlüssel werden mittels RSA verschlüsselt. Dateien lassen sich ebenfalls RSA-verschlüsseln, mit den bekannten Nachteilen der Public Key-Kryptographie. Digitale Signaturen werden durch hashen mit MD5 und anschließende RSA-Verschlüsselung erzeugt. PGP setzt zur Schlüsselverwaltung auf eine Netzstruktur (Web of Trust) und nicht auf eine Zertifizierungshierarchie.

Quellen:[Luckhardt 1997], [Klemm u.a. 1996], [Luckhardt/Bögeholz 1996]

Die Signaturfunktionalität von PGP kann auch zur Absicherung von Netzwerken eingesetzt werden.

Quelle:[Shecter 1997]

Elektronisches Grundbuch

Am 20. Dezember 1993 wurde das Registerverfahrensbeschleunigungsgesetz beschlossen. Dadurch wurden Rechtsgrundlagen für die Einführung eines elektronischen Grundbuchs geschaffen. Bis zu diesem Gesetz mußte das Grundbuch in Papierform geführt werden. Die Verantwortlichkeit für die Umsetzung liegt bei den einzelnen Bundesländern.

In mehreren Bundesländern (1996: Bayern, Sachsen, Sachsen-Anhalt, Hamburg) sind seitdem elektronische Grundbücher eingeführt worden oder befinden sich im Aufbau. Damit wurde die jahrhunderte alte Form des Grundbuchs (als Buch) abgelöst. Die Funktionen des Grundbuchs

- *``Stabilität*
- *Transparenz*
- *Vertrauen*

in den Rechtsverkehr an Grundstücken zu gewährleisten'' werden mittels elektronischer Dokumentenverwaltung umgesetzt. Zur Integritätssicherung und authentifizierten Wartung der Daten werden digitale Signaturen an Stelle der eigenhändigen Unterschrift des Grundbuchrechtspflegers eingesetzt. Erst durch diese digitale Signatur werden Einträge rechtskräftig. Uneingeschränkt lesenden Zugriff auf die Daten haben *``Gerichte, Behörden, Notare und öffentlich bestellte Vermessungsingenieure.''*Eingeschränkt lesenden Zugriff haben *``Kreditinstitute und Immobilienbesitzer.''* Der Zugriff erfolgt über ISDN-Leitungen. (Alle Zitate: [Göttlinger 1997])

Quelle:[Göttlinger 1997]

Datenaustausch im Bankwesen

Banken sind in besonderem Maße auf einen sicheren und authentischen Informationsaustausch angewiesen. Dafür kommen neben Verschlüsselungsverfahren im allgemeinen auch digitale Signaturen im besonderen zum Einsatz.

Der elektronische Datenaustausch findet u.a. statt:

- Bankintern;
- Von Bank zu Bank;
- Von der Bank zur Zentralbank;
- International;
- Beim Aktien- und Wertpapierhandel;
- Beim Homebanking;

In der Nachfolge des BTX-Systems wird ein neues Interface zur Bank für die Kunden entwickelt, das sogenannte ``Home Banking Computer Interface" (HBCI). Darin vorgesehen ist auch ein möglicher Einsatz digitaler Signaturen.

Quelle:[Glade 1997]

Datenaustausch im Gesundheitswesen

Der Einsatz hochautomatisierter Geräte im Gesundheitswesen führt dazu, daßeine Menge digitaler Daten anfallen. Diese sollen im Sinne des Patienten gesichert werden. Die Absicherung soll sowohl den notwendigen Vertrauensschutz, als auch die Integrität der Daten für eine korrekte Behandlung gewährleisten. Programme, die mit diesen Daten arbeiten, müssen selbstverständlich ihrerseits gegen Manipulationen geschützt sein. Mehrere, unterschiedliche Untersuchungs- und Behandlungsorte erfordern einen schnellen, sicheren Datenaustausch. Dazu kommen gesundheitspolitische Ziele, z.B. die

Krebsvorsorge, die ohne qualitativ hochwertige Daten nicht durchsetzbar sind. Computereinsatz in der medizinischen Praxis erfordert also Verschlüsselung und Signaturverfahren.

Die Umsetzung dieser Anforderungen werden u.a. durch folgende Systeme vorgenommen:

- **Health Professional Cards** (HPC): Jeder Versicherte verfügt inzwischen über eine elektronische Versicherungskarte mit Chip. In Zukunft sollen leistungsfähigere Chips zum Einsatz kommen, mit denen dann z.B. auch digitale Signaturen erzeugt werden können.
- **European Medical Data Interchange** (EMEDI): Ziel dieser europaweiten Vereinigung ist die Förderung des elektronischen Datenaustausches im Gesundheitswesen (``*Krankenhäuser, Laboratorien, Ärzte, Versicherungen, pharmazeutische Industrie und Lieferanten medizinischer Geräte sollen davon profitieren*" [Kruse 1997]).
- **Medical Network**: Ein von Ärzten gegründeter Verein, der die Vernetzung von Arztpraxen und Kliniken unterstützt.
- **Trusthealth 1:** EU-Programm zur Förderung des Vertrauens in öffentliche Telematik-Systeme im Medizinwesen durch Pilotprojekte. Dazu kommt kryptographische Technologie zum Einsatz.
- **Deutsches Krebsforschungszentrum** (Heidelberg): Mobile Datenerfassung für *Shared Care* (geteilte Pflege).

Quelle:[Kruse 1997]

Eine detaillierte Untersuchung von Rahmenbedingungen und Anforderungen der Datenverarbeitung im Gesundheitswesen findet sich bei [Pordesch/Schneider 1997].

Elektronische Steuerklärung

Im Zuge der Rationalisierung der Verwaltungen sollen Steuererklärungen auch elektronisch abgegeben werden können. Als Pendant zur rechtsverbindlichen, eigenhändigen Unterschrift der papiernen sollen bei der elektronischen Steuererklärung digitale Signaturen eingesetzt werden. Maßgeblich engagiert sich die Firma DATEVin diesem Bereich.

Quelle:[Kempf 1998]

Bedeutung Digitale Signaturen

zitat

``Digital signature schemes are cryptologic schemes that provide a similar function for digital messages as handwritten signatures do for messages on paper: They guarantee the authenticity of a message to its recipient, and the recipient can prove this authenticity to third parties, such as courts, afterwards. Hence digital signatures are necessary wherever legal certainty is to be achieved for digital message exchange." [Pfitzmann 1996]

Eingangsseite Mail
digitale signaturen diplomarbeit · robert gehring

Inhaltsverzeichnis

Grundlagen digitaler Signaturen

Vorwort

Diese Arbeit befaßt sich mit angewandter Informatik in einem weiten Sinne: Digitale Signaturen sind ohne Computer nicht realisierbar. Der breite Einsatz des Computers erfordert digitale Signaturen zur Absicherung aller Arten menschlicher Dokumentationstätigkeiten. Überlegt man sich, was alles unter `*Dokumentationstätigkeiten*' verstanden werden kann, ist es leicht einzusehen, daßdie Grundlagen digitaler Signaturen auf unterschiedlichen Gebieten zu suchen sind. *An dieser Stelle soll es darum gehen, die Zusammenhänge sichtbar zu machen, die den Einsatz digitaler Signaturen beeinflussen.*

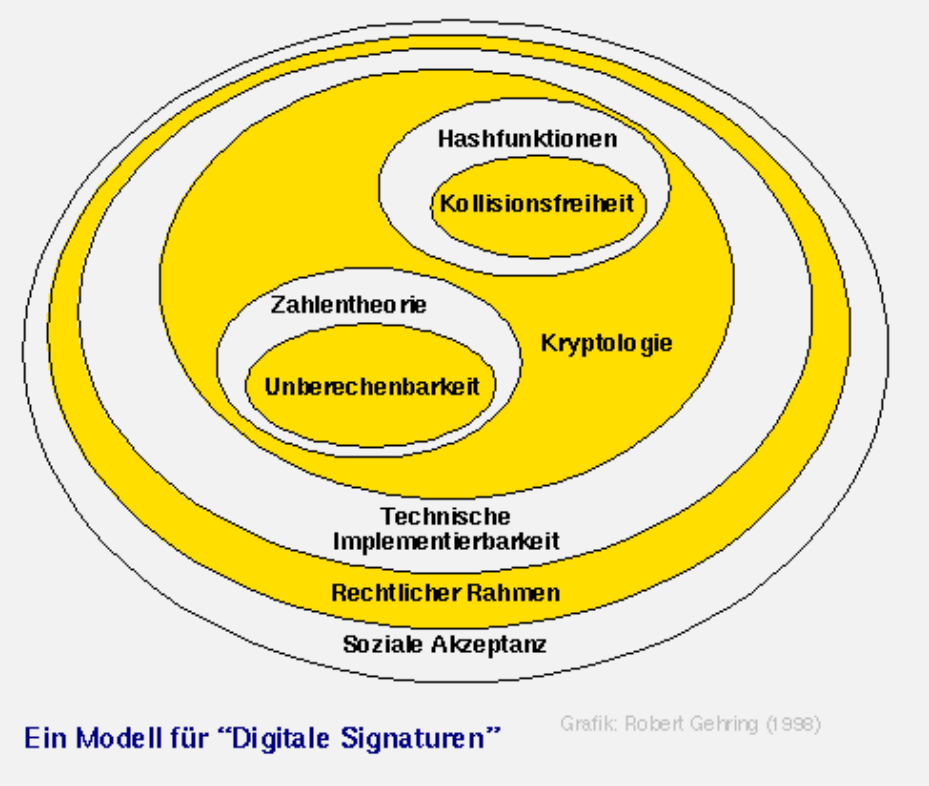
Grenzen der Betrachtung und Darstellung

Es soll nicht darum gehen, jedes Detail z.B. der zugrundeliegenden Zahlentheorieoder der optimalen Hardwareimplementierung von Hashfunktionenzu diskutieren. Auch soll nicht erschöpfend erörtert werden, wie sinnvoll oder unsinnig manche Abläufe im Rechtssystem sind. Bestimmte Fakten sind gegeben und zu akzeptieren. Der Schwerpunkt der Darstellung liegt darauf, Konzepte verständlich zu machen.

Das Modell

Zur Orientierung bei der Untersuchung der Zusammenhänge wurde ein Modell entworfen. ``Von Innen nach Außen'' werden darin die Erkenntnisse vager und die Aussagen unzuverlässiger. In der Konsequenz wird den sicheren Elementen des Modells mehr Aufmerksamkeit zuteil, als den schwerer einzuschätzenden. Mit dem Blick auf die Praxis scheint das paradox, aber auch symptomatisch für die Einführung neuer Technologie zu sein. In der Technikfolgeabschätzung scheint es großen Nachholbedarf zu geben.

Fragen nach der sozialen Akzeptanz ``digitaler Unterschriften'' in größeren Personenkreisen lassen sich bisher kaum beanworten. Ursache dafür ist der verhältnismäßig geringe Umfang des Einsatzes digitaler Signaturen in der Praxis. (Einige Beispiele wurden im Kapitel ``Einsatz digitaler Signaturen'' zusammengetragen.) Wo es dagegen einen relativ breiten Einsatz digitaler Signaturen gibt, fehlen systematische Untersuchungen zu den Erfolgen und Mißerfolgen. Generell läßt sich ein Mangel an empirischer Forschung konstatieren, was angesichts der allerorten prognostizierten Bedeutung digitaler Signaturen verwundert. Nicht zuletzt hemmt der nur langsam vorankommende Aufbau von Trustcentern (siehe z.B.: [Kempf 1998]) den erfolgreichen Einsatz der digitalen Signatur.



Erläuterung des Modells

Jede Erklärung setzt Worte und Begriffe voraus. Verständliche Erklärungen verwenden klare Worte und wohldefinierte Begriffe. → *Am Beginn dieser Arbeit wird die Terminologie definiert, ohne die ein Verständnis des Themas nicht möglich ist.*

Die innersten Kerne des entworfenen Schalenmodells werden vom Problem der Berechenbarkeit bestimmter mathematischer Zusammenhänge (Zahlentheorie) und dem der Kollisionsfreiheit bei Einweg-Hashfunktionen gebildet.

> Einige Bereiche der Zahlentheorie befassen sich mit Problemen, deren Lösung nicht trivial berechenbar ist. Ist der Aufwand zur Berechnung der Lösung eines solchen Problems praktisch nicht zu leisten, und gibt es keine alternativen Lösungsmöglichkeiten, kann man aus dem Problem eine Verschlüsselungsmethode ableiten.
>
> In der Informatik gab und gibt es oft einen Mangel an Speicherplatz oder verfügbarer Rechenzeit. Ein Ansatz, diesem Engpaß zu begegnen, war und ist die Entwicklung von Hashfunktionen zur komprimierten Speicherung und/oder zur Beschleunigung des Zugriffes auf gespeicherte Daten. Aus diesem Ansatz wurde eine Klasse von Hashfunktionen unter dem Kriterium der Kollisionsfreiheit von Kryptologen entwickelt.

→ *Die grundlegenden kryptologischen Ideen und Überlegungen werden skizziert.*

Für digitale Signaturen werden bestimmte Erkenntnisse der Kryptologen zu Zahlentheorie und Hashfunktionen kombiniert. Die Basis für digitale Signaturen bildet die asymmetrischen Verschlüsselung (auch Public Key-Verschlüsselung genannt). → *Deren Charakteristika werden dargestellt und gegen die der klassischen, symmetrischen Verschlüsselung abgegrenzt.*

Der Übergang von der Theorie zur Praxis erfolgt dabei fließend. → *Konkrete Verfahren werden vorgestellt und an ihrem Beispiel Konzepte verdeutlicht.*

Ein umfassender Einsatz digitaler Signaturen in der Praxis ist ohne einen geeigneten rechtlichen Rahmen nicht durchsetzbar. Im Sommer 1997 hat der Bundestag mit der Beschließung des Signaturgesetzes (SigG) einen Rahmen geschaffen. → *Dessen Aussagen, Wirkungsbereich und Eignung sollen an geeigneter Stelle untersucht werden.*

Terminologie

zitat

> ``*The scientific study of any discipline must be built upon rigorous definitions arising from fundamental concepts.*'' [Menezes/Oorschot/Vanstone 1997], S. 11

Um verbalen Mißverständnissen vorzubeugen, sollen zuerst grundlegende Termini definiert werden. Da ein Großteil der Fachliteratur in englischer Sprache vorliegt, werden die den deutschen korrespondierenden englischen Begriffe in Klammern mit eingeführt. In der Informatik -wie anderswo auch- ist es mittlerweile üblich, englische Begriffe wie deutsche einzusetzen. Einheitliche Standards haben sich dafür leider noch nicht etabliert.

Geheimhaltung, Sicherheit, Sicherheitskriterien

zitat

> ``*... nur auf dem Hintergrund von offengelegten Zwecken und Werten kann sinnvoll von Sicherheit gesprochen werden; ...*'' [Biskup 1993]

Unter **Geheimhaltung**(privacy, confidentiality) versteht man das Verbergen von Informationen vor allen Personen außer vor denjenigen, für die solche Informationen bestimmt sind. **Sicherheit**(security) ist das Ziel der Geheimhaltung, aber auch das Mittel. Ziel ist es insofern, als

die Geheimhaltung einem Zweck dient, den es abzusichern gilt. Mittel ist in dem Sinne, daßnur sichere Systeme geeignet sind, Geheimhaltung zu ermöglichen.

Im kryptographischen Sinne wird der Begriff der Sicherheit auf eingesetze Systeme, Verfahren und Protokolle bezogen.

Sicherheitskriterien (security criteria) werden entworfen, um die Sicherheit von Systemen, Verfahren und Protokollen einheitlich bewerten zu können. Oft werden sie in Katalogen zusammengefaßt und so formalisiert wie z.B. in den ITSEC-Kriterien oder im ``Orange book'' des US-Departement of Defense (DoD).

Sicherheitsmodelle

zitat

> *``The confidence level in the amount of security provided by a primitive or protocol based on computational or ad hoc security increases with time and investigation of the scheme.''* [Menezes/Oorschot/Vanstone]

Sicherheitsmodelle (security models) liegen dem Entwurf von Sicherheitskriterien zugrunde. Sie werden aus theoretischen Überlegungen oder den jeweiligen, konkreten Sicherheitsanforderungen abgeleitet. Erfahrungen aus der Praxis tragen ihren Teil zur Entwicklung der Modelle bei.

[Menezes/Oorschot/Vanstone], S. 42, 43 unterscheiden fünf Modelle zur Sicherheitsevaluierung:

1. **Uneingeschränkte Sicherheit** (unconditional security), bei der ein potentieller Angreifer mit unbegrenzter Rechenleistung erfolglos bleibt;
2. **Komplexitätstheoretische Sicherheit** (complexity-theoretic security), bei der ein potentieller Angreifer über polynomiale Rechenleistung verfügt und erfolglos bleibt;
3. **Überprüfbare Sicherheit** (provable security), bei der ein Nachweis erbracht werden muß, daß sie der Lösung eines gut bekannten, schwierigen Problems entspricht (z.B. dem Faktorisierungsproblem);
4. **Berechenbare Sicherheit**, bei der die notwendige Rechenleistung die höhstens verfügbare Rechenleistung eines potentiellen Angreifers signifikant übersteigt;
5. **Ad hoc-Sicherheit**, bei der für einen potentiellen Angreifer ein gewisses, fixes Maß an verfügbarer Rechenleistung angenommen wird, und er dennoch erfolglos bleibt;

Alle Modelle zielen auf die Sicherheit eines Systems/Verfahrens/Protokolls ab.

[**Anmerkung:** Genaugenommen handelt es sich bei den aufgeführten, konkreten Modellen nicht um Modelle. Dafür sind zu allgemein und abstrakt gehalten. Eine Charakterisierung als `Paradigmen' wäre vielleicht zutreffender.]

Informationsintegrität, Authentifizierung, Unabweisbarkeit

Die Garantie der **Informationsintegrität**(information integrity), durch die Verhinderung der Verfälschung von Informationen jedweder Art, spielt in einer Informationsgesellschaft eine überragende Rolle. Von besonderer Bedeutung sind außerdem die Feststellung der Herkunft einer Information, d.h. **Authentifizierung** [1](authentication), und die Möglichkeit, Abstammung/Erhalt und Integrität unabstreitbar zu beweisen (non-repudiation).

[**Anmerkung:** Anstelle von Unabweisbarkeit wird oft auch `Nachweisbarkeit' verwendet. Allerdings wird Nachweisbarkeit auch abweichend benutzt, so daß ich der Klarheit zuliebe bei `Unabweisbarkeit' bleiben werde. Der Begriff der Authentifizierung wird in vielen Zusammenhängen und sehr unterschiedlich benutzt. In einem engen Sinne bezieht er sich auf die bloße Herkunft einer Information. Etwas weiter ausgedehnt, umschließt er noch die Feststellung der Unveränderheit einer Information, d.h. die Sicherstellung ihrer Integrität. Maßgeblich ist,

wie so oft, der Kontext des Gebrauchs.]

Verschlüsselung, Entschlüsselung, Verschlüsselungsverfahren

Mit **Verschlüsselung**(encryption) bezeichnet man den Vorgang, eine verständliche Information reversibel in eine unverständliche Nachricht (s.u.) zu transformieren. Die Verschlüsselung stellt somit eine parametrisierte Funktion dar, deren Parameter der Klartext und der Schlüssel sind.

Entschlüsselung (decryption) beschreibt den umgekehrten Vorgang, bei dem aus der unverständlichen Nachricht die darin enthaltene Information zurückgewonnen wird. Auch die Entschlüsselung ist eine parametrisierte Abbildung. Ihre Parameter sind Schlüssel und Geheimtext.

Je nach Verfahren, handelt es sich um einen Schlüssel in zwei Kopien oder um zwei unterschiedliche Schlüssel, die zum Einsatz kommen.

Verschlüsselung/Entschlüsselung stellt eine Möglichkeit dar, um Geheimhaltung (z.B. bei der Kommunikation) zu wahren.

Ein **Verschlüsselungsverfahren** (encryption scheme, cipher) setzt sich aus dem Verfahren für die Verschlüsselung und dem für die Entschlüsselung zusammen. Damit folgen wir der Definition in [Menezes/Oorschot/Vanstone 1997].

[**Anmerkung:** Verbal besteht da ein gewisser Widerspruch. Es ist aber einsichtig, daß eine Verschlüsselung ohne zugehörige Entschlüsselung sinnlos ist, da jegliche Information verloren gehen würde. Eine einzige sinnvolle, jedoch unpraktische Anwendung ist denkbar. Mann kann eine Information verschlüsseln und den entstehenden Geheimtext zusammen mit dem Klartext aufbewahren (übermitteln etc.). Zur Prüfung der Integrität kann man jederzeit den Klartext erneut verschlüsseln und das Resultat mit dem vorhandenen Geheimtext vergleichen. Zeigen sich keine Differenzen, so ist die Integrität gewahrt worden. Allerdings hat sich die zu handhabende Informationsmenge auf diesem Wege stark vergrößert. Der Einsatzbereich für solche Verfahren wird deshalb stark eingeschränkt sein (z.B. `challenge and response'-Verfahren)].

Schlüssel, Schlüsselraum, Protokoll

Bei einem **Schlüssel**(key) handelt es sich um eine Information (genauer gesagt um eine nichtleere Menge an Information) die zur Steuerung von Verschlüsselung und Entschlüsselung benutzt wird. Ohne Schlüssel ist eine Verschlüsselung bzw. Entschlüsselung nicht möglich. Die Menge aller Schlüssel, mit dem ein Verschlüsselungsverfahren arbeitet, heißt **Schlüsselraum**(key space).

In der einen oder anderen Art und Weise wird der Schlüssel für die Entschlüsselung zur Verfügung gestellt. Dazu wird eine Vorgehensweise vereinbart, ein **Protokoll** (protocol). Nahezu alle Abläufe bei verschlüsselter Kommunikation werden durch Protokolle geregelt. So gibt es Festlegungen daß der Schlüssel für die Verschlüsselung beim Inhaber zu verbleiben hat, um eine unbeabsichtigte Aufdeckung, d.h. Kompromittierung (compromisation) möglichst zu verhindern. Auch kann dadurch die Wahrscheinlichkeit eines unbefugten Zugriffs (unauthorized access) auf den Schlüssel verringert werden.

Schlüssellebensdauer, Kryptoperiode

Von einem Schlüssel wird gesagt, daßer eine gewisse **Lebensdauer**(key lifetime) hat. Beeinflußt wird diese durch systematische Faktoren wie der Entwicklung der Arbeitsgeschwindigkeit von Computern, zunehmender Vernetzung mit der Möglichkeit der verteilten Schlüsselsuche und der Weiterentwicklung kryptanalytischer Verfahren. Hinzu kommen unsystematische Einflüsse wie z.B. ein nachlässiger Umgang mit Verschlüsselungstechnik oder schlicht Unerfahrenheit der Benutzer.

Die abschätzbare, zeitliche Sicherheit eines Verschlüsselungsverfahrens wird als **Kryptoperiode** (cryptoperiod) bezeichnet. Schlüssellebensdauer und Kryptoperiode sind nicht gleichzusetzen. Innerhalb der Kryptoperiode sollte ein Schlüssel mehrfach ausgewechselt werden, um Angriffe zu erschweren.

Kryptologie, Kryptographie, Kryptanalyse, Steganographie

Kryptographie (cryptography) beschäftigt sich mit der Geheimhaltung von Informationen durch Verschlüsselung.

Die Kryptographie ist ein Gebiet der **Kryptologie** (cryptology). Das Wort ist griechischer Abstammung. `crypto graphein' bedeutet `geheimes Schreiben'. Wir verwenden im gleichen Sinne den Ausdruck `verschlüsseln' (encrypt), `chiffrieren' (encipher) oder auch `codieren' (encode).

Die Kryptologie umfaßt weiterhin das Gebiet der **Kryptanalyse** (cryptanalysis), die sich mit dem unbefugten Lesbarmachen verschlüsselter Nachrichten beschäftigt, sprich: mit dem Entschlüsseln (decrypt, decode, decipher).

Neuerdings kommt die **Steganographie** (steganography) hinzu, die sich -wortwörtlich- mit dem `versteckten Schreiben' (griechisch: `stegano graphein') befaßt. Dabei geht es darum, die Tatsache, daß eine Information übermittelt wird, geheimzuhalten.

> [**Anmerkung:** Erreichen will man das z.B. durch die Modifikation von Bits in den Daten von Bildern. Nur, wer eingeweiht ist, kann den Bildern die Informationen wieder entnehmen.]

Nachricht, Klartext, Geheimtext

Die Information in der übermittelten, verschlüsselten Form nennen wir **Nachricht**(message). In einer intelligiblen, d.h. dem Menschen ohne Schlüssel und Entschlüsselung verständlichen Form wird sie als **Klartext**(plaintext) bezeichnet. **Geheimtext**(ciphertext) heißt sie, wenn sie nicht ohne Schlüssel und Entschlüsselung verständlich ist.

Eine Information liegt in unserem Verständnis vor der Verschlüsselung als Klartext vor, nach der Verschlüsselung als Geheimtext. Aus dem Geheimtext wird durch Entschlüsselung der Klartext gewonnen. Der Geheimtext auf dem Weg vom Sender zum Empfänger wird Nachricht genannt.

> [**Anmerkung:** Verschiedentlich wird in der Fachliteratur nicht zwischen der verschlüsselten und der unverschlüsselten Form der Information unterschieden, wenn von Nachricht die Rede ist. Um Verwirrungen zu vermeiden, werden wir Nachricht immer, wenn nicht anders angegeben, für `verschlüsselte, versandte Information' verwenden. In unserem Sinne wird also durch Verschlüsselung und Absendung einer Information daraus eine Nachricht und durch Entschlüsselung aus einer empfangenen Nachricht eine Information.]

Sender, Empfänger, Kanal

Eine Nachricht wird von einem (Ab-) **Sender**(sender) an den **Empfänger**(receiver) geschickt. In der Regel verschlüsselt der Sender eine Information, und der Empfänger entschlüsselt sie. Der Weg der Übertragung vom Sender an den Empfänger heiß**Kanal**(channel).

Unsicherer Kanal, sicherer Kanal

In einer Welt hochgradiger Vernetzung gibt es viele Möglichkeiten, Zugang zu einem Übertragungskanal zu bekommen. Deshalb geht man davon in der Regel aus, daßder Kanal unsicher ist (insecure channel, unsecured channel). Sollte es einen Weg abgesicherter Kommunikation geben, so stellt dieser einen sicheren Kanal (secure channel, secured channel) dar.

Klartextalphabet, Klartextraum, Geheimtextalphabet, Geheimtextraum

Das **Klartextalphabet** (plaintext alphabet) enthält die Menge aller Zeichen, aus denen ein Klartext bestehen kann. Beispiel: Ein Binärcomputer arbeitet mit Bitfolgen, d.h. sein Alphabet besteht aus der Menge {0,1}. Der **Klartextraum** (plaintext space) wird dann aus der Menge aller Zeichenfolgen gebildet, die für Sender und Empfänger eine sinnvolle Information darstellen, im Falle des Binärcomputers die Menge aller sinnvollen Folgen aus 0 und 1.

Analog umfaßt das **Geheimtextalphabet** (ciphertext alphabet) alle Zeichen, aus denen ein Geheimtext gebildet werden kann. Alle Zeichenfolgen, die entstehen können, wenn die Zeichenfolgen aus dem Klartextraum verschlüsselt werden, bilden den **Geheimtextraum** (ciphertext space).

Klartextalphabet und Geheimtextalphabet können gleich sein, aber auch unterschiedlich.

[**Anmerkung:** Diese Definitionen decken sich nicht unbedingt mit verschiedenen Definitionen aus der Fachliteratur (siehe z.B. [Menezes/Oorschot/Vanstone 1997]). Dies hat den Grund, daß sie semantisch und nicht allein syntaktisch gegeben werden. Eine syntaktische Definition für den Klartextraum würde alle möglichen Zeichenfolgen aus dem Klartextalphabet zulassen, nicht nur alle sinnvollen. Gleiches gilt für den Geheimtextraum. Dies steht in gewissem Widerspruch zur Praxis.]

Angriff, Angreifer, Manipulation

Ein **Angriff**(attack) ist der Versuch, auf die Geheimhaltung Einflußzu nehmen, um die Sicherheit zu gefährden. Bei Angriffen wird z.B. versucht, an die geheimgehaltene Information zu gelangen und/oder die Nachricht zu manipulieren.

Der **Angreifer** (attacker, adversary) ist derjenige, der die Geheimhaltung unterlaufen will. Bei der Entwicklung eines Verschlüsselungsverfahrens (encryption scheme) stellt der Angreifer die Fiktion dar, an dessen gemutmaßtem Verhalten sich der Kryptograph (cryptographer) orientiert.

In der Praxis handelt es bei Angreifern sich um reale Personen und Institutionen, die an geheime Informationen gelangen wollen. Dazu führen sie eine z.B. Kryptanalyse (cryptanalysis) durch. Derjenige, welcher diese vornimmt, heißt Kryptanalytiker (cryptanalyst). Andere Angriffe sind Versuche, Schlüssel zu stehlen oder die Unachtsamkeit im Umgang mit Schlüsseln auszunutzen.

Die meisten Angriffe sind passiv, d.h. sie zielen darauf ab, Kenntnis von der Information zu erlangen, die sich in einer Nachricht verbirgt. Solche Angriffe bezeichnet man als Lauschangriffe und entsprechend den Angreifer als Lauscher (eavesdropper).

Aktive Angriffe stellen den Versuch dar, die Kommunikation zu stören. Formen davon sind das Zurückhalten von Nachrichten oder ihre (Ver-)Fälschung (**Manipulation**).

Angriffe auf Daten

In [Mund 1993]werden folgende ``*Elementaroperationen der Manipulation*'' aufgeführt (Die Einordnung der Operationen als aktiv oder passiv stammt von mir.):

- **Modifizieren** (*aktiver A.*)
- **Einfügen** (*aktiver A.*)
- **Löschen** (*aktiver A.*)
- **Ausforschen** (*passiver A.*)
- **Ersetzen** (*aktiver A.*)
- **Weitergeben** (*passiver A.*)
- **Wiedereinspielen** (*aktiver A.*)
- **Vorenthalten** (*aktiver A.*)
- **Ableiten** (*passiver A.*)
- **Zweckentfremden**
- **Leugnen** (*aktiver A.*)
- **Unterlassen** (*passiver A.*)

[**Amerkung:** Bezüglich der Zusammenstellung ließe sich diskutieren, ob man z.B. `Ausforschen' als eine Form der Manipulation ansehen sollte. Das führt an dieser Stelle jedoch zu weit.]

Angriffe auf Protokolle

[Menezes/Oorschot/Vanstone 1997]führen auf Seite 42 Angriffe auf Protokolle an. Dazu rechnen sie:

1. **Angriff mit bekanntem Schlüssel** (known-key attack), bei dem alte, bekannte Schlüssel benutzt werden, um an neue zu gelangen;
2. **Angriff durch Wiedereinspielung** (replay attack), bei dem aufgezeichnete Sitzungen später wieder eingespielt werden;
3. **Angriff mit falscher Identität** (impersonation attack), bei dem ein Angreifer unberechtigt in die Rolle eines (berechtigten)

Kommunikationsteilnehmers schlüpft;
4. **Wörterbuchangriff** (dictionary attack), bei dem Wörter aus einem `Wörterbuch' als Paßwort ausprobiert werden;
5. **Vorwärtssuche** (forward search attack), bei dem vermutete Klartexte verschlüsselt und mit einem verfügbaren Geheimtext verglichen werden;
6. **`interleaving attack'**, bei dem im Ablauf eines Authentifizierungsprotokolls Identitäten vorgespielt werden;

Private Key-Kryptographie, Public Key-Kryptographie, hybride Kryptographie

Die moderne Kryptographie unterscheidet zwei differierende Ansätze für verschlüsselte Kommunikation: symmetrische Kryptographie, auch Private Key-Kryptographie genannt, und asymmetrische Kryptographie, auch Public Key-Kryptographie genannt.

Private Key-Kryptographie

Von **Private Key-Kryptographie** (private-key cryptography, single-key cryptography) wird gesprochen, wenn für die Verschlüsselung und für die Entschlüsselung derselbe Schlüssel benutzt wird, bzw. die Schlüssel relativ leicht voneinander abgeleitet werden können (d.h. sie können *``computationally easy''*[Menezes/Oorschot/Vanstone 1997]voneinander abgeleitet werden). Dazu müssen Sender und Empfänger jeweils über eine Kopie des Schlüssels verfügen.

Beide Kopien des Schlüssels müssen geheim bleiben. Aus diesem Grunde werden sie als private Schlüssel (private keys) bezeichnet. Mancherorts findet man die Bezeichnung `symmetrische Schlüssel', die verdeutlichen soll, daß die Schlüssel voneinander ableitbar sind.

Private Key-Verschlüsselungsverfahren basieren auf der Kombination und iterativen Wiederholung relativ simpler Verfahrensschritte. Dazu gehören beispielsweise Permutation, Substitution, Transposititon, XOR, Addition, Multiplikation und Modulus.

Die Operationen der Ver- und Entschlüsselung sind prinzipiell symmetrisch, daher der Name `symmetrische Kryptographie' (symmetric cryptography). Die Bezeichnung `Private Key-Kryptographie' wurde unter Bezugnahme auf die notwendige Geheimhaltung des Schlüssels gewählt. Beide Begriffe werden synonym verwandt.

Beim Einsatz symmetrischer Verschlüsselungsverfahren liegt die große Schwierigkeit darin, daß vor der Übermittlung der Nachricht ein Weg gefunden werden muß, den Schlüssel zu übermitteln. Um zu verhindern, daß ein Angreifer in der Besitz des Schlüssels gelangt, muß die Übermittlung über einen sicheren Kanal erfolgen. Der Name für dieses Problem lautet Schlüsselverteilungsproblem (key distribution problem).

Permutation

Wird verschlüsselt, indem jedes Zeichen aus dem Alphabet durch ein anderes Zeichen aus dem Alphabet eineindeutig ersetzt wird, so spricht man von einer **Permutation**. Es handelt sich um einen Spezialfall der einfachen Substitution, bei der Klartextalphabet und Geheimtextalphabet identisch sind.

Substitution, Transposition, Produktverschlüsselung

Die zwei ältesten symmetrischen Verschlüsselungsverfahren sind **Substitution**(substitution cipher) und **Transposition**(transposition cipher). Bei der Substitution werden die Zeichen des Klartextes schematisch durch Zeichen aus dem Geheimtextalphabet ersetzt (substituiert).

Zu unterscheiden sind bei Substitutionen (nach [Schneier 1996], S.11, 12):

- **Einfache Substitution**, bei der jedes Zeichen aus dem Klartextalphabet auf ein Zeichen aus dem Geheimtexalphabet abgebildet wird;
- **Homophone Substitution**, bei der Zeichen aus dem Klartextalphabet auf mehrere Zeichen aus dem Geheimtextalphabet abgebildet werden;
- **Polygraphische Substitution**, bei der Zeichengruppen aus dem Klartext auf Zeichen(gruppen) des Geheimtextalphabets abgebildet werden;
- **Polyalphabetische Substition**, bei mehrere Substitutionen mit unterschiedlichen Geheimtextalphabeten durchgeführt werden;

Für Substitutionen wurden schon relativ früh Maschinen entwickelt. Deren Evolution gipfelte in den Rotormaschinen, wie sie z.B. auch die

Enigma darstellte. Die Enigma wurde im zweiten Weltkrieg von den Deutschen zur Verschlüsselung ihrer Kommunikation benutzt.

Durch Transposition werden die Zeichen des Klartextes schematisch an eine andere Position gesetzt. Einfache Transpositionen sind:

- **Spaltentransposition**, wobei Teile des Klartextes spaltenweise vertauscht werden;
- **Zeilentransposition**, bei der Teile des Klartextes zeilenweise vertauscht werden

[**Anmerkung:** Spalten- und Zeilentransposition kann man sich leicht anschaulich machen, wenn man eine Buchseite nimmt und z.B. jede gerade gegen jede ungerade Spalte bzw. Zeile austauscht. Wenn man anschließend versucht, den so entstandenen ``Geheimtext'' zu lesen, wird man verstehen, was Transposition bedeutet.]

Kombiniert man beide Verfahren, z.B. indem erst eine Substitution und danach eine Transposition vorgenommen werden, so erhält man eine Produktverschlüsselung (product cipher). Die Transposition benötigt relativ viel Speicherplatz, da man den kompletten Geheimtext auf einmal verschlüsselt. Aus diesem Grunde ist sie nicht so verbreitet, wie die Substitution.

Diffusion und Konfusion

Diffusion(diffusion) und **Konfusion**(confusion) sind Begriffe, die aus der Informationstheorie stammen und auf deren Begründer, *Claude Shannon*, zurückgehen.

Konfusion bezeichnet die `Verschleierung' der Zusammenhänge zwischen Klartext, Schlüssel und Geheimtext. Mit Diffusion wird die Verteilung der in einem Klartext enthaltenen Redundanzen im zugehörigen Geheimtext beschrieben. In jeder Sprache tauchen z.B. bestimmte Buchstaben mit gewissen Häufigkeiten auf, ebenso Buchstabenfolgen. Würden diese Häufigkeiten unverändert im Geheimtext widergespielt werden, hätten die Kryptanalytiker leichtes Spiel.

Substitutionen erzeugen Konfusion, Transpositionen Diffusion. Die meisten symmetrischen Verschlüsselungsverfahren setzen auf komplizierte Substitionen, weniger auf Transpositionen. Durch wiederholte Anwendung der einzelnen Verfahrensschritte (in Runden/rounds) soll die bestmögliche Verschlüsselung erreicht werden. Transpositionen sind wegen ihres großen Speicherbedarfs von geringerer, praktischer Bedeutung.

XOR

XORist eine logische Operation, bei der zwei Eingabewerte zum Ergebnis `wahr' führen, wenn sie sich unterscheiden. Sind sie dagegen gleich, so liefert die XOR-Funktion die Ausgabe `falsch'. Auf der Ebene binärer Ein- und Ausgabewerte eines Computers ist die Funktion folgendermaßen definiert: f(1,1) = 0; f(0,0) = 0; f(1,0) = f(0,1) = 1.

Addition, Multiplikation

Diese zwei elementaren Operationen sind algebraisch definiert, wie in der Schule gelernt.

Modulus

Rechnen mit Modulen ist ganzzahliges Rechnen ``mit Rest''. Auch das sollte in der Schule vermittelt worden sein.

[**Beispiel (modulare Reduktion):** 3 mod 2 = 1; 5 mod 3 = 2]

Durch modulares Rechnen kann mit sehr großen Zahlen operiert werden. Bei Computern, deren Möglichkeiten zu Zahlendarstellungen begrenzt sind, ist dies eine wichtige Eigenschaft. ([Schneier 1996], S.284)

Vorteile, Nachteile von Private Key-Verfahren

Vorteile von Private Key-Verfahren sind vor allem zu sehen in:

- Gute Implementierbarkeit auf Basis einfacher Elementaroperationen;
- Hoher Datendurchsatz;
- Kurze Schlüssellänge;
- Sicheres, lange untersuchtes kryptologisches Fundament;

Nachteile existieren ebenfalls. Die wesentlichen sind:

- Das Schlüsselverteilungsproblem kann nur mit einem sicheren Kanal gelöst werden.
- Die Schlüssel müssen an zwei Stellen, bei Sender und Empfänger geheimgehalten werden
- Digitale Signaturen lassen sich nur schwer realisieren.
- Man benötigt neue Schlüssel für je ein Paar aus Sender und Empfänger.

Public Key-Kryptographie

Bei der **Public Key-Kryptographie** (public key cryptography) kommt für die Verschlüsselung ein Schlüssel zur Anwendung, für die Entschlüsselung ein anderer. Schlüssel werden als Paar benutzt. Ein Schlüssel aus dem Paar muß geheim bleiben. Dieser heißt privater Schlüssel (private key). Der andere Schlüssel, der nicht notwendig geheim bleiben muß heißt öffentlicher Schlüssel (public key). Die Ungleichheit der Schlüssel hat zu der Bezeichnung `*asymmetrische Schlüssel*' geführt.

Ein alternativer Name für die Public Key-Kryptographie ist *asymmetrische Kryptographie* (asymmetric cryptography). Er spiegelt wider, daß die Operationen für Ent- und Verschlüsselung nicht symmetrisch, sondern asymmetrisch sind. Grundsätzlich handelt es sich um nichtidentische inverse Funktionen und nicht um involutorische Funktionen (involution), d.h. es gilt: d(e(x)) = x, wobei e ungleich (!) d ist.

Elementare Bedeutung für die Implementierung von Verfahren für die Public Key-Kryptographie haben Einweghashfunktionen und Einwegfunktionen mit Falltür.

Hashfunktion, Einwegfunktion, Einweghashfunktion, Einwegfunktion mit Falltür

Eine **Hashfunktion** (hash function) ist eine Komprimierungsfunktion für Informationen. Sie berechnet aus Eingabewerten (Informationen) mit beliebiger Länge Ausgabewerte (Informationen) mit fixer Länge. Dabei ist die Länge der Ausgabewerte im Mittel kürzer, als die der Eingaben. In der Regel ist die Menge der möglichen Ausgabewerte deutlich kleiner, als die Menge der möglichen Eingabewerte. Die Komprimierung ist fast immer mit einem Informationsverlust verbunden.

> [**Anmerkung:** Die Hashfunktion in der Kryptologie ist nur bedingt mit der informatischen Hashfunktion vergleichbar. Die oben gegebene Definition gilt für kryptographische Hashfunktionen.]

Einwegfunktionen (one-way function) sind Abbildungen, deren Umkehrung praktisch nicht bestimmbar ist. Es ist bei Einwegfunktionen relativ leicht, den Funktionswert f(x) zu berechnen. Das Inverse $f^{-1}(x)$ läßt sich im Gegensatz dazu höchstens unter unbezahlbarem Rechenaufwand ermitteln.

Einweghashfunktionen (one-way hash function) vereinen die Eigenschaften beider vorgenannter Funktionstypen: Sie komprimieren ihre Eingabe, und aus der Ausgabe läßt sich nicht auf die Eingabe schließen.

> [**Anmerkung:** Anonyme Wahlen lassen sich in gewissem Sinne als Einweghashfunktionen interpretieren. Zuerst werden sämtliche Argumente pro oder contra Wahlgegenstand auf ein `dafür' oder `dagegen' reduziert, also komprimiert. Anschließend werden die `dafür'- und `dagegen'-``Ausgaben'' zusammengezählt, zum Wahlergebnis. Aus diesem läßt sich aber nicht mehr bestimmen, wer mit `dafür' und wer mit `dagegen' gestimmt hat, da es eine anonyme Wahl war.]

Einwegfunktionen mit Falltür (trapdoor one-way function) sind besondere Einwegfunktionen, bei denen es eine schlüsselgesteuerte, effektive Lösung für die Inversion gibt. In Unkenntnis des Schlüssels steht diese Lösung nicht zur Verfügung. Wegen dieser Eigenschaft spricht man oft auch von kryptographischen Falltüreinwegfunktionen. Einwegfunktionen mit Falltür sollten

nicht mit Einweghashfunktionen verwechselt werden.

Alle bedeutenden Public Key-Verschlüsselungsverfahren basieren auf Einwegfunktionen mit Falltür (z.B. RSA, ElGamal).

Digitale Signatur

Eine **digitale Signatur** (digital signature) ist eine Annotation (tag) zu einer Information. Die Annotation enthält verschlüsselte Aussagen zur Identität der Information. Anhand einer Überprüfung dieser Annotation, wozu ein Schlüssel benötigt wird, kann festgestellt werden, ob die Information unverändert geblieben ist. Die zu verschlüsselnden Aussagen über die Information erhält man durch die Anwendung einer Einweghashfunktion auf die Information.

Digitale Signaturen dienen der Authentifizierung von Kommunikation und der Identifizierung von Informationen. Sicherheit können sie nur zusammen mit einer geeigneten Schlüsselverwaltung bieten.

> [**Anmerkung:** Zwar gibt es auch Verfahren für digitale Signaturen, die auf symmetrischer Verschlüsselung basieren. Diese sind jedoch nicht für den Einsatz in offenen Netzen (z.B. Internet) geeignet. Dafür sind nur Public Key-Verfahren einsetzbar. Aus diesem Grunde werden `digitale Signaturen' im Rahmen der Public Key-Verschlüsselung eingeführt.]

Vorteile, Nachteile von Public Key-Verfahren

Vorteile von Public Key-Verfahren sind zu sehen in:

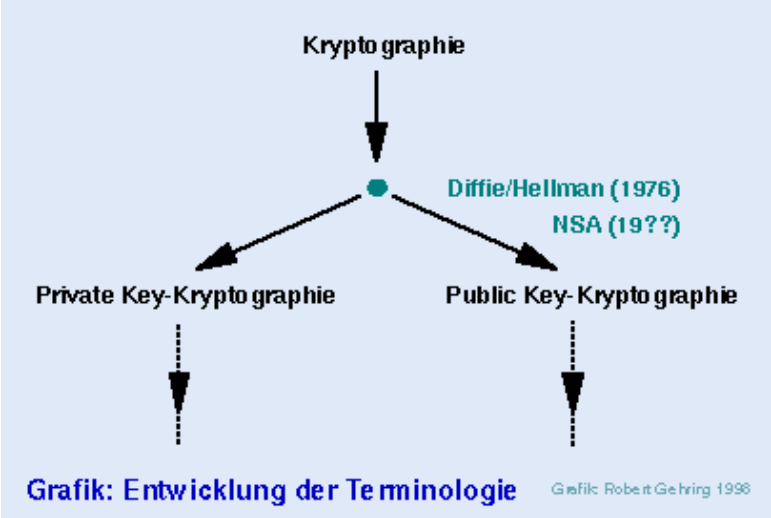
- Der geringeren Menge an geheimzuhaltener Information (nur privater Schlüssel) ggü. Private Key-Verfahren;
- Ihrer guten Eignung für die Konstruktion von Verfahren für digitale Signaturen;
- Im geringeren Aufwand für die Schlüsselverwaltung;
- Ihrer leichten Softwareimplementierbarkeit;
- Der -nach bisherigem Kenntnisstand- extremen kryptologischen Unangreifbarkeit;

Als Nachteile müssen gelten:

- Die im Vergleich zu Private Key-Verfahren großen Schlüssellängen ;
- Ein geringer Datendurchsatz bei der Ver- und Entschlüsselung;
- Daß die Sicherheit nach bisherigem Kenntnisstand nicht beweisbar ist;
- Daß sie aus kryptologischer Sicht erst sehr kurze Zeit existieren;
- Der Patentschutz für nahezu alle wichtigen Verfahren;

Begriffsabgrenzung

Public Key-Kryptographie hat sich historisch gesehen als Konsequenz aus der Private Key-Kryptographie entwickelt. Am Anfang war alle Kryptographie Private Key-Kryptographie. Deshalb gibt es die verbale Unterscheidung in Public Key-Kryptographie und Private Key-Kryptographie erst seit relativ kurzer Zeit. Vorher sprach man nur von Kryptographie.



Hybride Kryptographie

Von hybrider Kryptographie (hybrid cryptography) spricht man, wenn Public Key- und Private Key-Kryptographie kombiniert werden. Sie kommt zum Einsatz, um die Vorteile beider Arten auszunutzen und gleichzeitig ihre Nachteile zu kompensieren bzw. zu minimieren.

Verschlüsselungsmodi

Man unterscheidet prinzipiell zwei **Verschlüsselungsmodi**(encryption modes): Blockverschlüsselung (block encryption) und Stromverschlüsselung (stream encryption). Bei der Blockverschlüsselung werden Teile des Klartextes zu einem Block zusammengefaßt und dieser anschließend verschlüsselt. Bei einer Stromverschlüsselung werden die kleinsten logischen Einheiten (Bit, Byte, Wort, ...) des Klartextes als kontinuierlicher Datenstrom verschlüsselt.

Betriebsarten von Blockverschlüsselungsverfahren

Es gibt vier **Betriebsarten** (modes of operation) für Blockverschlüsselungsverfahren:

- ECB - Electronic Codebook mode;
- CBC - Cipher-block Chaining mode;
- CFB - Cipher feedback mode;
- OFB - Output feedback;

Diese Betriebsarten dienen unterschiedlichen Zwecken, wie z.B. Fehlerkorrektur oder statistischer Verschleierung der Zusammenhänge zwischen Klartextblöcken und Geheimtextblöcken.

Zertifizierung, Zertifikate, Zertifizierungsinstanzen

Unter **Zertifizierung**(certification) versteht man den Prozeßder eindeutigen Zuordnung von natürlichen Personen zu einem Paar Schlüssel für die asymmetrische Verschlüsselung. Dazu gehören die eindeutige Identifizierung der Person sowie der Nachweis der Person über den Besitz eines öffentlichen Schlüssels. Wurden diese Nachweise erbracht, so stellt eine **Zertifizierungsinstanz**(certification authority) einen formellen Beleg aus, das **Zertifikat**(certificate). Ein Zertifikat enthält im Minimum einen Vermerk über die Identität der Person und deren öffentlichen Schlüssel. Die Zertifizierungsinstanz hält die Zertifikate in einer Form bereit, daßein lesender Zugriff durch Dritte möglich ist, die sich von der Zuordnung eines öffentlichen Schlüssels zu einer Person überzeugen wollen. Sie verhindert gleichzeitig die unbefugte Veränderung der Einträge im Zertifikat.

[**Anmerkung:** In anderen Zusammenhängen ist auch viel von Zertifizierung und Zertifikaten die Rede, z.B. bei der Sicherheitsevaluierung von Computersystemen.]

Fehlerbegriffe

zitat

> *``Als Chiffrierfehler bezeichnet man nicht nur den Gebrauch eines zu naheliegenden Schlüssels, sondern alles, was dem unberufenen Entzifferer die Arbeit leicht macht.''* [Bauer 1994], S.130

Von einem **Fehler**kann man sprechen, wenn ein System/Protokoll in Gestaltung und/oder Bedienung nicht den Sicherheitsanforderungen gerecht wird, für die es konzipiert und entwickelt wurde. Durch das Ausnutzen von Fehlern können Angriffe erfolgreich durchgeführt werden.

In der Kryptologie lassen sich grundsätzlich zwei Kategorien von Fehlern unterschieden:

- Technische Fehler: Verfahrensfehler, Systemfehler, Implementierungsfehler;
- ``Menschliche'' Fehler: Protokollfehler (protocol failure) und Gebrauchsfehler;

Die Fehler in der ersten Kategorie gehen üblichweise auf die Handlungen von Experten zurück. So werden häufig Verschlüsselungsverfahren, Hashverfahren, Schlüsselauswahlverfahren etc. durch Analyse als fehlerhaft erkannt (siehe z.B. [Damgard/Knudsen 1994]). Nicht selten stellen sich auch Annahmen über die Sicherheit eines Systems oder einer Implementierungstechnologie als irrig heraus (siehe z.B. [Anderson/Kuhn 1996]) . Als technische Fehler werden sie hier bezeichnet, da sie dem System unabhängig von dessen Gebrauch anhaften.

Sollte ein Verfahren keine Fehler aufweisen, die in die erste Kategorie fallen, so besteht nach den Erfahrungen aus der Praxis immer noch eine große Wahrscheinlichkeit, daß Protokoll- und/oder Gebrauchsfehler auftreten. Einer der häufigsten Fehler ist die Kompromittierung eines geheimen Schlüssels. Andere, klassische Fehler sind die Akzeptanz falscher Identitäten oder die fehlerhafte Bedienung eines Verschlüsselungssystems (z.B. indem Schlüssel seltener als notwendig gewechselt werden). Die Unterlassung von vorgeschriebenen Überprüfungen ist gleichfalls ein `beliebter' Protokollfehler.

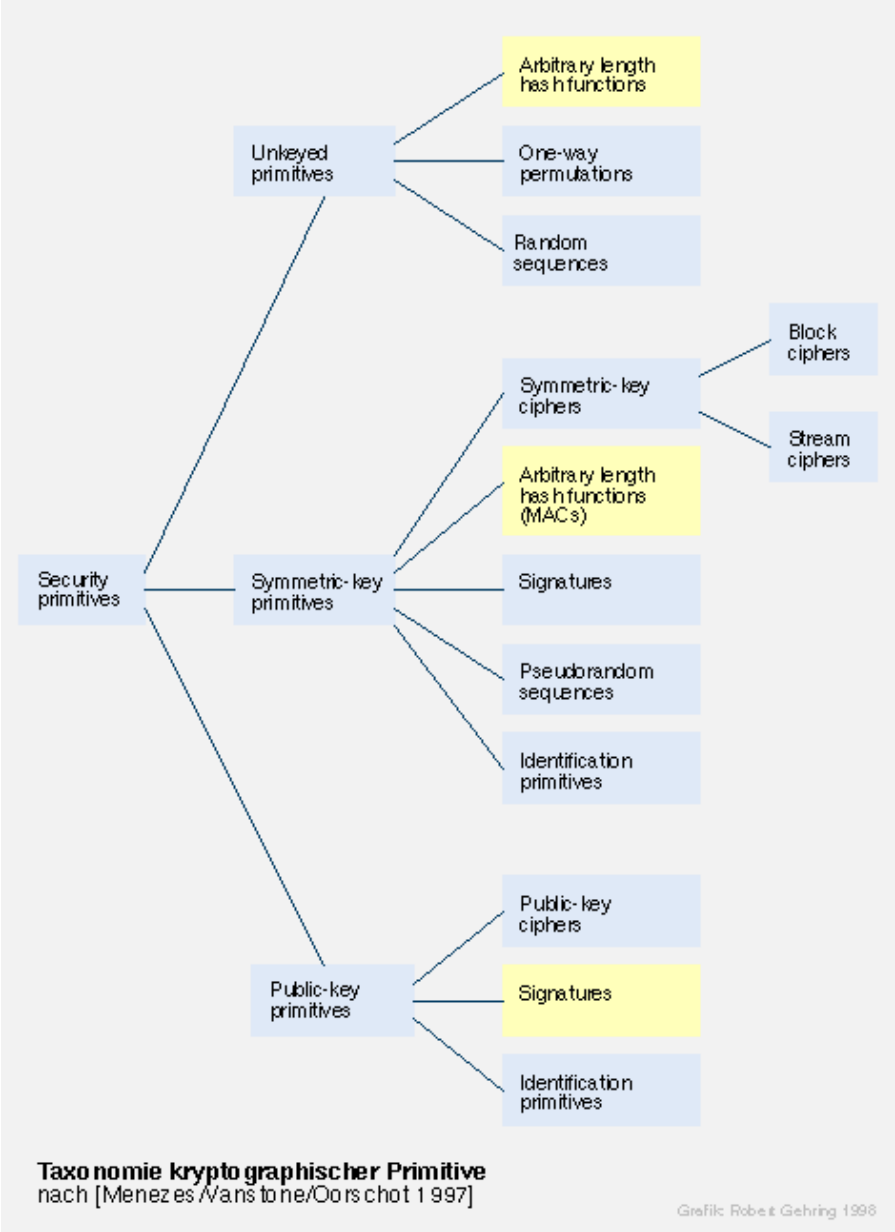
Im Einzelfall ist es nicht immer möglich, einen auftretenden Fehler eindeutig einer der beiden Kategorien zuzuordnen.

Zahlentheorie

Die **Zahlentheorie**ist das Gebiet der Mathematik, das sich mit den Eigenschaften ganzer Zahlen befaßt. Im Zusammenhang mit der Public Key-Kryptographie hat das Interesse an der Zahlentheorie deutlich zugenommen, da viele asymmetrische Verschlüsselungsverfahren auf klassischen Problemen der Zahlentheorie (z.B. diskrete Logarithmen bei ElGamal, Faktorisierung bei RSA) aufbauen.

Einordnung der Begriffe

Folgende Grafik, die nach [Menezes/Oorschot/Vanstone 1997], S. 5, gestaltet wurde, verschafft einen ersten Überblick über die Zusammenhänge.



(Die Elemente, die für digitale Signaturen von besonderer Bedeutung sind, wurden gelb hervorgehoben.)

Konzepte

Numerische Alphabete - Maschinenlesbarkeit

Sichere Verschlüsselung größerer Mengen von Informationen läßt sich nur unter Zuhilfenahme eines Computers druchführen. Da Computer Informationen als Zahlen verarbeiten, müssen die zu verschlüsselnden Informationen in eine maschinenlesbare Form gebracht werden. Wenn es um die Verschlüsselung von Texten geht, erfolgt die Umwandlung durch eine einfache Substitution. Dabei werden alle Zeichen des Klartextalphabets auf die Zeichen eines maschinenlesbaren Alphabets abgebildet. Üblicherweise greift man zu einem numerischen Alphabet, das durch die Stellung der Zeichen im Klartextalphabet definiert wird. Informatik-typisch wird die Zählung oft mit `0' begonnen:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Die Ordnung des Alphabets bleibt dadurch erhalten. Da eine getrennte Groß- und Kleinschreibung in den meisten Sprachen unbekannt ist, wird die Codierung auf Kleinbuchstaben (ggf. noch Ziffern und unverzichtbare Sonderzeichen) beschränkt. Auf einer solchen Substitution

bauen auch die Beispiele im Glossar, z.B. für RSA, auf. Kommt es darauf an, auch Leerzeichen verschlüsseln zu müssen, so wird dafür oft die `0' vergeben und die Stellung des `a' als `1', b als `2', c als `3', ... definiert.

Hat man ein eindeutiges numerisches Alphabet festgelegt, lassen sich die notwendigen mathematischen Operationen darauf definieren. Naheliegend ist es, deren Definition an der Algebra auszurichten. Die Addition von Zeichen wird als Addition ihrer Stellen definiert. Da Überläufe unvermeidlich sind, wird das algebraische Alphabet als zyklisch definiert. Nach dem z folgt also wieder das a.

Beispiel:

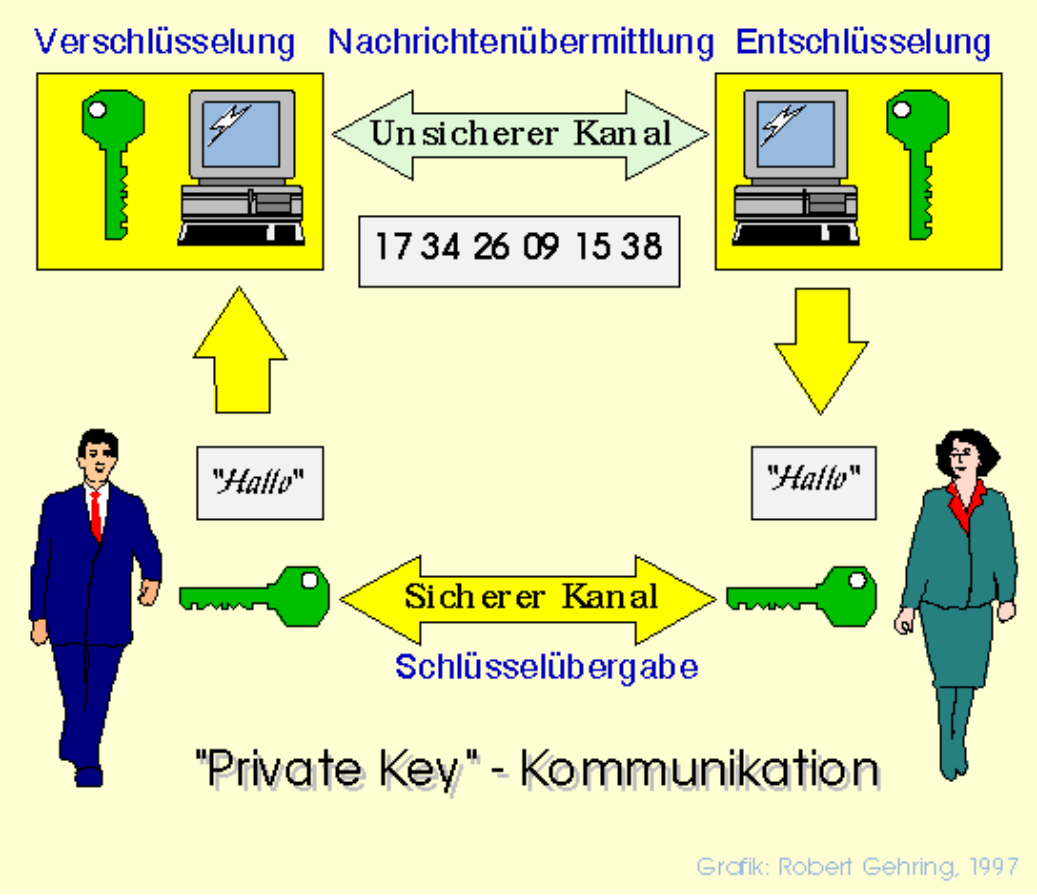
> Die Cäsar-Chiffrierung, benannt nach dem römischen Kaiser Julius Cäsar, war eine simple Addition. Dabei wurde jedes Zeichen im Alphabet durch das um drei Stellen versetzte Zeichen substituiert. Den Schlüssel stellte die Information `plus drei' dar. Aus dem `a' wurde dann das `d', aus dem `p' das `s' und aus dem `y' das 'b'. (Man beachte den Überlauf bei `y'!) Da römische Zahlen aus Buchstaben zusammengesetzt wurden, kam man mit dem normalen Alphabet aus. Eine solche Chiffrierung ist heute allenfalls noch zu Lehrzwecken interessant.

Diese allererste Substitution von Buchstaben durch Zahlen liegt praktisch jedem computergestützten Verschlüsselungsverfahren zugrunde. Häufig kommen jedoch nicht Dezimal- sondern Binärzahlen zum Einsatz. Die meisten Computer rechnen nun einmal binär.

Private Key-Kryptographie

Konzept der Private Key-Kryptographie

Private Key-Kryptographie arbeitet mit einem einzigen Schlüsselfür Verschlüsselungund Entschlüsselung, bzw. mit leicht voneinander ableitbaren Schlüsseln. Das Protokolleiner Kommunikation, die mit Private Key-Kryptographie abgesichert wird, wird in der Grafik schematisch gezeigt.



(Identische Schlüssel haben im Bild dieselbe Gestalt.)

Der Ablauf des Protokolls teilt sich in folgende Schritte auf (wenn zwischen Sender und Empfänger Einigkeit über das

Verschlüsselungsverfahren herrscht):

Vor der Kommunikation:

1. Auswahl des Verschlüsselungsverfahrens
2. Schlüsselgenerierung bzw. Schlüsselvereinbarung
3. geheime Schlüsselübergabe

Während der Kommunikation:

1. `Erzeugen' der Informationen
2. Verschlüsseln der Informationen zur Nachricht
3. Übermitteln der Nachricht
4. Entschlüsseln der Nachricht, Rezeption der Informationen

Nach der Kommunikation

1. Ggf. Vernichten der Informationen und der Nachricht
2. Ggf. Vernichten des Schlüssels

Unter der Annahme, daßdie empfangene Nachricht auch die abgesandte Nachricht ist, sowie daßnur Sender und Emfänger über den Schlüssel verfügen, kann davon ausgegangen werden, daßdie Nachricht authentisch ist. Einem Außenstehenden gegenüber kann allerdings nicht bewiesen werden, daßeine bestimmte Person eine Nachricht geschickt hat, da zwei Personen über denselben Schlüssel verfügen.

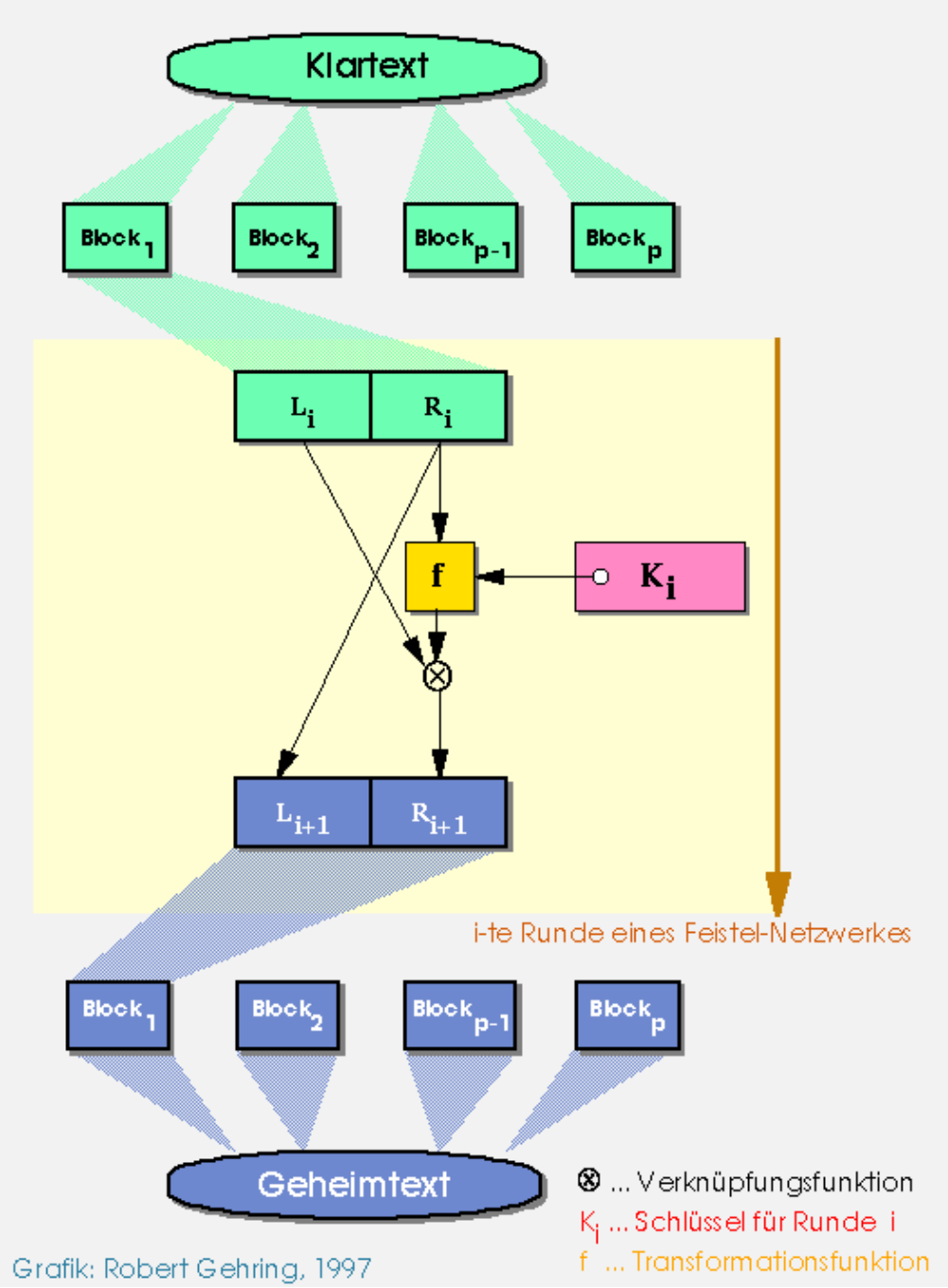
Runde

Symmetrische Verschlüsselungsverfahren verknüpfen elementare Verschlüsselungsoperationen. Ein solcher Verküpfungsschritt heißt **Runde**. Eine komplette Verschlüsselung besteht aus mehreren Runden. In den allgemeinen Definitionen war bisher immer von Schlüsseln die Rede. Oft wird für jede Runde in einem symmetrischen Verschlüsselungsverfahren ein anderer Schlüssel eingesetzt. Solche Schlüssel heißen dann Rundenschlüssel.

Die einzelnen Rundenschlüssel werden aus dem Sitzungsschlüssel abgeleitet. Letzterer kann auf unterschiedliche Arten zustande kommen, z. B. durch Festlegung oder durch Kombination aus einem fixen Anteil und einer Zufallszahl.

Feistel-Netzwerke

In vielen symmetrischen Verfahren bestehen die Runden aus Feistel-Netzwerken, benannt nach ihrem Erfinder *Horst Feistel*. Auf Feistel-Netzwerken baut auch DES auf. Schematisch sieht ein solches Netzwerk so aus:



Arbeitsweise eines Feistel-Netzwerks

Feistel-Netzwerke arbeiten mit Klartextblöcken. In einem ersten Schritt wird jeder Klartextblock in zwei Teile, linke (L) und rechte (R) Hälfte, zerlegt. Die rechte Hälfte (R) wird mit dem Rundenschlüssel (K) über eine Funktion (f) verknüpft. Das Ergebnis wird anschließend mit der linken Hälfte z.B. XOR verknüpft und zur neuen rechten Hälfte erklärt. Aus der (alten) rechten Hälfte wird ohne weitere Veränderung die neue linke Hälfte. Beide, neue linke und neue rechte Hälfte, bilden den Eingabeblock für die nächste Runde. Die Indizes i und i+1 kennzeichnen jeweils die i-te bzw. i+1-te Runde.

Derartige Netzwerke arbeiten sehr schnell und ermöglichen einen hohen Datendurchsatz. Die Verknüpfungsfunktion f kann dem jeweiligen Sicherheitsbedürfnis entsprechend gewählt werden. Eine entsprechende Anzahl von Runden mit ggf. unterschiedlichen Rundenschlüsseln und Verknüpfungsfunktionen ermöglicht eine hohe Sicherheit der Verschlüsselung.

DES als Beispiel

zitat

> ``*Der Data Encryption Standard (DES) ... stellt seit zwanzig Jahren einen weltweiten Standard dar. DES zeigt zwar einige Alterserscheinungen, hat jedoch jahrelanger Kryptanalyse erstaunlich gut widerstanden und bietet immer noch Schutz vor den meisten Angreifern, sofern diese ihre Attacken nicht höchst aufwendig gestalten.''* [Schneier 1996], S.309

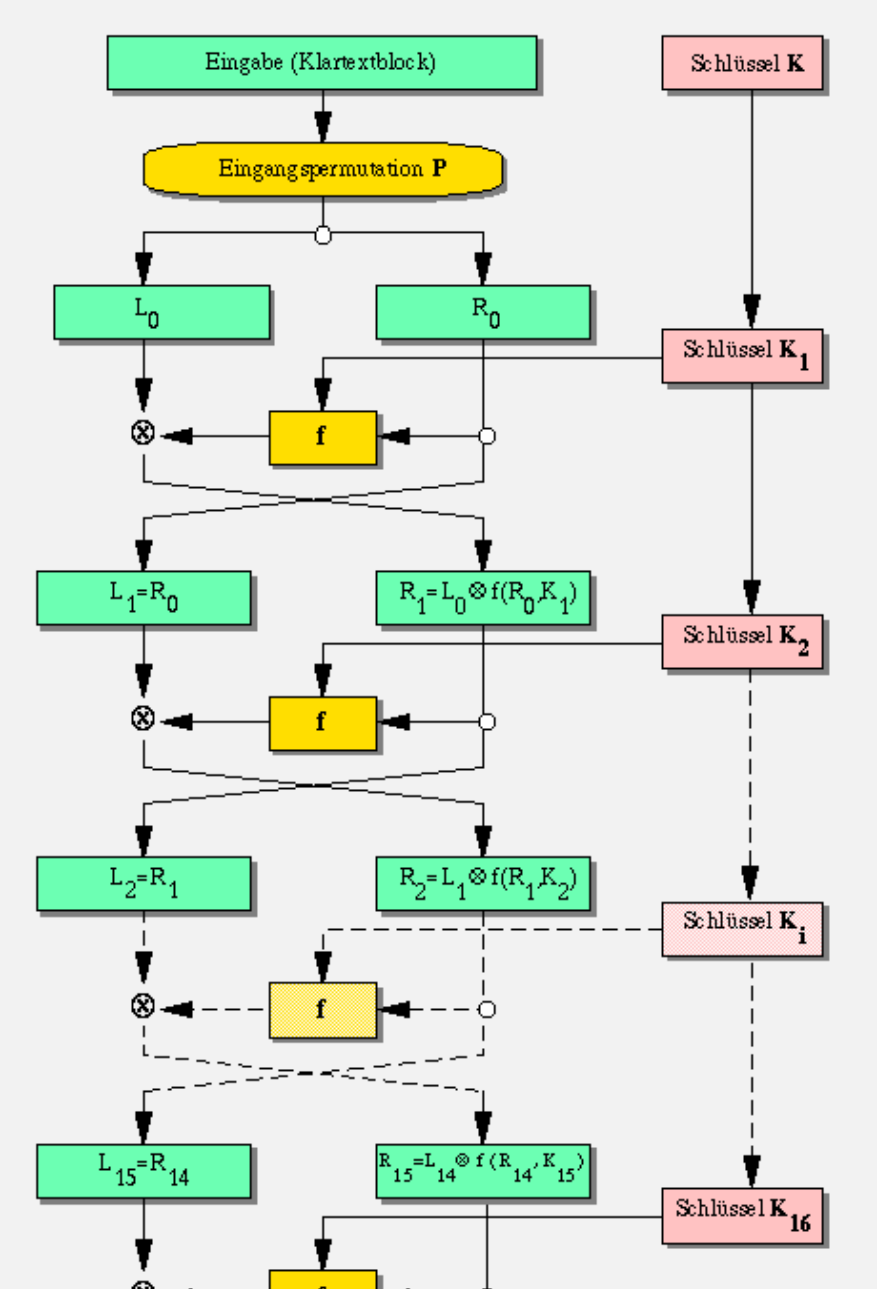
> ``*Eine Maschine zum Knacken von DES mittels Brute-Force, die einen Schlüssel in durchschnittlich 3,5 Stunden ermittelt, kostete 1993 nur 1 Mio. Dollar ...''* [Schneier 1996], S.349

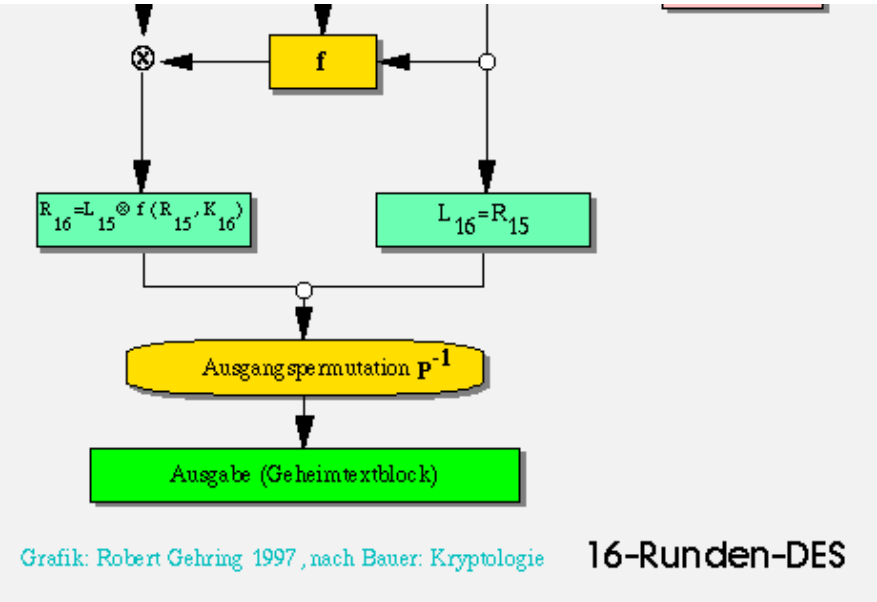
Das `klassische' symmetrische Verschlüsselungsverfahren ist DES.

DES wurde bereits in den 70'er Jahren entwickelt, ist effizient und weit verbreitet, z.B. im Bankensektor. Allerdings kann es bei kurzen Schlüssellängen nicht mehr als sicher gelten, wie bei verschiedenen Aktionen im Internet demonstriert wurde (z.B. RSA-Challenge [c't 6/1998]). Aus DES wurde z.B. Triple-DES entwickelt, das mit dreifacher Verschlüsselung eine etwas höhere Sicherheit bietet.

DES-Schema

DES arbeitet nach folgendem Schema:





Die Eingabeblöcke haben eine Länge von 64 Bit, ebenso die Ausgabeblöcke. Schlüssel haben eine Länge von 64 Bit, wobei 8 Bit für die Parität vorgesehen sind. Es verbleiben also 56 Bit effektive Schlüssellänge. Der Schlüsselraum hat folglich eine Größe von 2^{56}Bit, was 72 057 594 037 927 936 möglichen Schlüsseln entspricht.

Aus dem Schlüssel K werden 16 Rundenschlüssel abgeleitet. Klartextblöcke werden in zwei Hälften zerlegt. Eine Hälfte wird über sogenannte S-Boxen transformiert und das Ergebnis mit der verbleibenden Blockhälfte per XOR verknüpft. Dann werden die entstehenden Hälften vertauscht.

Die S-Boxen sind in der Funktion f enthalten. Es handelt sich dabei um nichtlineare, bitweise Abbildungen. Über ihr Geheimnis wurde und wird unter Kryptologen viel diskutiert. Im Glossar, unter dem Eintrag für `S-Boxen' wird Näheres geschildert.

Aus- und Eingabepermutation sind nach Meinung fast aller Experten überflüssig und in kommerziellen Implementierungen häufig nicht enthalten.

Für die Entschlüsselung wird der Algorithmus erneut in derselben Reihenfolge durchlaufen, wobei die Rundenschlüssel in umgekehrter Reihenfolge zum Einsatz kommen. Darin ist ein wesentlicher Grund für die gute Implementierbarkeit zu sehen.

Zu DES-Details siehe [Schneier 1996], S.310-350, sowie [Menezes/Oorschot/Vanstone 1997], S. 252-259. Ebenso kann im Glossar unter DES nachgelesen werden.

Weitere symmetrische Verfahren

DES war richtungsweisend für die Entwicklung der symmetrischen Verschlüsselungsverfahren. Viele der später entwickelten Algorithmen weisen große Ähnlichkeit mit DES auf, so z.B.:

- FEAL
- LOKI91
- Khufu
- IDEA

[**Anmerkung:** Ausgefallenere Algorithmen setzen z.B. auf zelluläre Automaten (z.B. CA-1.1). Nicht unbedingt erfolgreich. Von deren Betrachtung sehen wir an dieser Stelle ab.]

Algorithmen wie FEAL, Khufu oder auch IDEA unterscheiden sich hauptsächlich in der Komplexität der einzelnen Verfahrensschritte (Rundenschlüsselauswahl, Verknüpfungsfunktion, Transformationsfunktion, Anzahl der Runden, Schlüssellänge, ...), nicht jedoch im Konzept. Eine Ursache dafür ist der ausführlichen Analyse zu sehen, der DES seit seiner Veröffentlichung weltweit unterworfen war, seit mehr als zwanzig Jahren. Dabei gewonnene Erkenntnisse wurden umgesetzt und oft sogleich patentiert.

Resumee der symmetrischen Verschlüsselung

DES leitete einen ``Paradigmenwechsel'' (*T. Kuhn*) in der Kryptologie ein. Erstmals wurde ein Verschlüsselungsverfahren zur Analyse veröffentlicht. Sicherheit war von da an nicht mehr durch die Geheimhaltung des Verfahrens samt Schlüssel, sondern nur noch durch die Geheimhaltung des Schlüssels definiert. Daraus ergab sich (von der NSAunbeabsichtigt) einerseits die Möglichkeit eines breiten Einsatzes von Verschlüsselungstechnologie. Auf der anderen Seite erwuchs aus eben diesem breiten Einsatz das bekannte Schlüsselverwaltungsproblem, d.h. das Problem der sicheren Schlüsselübergabe.

Verschlüsselungsverfahren werden seit DES als sicher anerkannt, wenn sie trotz Veröffentlichung des Verfahrens und der Entwurfskriterien einer breiten, andauernden Kryptanalyse widerstehen.

Von DES abstammende Blockverschlüsselungsverfahren stellen die Majorität der symmetrischen Verschlüsselungsverfahren. Sie sind schnell, gut implementierbar und bei ausreichender Schlüssellänge sicher.

Die Basis der symmetrischen Verschlüsselungsverfahren bilden einfache mathematische Operationen, die oft in Feistel-Netzwerken ablaufen. Solche Operationen sind schnell und besonders geeignet für die Verschlüsselung großer Datenmengen.

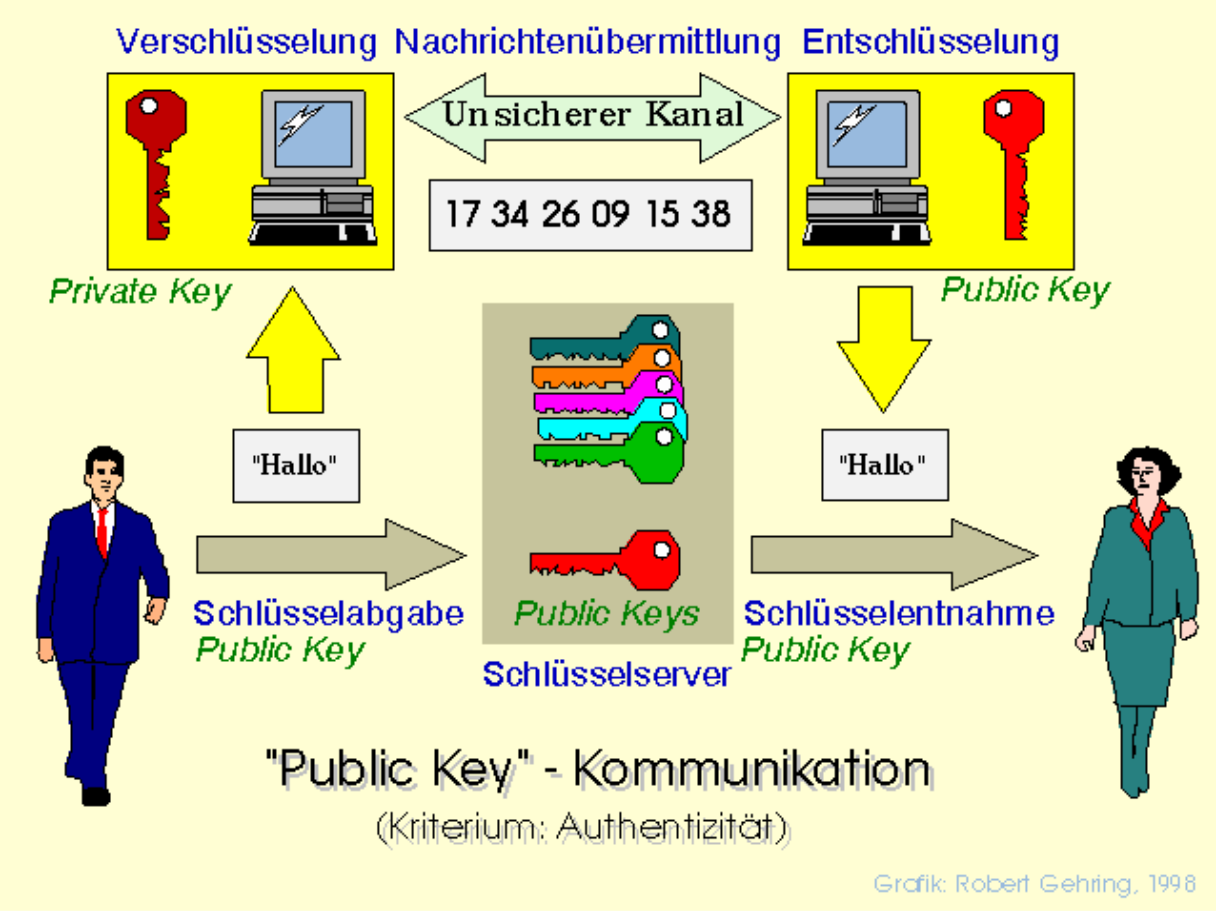
Public Key-Kryptographie

zitat

> ``*Only the private key must be kept secret (authenticity of public keys must, however, be guaranteed).''* [Menezes/Oorschot/Vanstone 1997], S. 31

In der Public Key-Kryptographie werden zwei Schlüssel benutzt. Der eine Schlüssel dient der Verschlüsselung, sein Pendant der Entschlüsselung. Ein Schlüssel ist ausschließlich im Besitz einer einzelnen Person, als sein privater (geheimer) Schlüssel. Der zugehörige, zweite Schlüssel wird den potentiellen Kommunikationspartnern zugänglich gemacht, man spricht vom öffentlichen Schlüssel.

Die nächste Grafik stellt die sichere Nachrichtenübermittlung unter dem Kriterium der Authentizität dar, d.h. die Empfängerin soll sicher sein können, daß die Nachricht vom Besitzer des privaten Schlüssels stammt.



(*Identische Schlüssel haben dieselbe Gestalt.*)

Der Ablauf des Protokolls geht folgendermaßen vor sich (wenn beiderseitig Einvernehmen über das Verschlüsselungsverfahren herrscht):

Vor der Kommunikation:

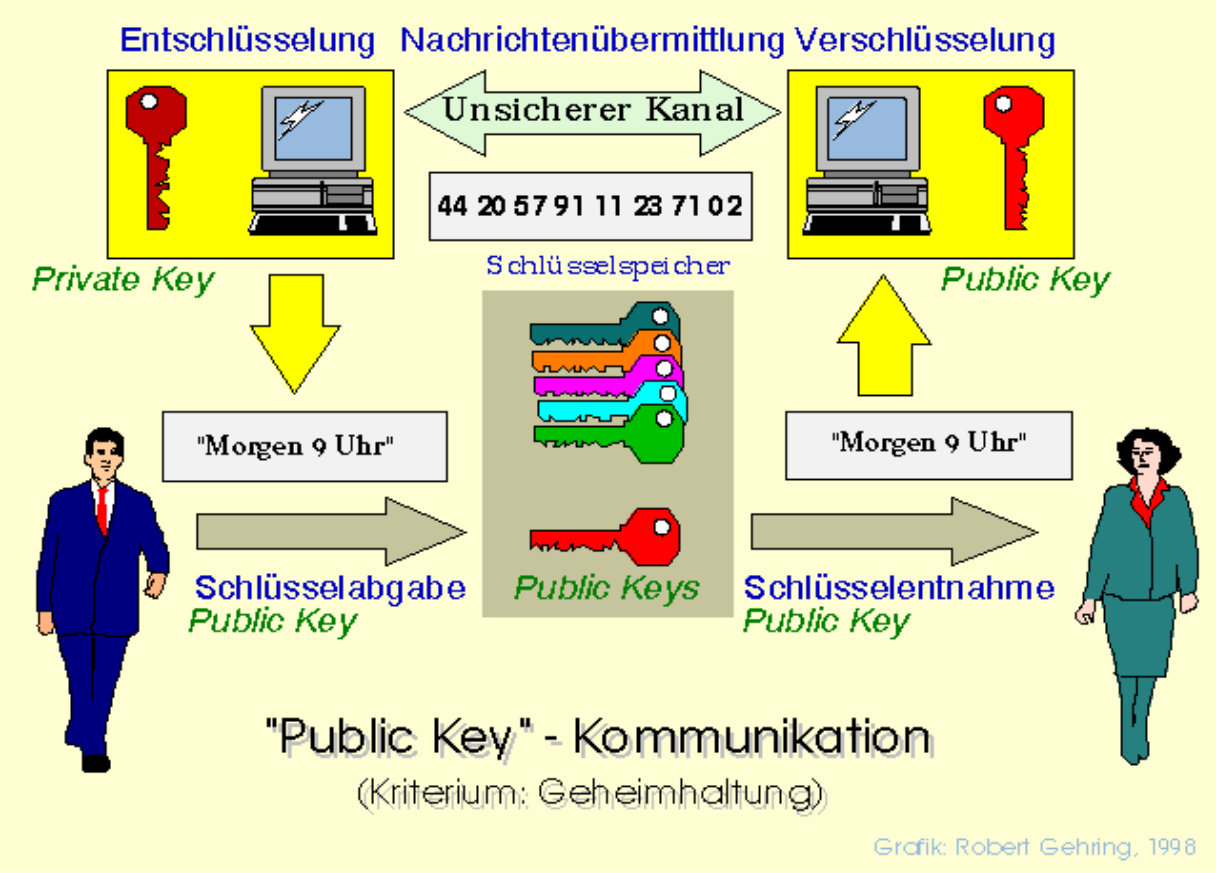
1. Paarweise Schlüsselgenerierung;
2. `Veröffentlichung' eines Schlüssels (öffentlicher Schlüssel) aus dem generierten Paar, z.B. auf einem öffentlichen Schlüsselserver oder mittels persönlicher Übergabe des zugehörigen privaten (geheimen) Schlüssels durch den Inhaber;

Während der Kommunikation:

1. Sender `erzeugt' Information, verschlüsselt sie mit seinem geheimen Schlüssel und sendet die Nachricht an die Empfängerin;
2. Empfängerin nimmt den öffentlichen Schlüssel des Senders, z.B. von einem öffentlichen Schlüsselserver, und entschlüsselt die Nachricht; gelingt die Entschlüsselung, so stammt die Nachricht vom Inhaber des geheimen Schlüssels;

Im Gegensatz zur symmetrischen Verschlüsselung ist damit das Protokoll in der Regel bereits beendet. Die Nachricht wurde so übermittelt, daßdie Empfängerin sicher sein kann, daßsie vom Inhaber des geheimen Schlüssels stammte. Allerdings kann jede beliebige Person, die ebenfalls über den öffentlichen Schlüssel verfügt, die Nachricht ebenso lesbar machen (falls sie sich Zugang dazu verschaffen kann). Eine Geheimhaltung ist auf diesem Wege nicht zu erreichen.

Kehrt man die Richtung der Kommunikation um, so erreicht man die Geheimhaltung der Information. Nachfolgende Grafik zeigt das Vorgehensschema:



(*Identische Schlüssel haben dieselbe Gestalt.*)

Das Protokoll wird wie folgt abgewickelt (wenn Einigkeit über das Verschlüsselungsverfahren herrscht):

Vor der Kommunikation:

1. Paarweise Schlüsselgenierung;
2. Veröffentlichung oder Übergabe des einen Schlüssels (public key) aus dem Paar (z.B. mittels öffentlichen Schlüsselservers) durch den Inhaber des zugehörigen, geheimen Schlüssels;

Während der Kommunikation:

1. Senderin `erzeugt' die geheim zu übermittelnde Information, nimmt den öffentlichen Schlüssel (z.B. vom Schlüsselserver), verschlüsselt die Information und sendet die Nachricht;
2. Empfänger der Nachricht entschlüsselt die Nachricht mit seinem privaten (geheimen) Schlüssel;

Damit ist das Protokoll beendet. Der Empfänger weißdann, daßniemand außer ihm die Information lesen konnte, da nur er allein im Besitz des privaten (geheimen) Schlüssels ist, der zur Entschlüsselung benötigt wird. Ob die Nachricht abgehört wurde spielt keine Rolle, da sie für den Lauscher unlesbar bleibt. Damit ist beschrieben, wie Public Key-Kommunikation abläuft. Zu fragen ist, welche Verfahren bei einem Ablauf, wie dem beschriebenen, die Sicherheit der Verschlüsselung garantieren.

Die beschriebenen Protokolle lassen sich bi- oder multidirektional, d.h. zwischen zwei oder mehr Parteien einsetzen, wenn jeder Kommunikationsteilnehmer jeweils ein Paar aus öffentlichem und privatem Schlüssel einbringt, wobei alle Paare unterschiedlich (disjunkt) sein müssen. Das Problem, Nachrichten entweder authentifiziert oder geheim übermitteln zu können, läßt sich damit jedoch nicht lösen.

`Harte' mathematische Probleme

zitat

> *``There are thousands of problems drawn from diverse fields such as combinatorics, number theory, and logic, that are known to be NP-complete.''* [Menezes/Oorschot/Vanstone 1997], S. 61

Wie oben dargestellt, arbeiten symmetrische Verschlüsselungsverfahren mit einer geeigneten Verküpfung an sich einfacher Verschlüsselungsschritte (Permutation, Substitution, arithmetische Verknüpfungen etc.). Public Key-Verfahren haben eine gänzlich andere Basis. Sie benutzen sogenannte `harte' mathematische Probleme. Davon gibt es eine ganze Anzahl. Leider sind nur die wenigsten von ihnen zur Entwicklung von Verschlüsselungsverfahren geeignet.

Der Begriff des `harten' mathematischen Problems stammt aus der Komplexitätstheorie. Dort werden mathematische Problemstellungen bezüglich des zu ihrer Lösung notwendigen Aufwandes untersucht und klassifiziert. Man unterscheidet Probleme die nicht in polynomialer Zeit lösbar sind (non polynomial = NP), und jene, für die in polynomialer Zeit eine Lösung zu finden ist. Letztere gehören der Klasse P an und heißen effizient lösbar, d.h. es gibt effiziente Algorithmen zu ihrer Lösung.

Für viele Probleme die NP-klassifiziert sind, gibt es keinen Beweis, daß sie der Klasse NP angehören.

Ein polynomialer Algorithmus erfordert im schlimmsten Falle (worst case) einen Zeitaufwand zu seiner Lösung, der durch eine Funktion der Art $O(n^k)$ beschränkt wird. n repräsentiert in der Formel die Länge der Eingabe, k eine Konstante. Zu beachten ist, daß die Funktion eine obere Schranke darstellt. Es ist gut möglich, und in der Praxis häufig der Fall, daß ein Algorithmus für den größten Teil seiner Eingaben die Lösung(en) mit deutlich geringerem Aufwand findet.

Kryptologen interessieren sich besonders für eine Teilmenge von NP-Problemen: NP-vollständige (NP-complete) Probleme. Diese sind mindestens genauso schwer zu lösen, wie jedes beliebige andere NP-Problem. D.h. sie sind signifikant schwerer lösbar, als `leichte' NP-Probleme. Alle NP-vollständigen Probleme sind auch sogenannte NP-`harte' (NP-hard) Probleme, womit die Abstammung des Begriffs der `harten' Probleme erklärt wäre. Toleranter formuliert könnte man sagen, daß für `harte' Probleme keine guten, allgemeinen Lösungen bekannt sind und es sie vermutlich auch nicht gibt.

Beispiel (nach [Menezes/Oorschot/Vanstone], S.61):

> Das ``subset sum"-Problemist NP-vollständig und stellt sich folgendermaßen dar:
>
> > Gegeben sei eine Menge von positiven ganzen Zahlen $Z = \{z_1, z_2, z_3, z_4, \ldots, z_n\}$, sowie eine positive Ganzzahl s. Die Aufgabe lautet festzustellen, ob $s$durch eine Summierung über die Elemente einer Teilmenge von Zgebildet werden kann.
>
> Auf dem ``subset sum"-Problem baute *Ralph Merkle*seinen ``Rucksack" auf.

Einige wenige der bekannten `harten' Probleme wurden von Kryptologen aufgegriffen und mit einer geheimen Falltür (trap door) versehen. Falltüren sind nichts weiter als geheime Zugänge zur Lösung eines `harten' Problems. Als geheime Zugänge werden sie deshalb bezeichnet, weil sie so konstruiert sind, daßsie sich aus dem Problem selbst nicht ableiten lassen (sonst würden sie ja eine gute, allgemeine Lösung darstellen). Nur derjenige, der über eine geheime Information verfügt, kann den geheimen Zugang nutzen. Mit dieser geheimen Information hält man also den Schlüssel zur Lösung der Aufgabe in der Hand.

Diffie und *Hellman* hatten die erste Idee (1976). Allerdings konnten sie anfangs noch kein Exemplar einer Falltürfunktion vorführen. Das blieb *Rivest*, *Shamir* und *Adleman* (1978) vorbehalten. Ihr Verfahren wurde als RSA bekannt, patentiert, und stellt in unseren Tagen das meistapplizierte dar.

> [**Anmerkung:** Die Private Key-Kryptographie ist im Vergleich zur Public Key-Kryptographie einfach. Nicht im Hinblick auf die Qualität der Verschlüsselung, sondern im Aufbau. Jedes Verfahren besteht aus einer Menge für sich verständlicher Schritte, und deren Hintereinanderschaltung läßt sich ganz gut nachvollziehen. Ganz anders die Public Key-Kryptographie. Wie kommt man auf die Idee für eine Falltür zu der Lösung eines NP-`harten' Problems? Mystik, Esoterik, Genie ... ? Jedenfalls gibt es nur wenige solcher Verfahren und noch weniger Entwickler, die wirksame Verfahren entworfen haben. Im Gegensatz zur symmetrischen Kryptographie kann man

bei der asymmetrischen Kryptographie keine Systematik angeben, nur Beispiele.]

RSA

RSA ist der herausragende Vertreter der Klasse `Public Key-Verfahren'. RSA ist etwas jünger als DES, hat für die öffentliche Kryptologie aber eine ähnliche Bedeutung.

Das RSA zugrundeliegende `harte' mathematische Problem ist das der Faktorisierung (factoring, factorization), d.h. der Zerlegung von ganzen Zahlen in ihre Primfaktoren. Bekanntlich läßt sich jede positive ganze Zahl als Produkt aus den Potenzen ihrer Primfaktoren darstellen.

Beispiele:

Die Zahl 99 soll faktorisiert werden. Mit ein wenig Kopfrechnen findet man heraus, daß$99 = 3 * 33 = 3 * 3 * 11$ ist. 99 läßt sich dann als $3^2 * 11$ darstellen. Die Primzahlen 3 und 11 sind die Primfaktoren von 99.

528 ist mit Kopfrechnen schon schwieriger zu faktorisieren. $528 = 2 * 262 = 2 * 2 * 132 = 2 * 2 * 11 * 12 = 2 * 2 * 11 * 2 * 6 = 2 * 2 * 11 * 2 * 2 * 3 = 2^4 * 3 * 11$. Geschafft.

In [Schneier 1996] findet sich auf S. 299 die Faktorisierung von $2^{113} -1$: $3391 * 23279 * 65993 * 1868569 * 106681832868207$.

Wer Spaß daran findet, kann es jetzt mit 937 116 165 963 427 881 912 262 106 681 832 868 207 versuchen.

Die letzte Aufgabe aus den Beispielen wird mit Kopfrechnen wohl kaum mehr zu lösen sein. Sie illustriert gerade deswegen gut das Faktorisierungsproblem. Allen Bemühungen von Mathematikern aus der ganzen Welt zum Trotz wurde noch keine gute allgemeine, d.h. polynomiale, Lösung dafür gefunden.

Überhaupt haben die Primzahlen trotz jahrtausendealtem Interesse dafür wenig von ihren Geheimnissen hergegeben. Man weiß weder, wieviele es gibt, noch wo sie auftauchen. Eines der ältesten Verfahren, um Primzahlen zu finden, ist das ``Sieb des Erathostenes''. Viel weiter ist man heute noch nicht.

Inzwischen gibt es zwar Verfahren wie das Zahlkörpersieb (number field sieve) und das quadratische Sieb (quadratic sieve), mit denen man verhältnismäßig große Zahlen faktorisieren kann. Aber diese Verfahren brauchen auch verhältnismäßig lange, um die Lösung zu präsentieren. Von einer guten allgemeinen Lösung sind sie noch unendlich weit entfernt. [Damm 1995]

Rivest, *Shamir* und *Adleman* haben nun einen Weg gefunden, das Faktorisierungsproblem mit einer Falltür zu versehen und es für ein Verschlüsselungsverfahren nutzbar zu machen - RSA. Dazu benutzen sie die Multiplikation zweier großer Primzahlen.

Arbeitsweise von RSA

Es werden zwei große Primzahlen benötigt. Da es kein Verfahren gibt, das große Primzahlen generiert (das `Sieb des Erathostenes' ist nur für kleine Primzahlen praktibabel), werden zwei Zahlen gewählt und mit einem geeigneten Verfahren auf die Primzahleigenschaft geprüft.

Übliche Tests sind (z.B. nach [Damm 1995] und [Schneier 1996]):

- Das Verfahren von Miller-Rabin
- Das Verfahren von Solovay-Strassen
- Das Verfahren von Lehmann

Alle drei Verfahren stellen mit einer gewissen Wahrscheinlichkeit fest, ob eine gegebene Zahl eine Primzahl ist, oder nicht. Aufgrund der

Einschränkung, daß mit Wahrscheinlichkeiten operiert wird, sind derartige Verfahren deutlich schneller als Faktorisierungsverfahren.

Aus beiden Primzahlen, in der Literatur üblicherweise mit p und q bezeichnet, wird das Produkt n berechnet:

n = p * q.

p und q müssen unterschiedliche Zahlen sein. Die Länge von n sei dabei k Bit. Normalerweise wird k vorgegeben, und p und q werden so gewählt, daßn die Länge k hat. n wird zum ersten Bestandteil des öffentlichen Schlüssels.

Dann berechnet man das Produkt z der Vorgänger von p und q:

z = (p - 1) * (q - 1).

Nun werden der geheime Schlüssel und der zweite Bestandteil des öffentlichen Schlüssels gewählt. Beide müssen so gewählt werden, daßsie folgende Bedingung erfüllen:

e * d =1 mod(z), e hat keinen gemeinsamen Teiler mit z (e teilerfremd zu z).

Ob dabei e oder d als privater Schlüssel verwendet wird, ist im Prinzip egal. Der andere wird dann zum Bestandteil des öffentlichen Schlüssels. In der Literatur (z.B. bei [Schneier 1996]) steht e üblicherweise im öffentlichen Schlüssel und d ist der private Schlüssel.

Achtung: p und q müssen unbedingt geheim bleiben! Wer ganz sicher gehen will, sollte sie vernichten.

Damit hat man folgende Schlüssel erhalten:

- Privater Schlüssel: d;
- Öffentlicher Schlüssel: (e, n).

Man könnte auch (d, n) als den privaten Schlüssel bezeichnen. In der Literatur findet man es allerdings wie oben angegeben.

RSA-Verschlüsselung

Der Klartext wird in Blöcke zerlegt, die kürzer als n sind. Bei Binärzahlen wird die größtmögliche Zweierpotenz gewählt, die noch kleiner als n ist. Handelt es sich beim Klartext nicht um Zahlen oder Bitmuster, so mußman diese erst entsprechend aufbereiten (Buchstaben könnte man z.B. durch ihre Stellung im Alphabet ersetzen.) Die einzelnen Blöcke sollten gleich lang sein, wozu man ggf. Nullen voranstellt. Ein solcher Block wird dann entsprechend der folgenden Formel verschlüsselt:

Geheimtextblock = (Klartextblock ^{e}) mod n.

RSA - Entschlüsselung

Die Entschlüsselung erfolgt für RSA so:

Klartextblock = (Geheimtextblock ^{d}) mod n.

Durch die Verschlüsselung mit dem öffentlichen Schlüssel ist sichergestellt, daßnur der berechtigte Empfänger, der als einziger über den geheimen (privaten) Schlüssel d verfügt, den Klartext wiederherstellen kann.

Beispiel (nach [Schneier 1996], S.533, 534):

Beispiel aus Bruce Schneier: Angewandte Kryptographie, S. 533, 534

Seien p = **47** und q = **71.**

Dann ist n = p * q = **3337** und z = (p - 1) * (q - 1) = **3220**.

Der öffentliche Schlüssel e darf dann keine gemeinsamen Teiler mit z = **3220** haben. e kann also gewählt und dann auf diese Eigenschaft überprüft werden.

e wird gewählt: e = **79**

Dann gilt: e * d = **1** mod **3220**, d.h. d = **1/79** mod **3220** = **1019.**

Der öffentliche Schlüssel lautet dann: (e, n) = (**79, 3337**).
Der geheime Schlüssel lautet: (d) = **1019**.

Der Klartext **688232687966668 3** soll verschlüsselt werden.
Zuerst wird er in Blöcke zerlegt, die kürzer als n sind.

b_1=**688** b_4=**966**
b_2=**232** b_5=**668**
b_3=**687** b_6=**003**

Die Blöcke werden nach der Vorschrift $g_i = b_i^e \bmod n$ verschlüsselt.

g_1=688^{79} mod **3337** = **1570** g_4=966^{79} mod **3337** = **2276**
g_2=232^{79} mod **3337** = **2756** g_5=668^{79} mod **3337** = **2423**
g_3=687^{79} mod **3337** = **2091** g_6=003^{79} mod **3337** = **0158**

Die Blöcke werden nach der Vorschrift $b_i = g_i^d \bmod n$ entschlüsselt.

b_1=1570^{1019} mod **3337** = **688** usw. usf.

Wenn zur Verschlüsselung anstelle des öffentlichen Schlüssels e der geheime Schlüssel d verwendet wird, kann jeder, der die Nachricht mit dem öffentlichen Schlüssel entschlüsselt, sicher sein, daß die Nachricht vom Besitzer des geheimen Schlüssels stammt. Das wurde bereits oben dargelegt. Aber wer ist dessen Besitzer? Mehr dazu im Abschnitt über `Schlüsselbesitz'.

Die Sicherheit von RSA-verschlüsselten Nachrichten ist eine vermutete. Die Kryptologen sind zu der Annahme gekommen, daß die Berechnung des geheimen Schlüssels aus öffenlichem Schlüssel und einem Geheimtext äquivalent zum Problem der Faktorisierung des Produkts der beiden Primzahlen ist, aus denen die Schlüssel abgeleitet worden sind. Einen Beleg für die Richtigkeit dieser Annahme gibt es nicht! Statt dessen gibt es keinen vernünftigen Ansatz für die Widerlegung dieser sogenannten kryptologischen Annahme (cryptologic assumption).

Unter der Annahme also, daß die Faktorisierung zum Brechen der RSA-Verschlüsselung unumgänglich ist, wird klar, daß die Schlüssellängen sehr groß sein müssen: kleine Zahlen, d.h. Produkte kurzer Schlüssel, lassen sich gut faktorisieren. RSA arbeitet aus diesem Grunde mit Schlüsseln von mindestens 512 Bit Länge. Besser sind 1024 oder 2048 Bit, was leider einen erheblich größeren Rechenaufwand nach sich zieht. Die angemessene Wahl wird durch den Zweck bestimmt, ist eine Sicherheitsfrage.

Neben der großen Schlüssellänge ist das modulare Rechnen daran beteiligt, den Rechenaufwand von RSA im Vergleich zu DES um den Faktor 1000 (Hardware) bzw. 100 (Software) zu erhöhen. Verschlüsselungen großer Datenmengen in Echtzeit sind damit ausgeschlossen.

Vorteile, Nachteile von RSA

Man erkennt klar die Vor- und Nachteile von RSA.

Als Vorteile sind zu nennen:

- Das Problem der Schlüsselgeheimhaltung reduziert sich um die Hälfte, da nur eine Person über einen geheimen Schlüssel verfügt.
- Die Schlüsselverteilung stellt -fast- kein Problem mehr dar, zumindest kein technisches Problem. Den öffentlichen Schlüssel darf jeder kennen, solange er nicht über ein allgemeines, schnelles Faktorisierungsverfahren verfügt.

Diesen Vorteilen stehen nicht zu übersehene Nachteile gegenüber:

- RSA ist langsam, sehr langsam.
- Statt eines technischen Schlüsselverteilungsproblems hat man ein logistisches. Da die öffentlichen Schlüssel jedermann frei zugänglich sind, kann man nicht ohne Weiteres sicher sein, ob der vorgebliche Besitzer auch der Eigentümer des Schlüssels ist.
- Last but not least: RSA ist patentiert und der Patentnutzer RSADSI kassiert von den Anwendern. Im Gegensatz dazu darf DES trotz Patentierung ohne Gebühren implementiert werden. Das Urheberrecht an einem bestimmten Quelltext ist allerdings zu beachten!

Andere Public Key-Verfahren

zitat

> *``The famous RSA scheme still is the de-facto-standard in all branches of public-key applications, but it is rapidly loosing its attractiveness.''* [Hess 1997]

RSA ist das wichtigste, jedoch nicht das einzige Public Key-Verschlüsselungsverfahren. Bedeutsam ist zum Beispiel auch das Verfahren von *ElGamal*, das in abgewandelter Form im Digital Signature Standard (DSS) zum Einsatz kommt. ElGamal baut auf dem Problem diskreter Logarithmen auf, das ebenso, wie die Faktorisierung vermutlich NP-vollständig ist.

Neuere Ansätze greifen auf diskrete Logarithmen bei elliptischen Kurven zurück, nicht zuletzt um die fälligen Patentgebühren zu vermeiden (z.B. [Hess 1997]). In der Praxis finden sie bisher noch keine große Anwendung.

Hybride Kryptographie

Konzept der hybriden Kryptographie

Das Konzept der hybriden Kryptographie ist schnell beschrieben. Ihr Ziel ist es, die Nachteile von symmetrischer und asymmetrischer Verschlüsselung zu kompensieren, und ihre Vorteile zu kombinieren.

Grundproblem der Schlüsselverwaltung bei symmetrischen Verfahren ist die Geheimhaltung des privaten Schlüssels bei beiden Kommunikationsteilnehmern. Public Key-Kryptographie mit ihrem Paar aus privatem (geheimem) und öffentlichem Schlüssel umschifft diese Klippe. Da liegt es nahe, zuerst ein Paar asymmetrischer Schlüssel zu generieren. Der erzeugte öffentliche Schlüssel wird dann an den zweiten Kommunikationsteilnehmer geschickt, öffentlich. Hat dieser ihn erhalten, erzeugt er einen symmetrischen Schlüssel, verschlüsselt ihn mit dem öffentlichen Schlüssel und schickt ihn an den Eigentümer des privaten asymmetrischen Schlüssels zurück. Jener kann die Sendung entschlüsseln und verfügt jetzt über eine Kopie des symmetrischen Schlüssels. Die zweite Kopie kann sich ohne Zweifel nur im Besitz des Senders befinden (falls dieser nicht noch mehr Kopien verteilt). Nun steht einer schnellen symmetrischen Verschlüsselung großer Datenmengen, z.B. mit DES, und ihrer Versendung über einen unsicheren Kanal nichts mehr im Wege.

Nach diesem Modell arbeitet zum Beispiel PGP. Für die Datenverschlüsselung kommt IDEA als symmetrisches Verfahren zum Einsatz, die Schlüssel werden mit RSA ``verpackt und versandfertig gemacht''. Das leidige Problem der Lizenzgebühren für die RSA-Nutzung fällt bei einem privaten PGP-Einsatz nicht zur Last. Der PGP-Entwickler *Phil Zimmerman* hat darüber eine Vereinbarung mit RSADSI. Wer auf PGP im kommerziellen Gebrauch setzt, muß allerdings eine entsprechende Lizenz von PGP International erwerben.

Schlüsselbesitz

Public Key-Verschlüsselung räumt viele Schwierigkeiten mit der Geheimhaltung bei Verschlüsselung aus dem Weg. Informationen, die mit einem öffentlichen Schlüssel chiffriert wurden, können nur mit dem privaten Schlüssel wieder lesbar gemacht werden. Die Nachricht bleibt geheim für alle unbefugten Lauscher (von denen es eine Menge gibt, siehe [Ruhmann/Schulzki-Haddouti 1998]).

Trotzdem gibt es ein grundsätzliches Problem: Der Empfänger einer Nachricht weiß nicht, ob diese tatsächlich von der vorgeblichen Senderin stammt. Normalerweise haben noch andere Personen Zugriff auf seinen öffentlichen Schlüssel. Diese könnten einfach eine verschlüsselte Nachricht an ihn schicken und ihn in die Irre führen.

Wenn die andere Richtung der Verschlüsselung gewählt wird, d.h. der Sender chiffriert mit seinem geheimen Schlüssel und schickt die Nachricht an die Empfängerin, so kann diese sich darauf verlassen, daß nur der Inhaber des geheimen Schlüssels Urheber der Nachricht sein kann. Den Fall der Schlüsselkompromittierung betrachten wir einmal nicht. Die Empfängerin kann ebenso wie jeder andere Neugierige den öffentlichen Schlüssel nehmen und die Nachricht lesbar machen. Das war's mit der Geheimhaltung. Zudem weiß sie nur dann genau, wem der öffentliche Schlüssel gehört, wenn sie diesen erstens vom Eigentümer hat und zweitens jener ihr das Eigentum durch einen Test nachgewiesen hat.

Asymmetrisch verschlüsselte Kommunikation mit einem Paar Schlüssel führt zu dem Dilemma, daß entweder der Nachrichteninhalt geheim bleibt oder die Urheberschaft belegt ist. Das ist weder für geschäftliche Transaktionen hinnehmbar, noch legitimen Bedürfnissen nach Privatheit angemessen.

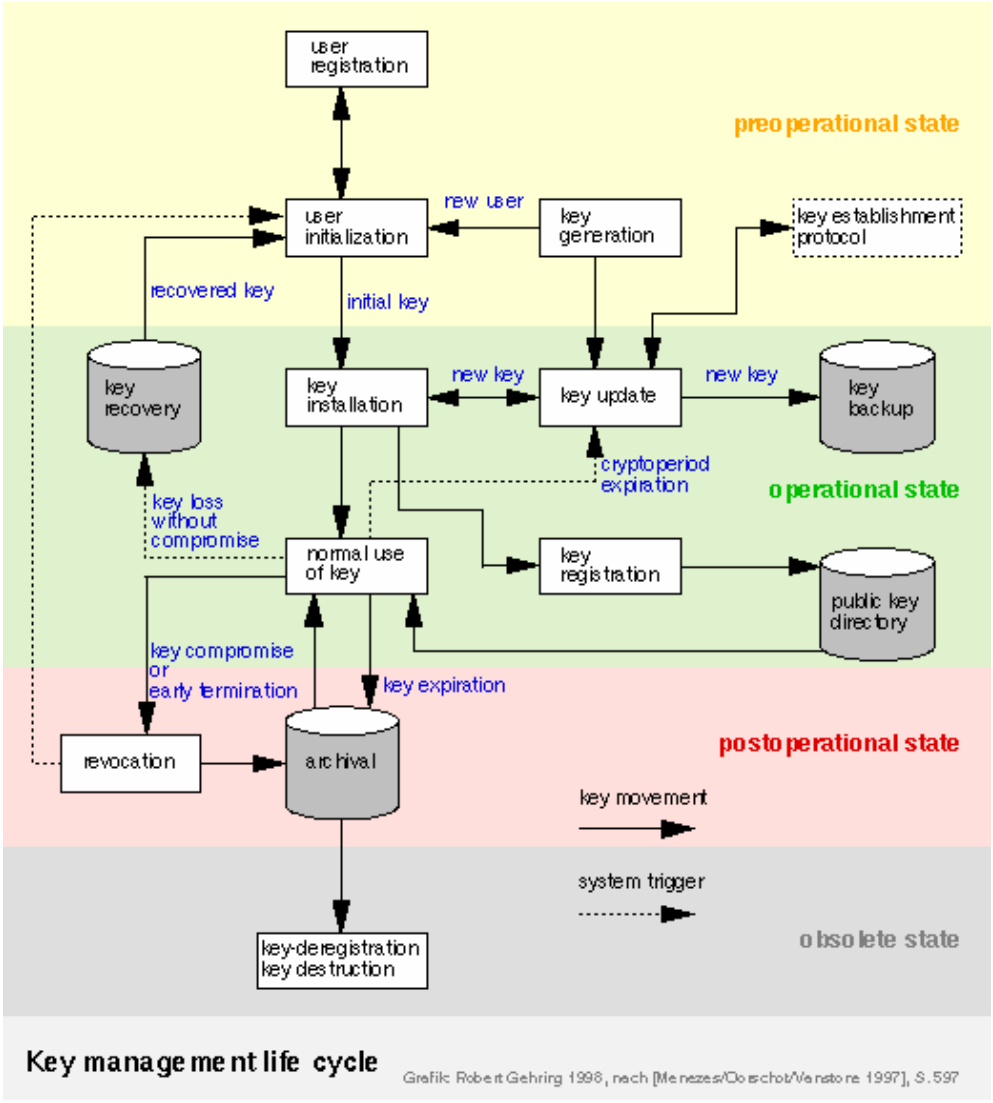
Es steht die Frage der Authentizität der Schlüssel, also einer authentischen Schlüsselverwaltung im Raum.

Schlüsselverwaltung für Verschlüsselungsverfahren

zitat

> *``Bei einem guten Kryptosystem hängt die Sicherheit vollständig von der Kenntnis des Schlüssels und nicht von der Kenntnis des Algorithmus' ab. Deshalb ist die Schlüsselverwaltung in der Kryptographie auch so wichtig.''* [Schneier 1996], S.33

Anhand der folgenden Grafik kann man sich ein Bild über die Zusammenhänge bei der Schlüsselverwaltung machen.



[Die Grafik wurde nach einer Abbildung aus dem ``Handbook of Applied Cryptography'' gestaltet ([Menezes/Oorschot/Vanstone 1997], Seite 579).] Z.B. in ISO/IEC CD 11770-1 (*Key Management - Part 1: Framework*) findet sich ein anderes Modell für einen Schlüssellebenszyklus ([Fumy 1995]).

Der Schlüssellebenszyklus

Ein Schlüssel beginnt seine Existenz durch die Schlüsselgenerierung. Dieser mußdie Auswahl eines Verschlüsselungsverfahrens vorausgegangen sein, durch welches die Art des/der Schlüssel(s) determiniert wird. Der sorgfältigen Schlüsselgenerierung ist große Aufmerksamkeit zu widmen, da viele Verschlüsselungsverfahren sogenannte schwache Schlüsselaufweisen. Verwendet man derartige unsichere Schlüssel, wird eine Sicherheitslücke im System verursacht.

Je nach Implementierung des Verschlüsselungsverfahrens wird der Schlüssel implizit oder explizit installiert. Von einer impliziten Installation kann man sprechen, wenn der Schlüssel auf der Chipkarte generiert wird, auf der er dann verbleibt. Demgegenüber erfordert die explizite Installation die aktive Einbringung des Schlüssels ins Verschlüsselungssystem, da der Schlüssel außerhalb des Systems generiert wird.

Schlüsselgenerierung ist oft eng gekoppelt mit Schlüsselvereinbarung (key agreement). Letztere stellt eine Schlüsselgenerierung durch die beteiligten Parteien dar, d.h. eine Seite ist allein nicht in der Lage, einen Schlüssel zu erzeugen. Verfahren der Schlüsselvereinbarung kommen insbesondere dann zum Einsatz, wenn es gilt, geheime Schlüssel zu generieren. Aus technischer Sicht gibt es große Schwierigkeiten, praktikable Verfahren zu implementieren. Gelingt es jedoch, solche Verfahren zu realisieren, bieten sie eine implizite Authentifizierung, da per definitionem beide Kommunikationspartner zusammen den Schlüssel erzeugen. [Blake-Wilson/Johnson/Menezes 1997]

Soll die Verschlüsselung in einem (rechts-)verbindlichen Rahmen eingesetzt werden, muß der Schlüsselinhaber registriert werden. Im Falle

der Public Key-Kryptographie wird dabei der öffentliche Schlüssel bei einem vertrauenswürdigen Dritten hinterlegt (Kopie), der sie öffentlich zugänglich macht. Über die Registrierung von Benutzer und öffentlichem Schlüssel fertigt der vertrauenswürdige Dritte ein Zertifikat aus, von dem der Benutzer eine Kopie erhält. Eine ander Kopie wird ihrerseits öffentlich zugänglich gemacht. Anhand der öffentlichen Kopie kann sich eine interessierte Partei über die Authentizität eines Schlüssels informieren.

In einigen Fällen ist es sinnvoll, eine Schlüsselkopie zu Reservezwecken an einem sicheren Ort aufzubewahren oder ein `key recovery' vorzusehen. Dafür sollte zwischen einer privaten Nutzung und einer nicht privaten (amtlichen/betrieblichen/funktionalen) Nutzung unterschieden werden:

- **Private Nutzung**des Schlüssels:

  Der Schlüssel dient zur Verschlüsselung privater Angelegenheiten, bei denen der Anwender keinen Rechtsschutz in Anspruch nehmen will/kann. Dazu gehören z.B. der Schutz privater Daten auf der heimischen Festplatte, der email-Briefwechsel mit dem/der Geliebten, `Online-Beichten' usw. Im Sinne eines umfassenden Schutzes der Privatsphäre sollte in diesen Fällen sowohl von der Verwendung registrierter Schlüssel, als auch von der Anfertigung von Sicherungskopien des Schlüssels abgesehen werden. Im Zweifelsfalle wäre dem Schutz der Intimsphäre höherer Wert zuzumessen als dem möglichen Datenverlust.

- **Nicht-private Nutzung**des Schlüssels:

  Werden Daten verschlüsselt, an denen ein über das Private hinausgehendes oder kein privates Interesse besteht, sollte eine Schlüsselkopie an einem sicheren Ort verwahrt werden. Eventuell sind auch Verschlüsselungsverfahren mit `key recovery' in Betracht zu ziehen. Besondere Bedeutung erlangen solche Maßnahmen im Zusammenhang mit Archivierungszwecken, wie sie viele gesetzliche Vorschriften erfordern. Ein möglicher Datenverlust ist dafür als nicht hinnehmbar einzustufen.

Werden Schlüssel regelmäßig ausgewechselt, wie die moderne Kryptologie es empfiehlt, so ist in den Fällen der nicht-privaten Nutzung ein Archiv einzurichten, in denen alte Schlüssel verwahrt werden. Sie stehen damit für eine später vielleicht notwendige Entschlüsselung alter Dokumente zur Verfügung. Den zulässigen Zeitraum für die Schlüsselnutzung, müssen die Kommunikationspartner zusammen mit dem Verschlüsselungsverfahren vereinbaren.

Nach der Benutzung, spätestens jedoch nach Ablauf der Archivierungsfristen oder der Kryptoperiode, sollten sämtliche Schlüssel zerstört werden. Nicht mehr im Gebrauch befindliche Schlüssel sollten nicht länger in den öffentlich zugänglichen Verzeichnissen der vertrauenswürdigen Dritten geführt werden. Will ein registrierter Benutzer einen neuen Schlüssel benutzen, so sollte dieser zusammen mit einem entsprechenden Vermerk (Zeitstempel) anstelle des alten Schlüssels in das Zertifikat aufgenommen werden.

Schwierig gestaltet sich die eventuell notwendige Rückrufaktion bzw. Widerrufsaktion (key revocation), falls ein Schlüssel kompromittiert wurde oder verloren gegangen ist. Bei ausschließlich privater Nutzung obliegen die notwendigen Aktionen dem Benutzer. Eine Rückrufaktion erfordert entweder einen Rundruf, wozu die Daten all' jener Kommunikationspartner, die den zugehörigen öffentlichen Schlüssel benutzen, bereitgehalten werden müssen. Oder die betroffenen Kommunikationspartner müssen von sich aus permanent nachfragen, ob der Schlüssel noch gültig ist. Beide Varianten stellen die Betroffenen vor erhebliche organisatorische Probleme.

Für ein öffentliches System zur Absicherung digitaler Signaturen sind nicht alle im Schema abgebildeten Teile notwendig. Einige Elemente, wie Schlüsselkopien (key backup) oder Schlüsselwiederherstellung (key recovery), dürfen für öffentliche Schlüssel (für digitale Signaturen) gar nicht implementiert werden, wenn sichergestellt sein soll, daß ein Paar aus privatem und öffentlichem Schlüssel nur einmal existiert. Andernfalls wäre es möglich, mit einer Kopie des privaten Schlüssels digitale Signaturen zu fälschen, was die Bemühungen, Rechtssicherheit herzustellen konterkarieren würde. Man beachte, daß in der Grafik keine Angaben über die Lokalisierung der einzelnen Komponenten gemacht werden. Fragen der Implementierung bleiben unberührt.

Das Schlüsseltransportproblem

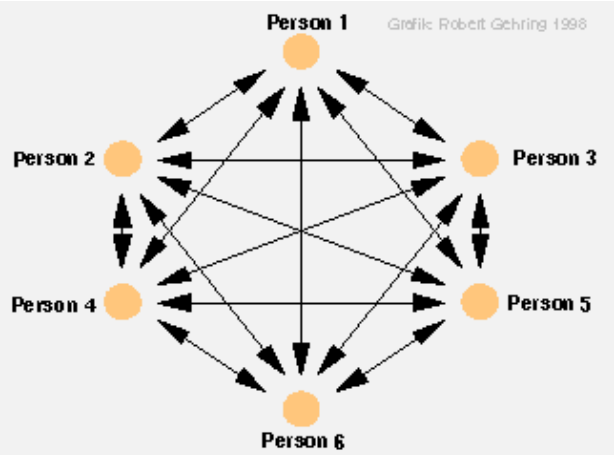
Verschlüsselung kann symmetrisch oder asymmetrisch vorgenommen werden. Im Falle der klassischen, symmetrischen Verschlüsselung sind Geheimhaltung und Authentifizierung relativ leicht sicherzustellen:

Es gibt nur einen Schlüssel. Kopien davon bekommen alle Kommunikationsteilnehmer. Solange der Schlüssel geheim bleibt, kann niemand außerhalb des Kreises der Schlüsselinhaber Nachrichten lesen oder (ver-)fälschen.

Wenn sich immer nur je zwei Personen einen Schlüssel `teilen', d.h. über eine Kopie verfügen, kann der Empfänger sicher sein, daß

eine Nachricht authentisch ist. Solange der Schlüssel geheim bleibt, muß man hinzufügen. Die Frage nach der Authentizität der Kommunikation reduziert sich dann auf die Frage nach der Authentizität des Schlüssels.

So schön es klingt, das Verfahren hat gravierende Nachteile. Die zwei größten Nachteile sind, daß(1) der Schlüssel von mindestens zwei Personen geheimgehalten werden mußund (2) bei einer genügend großen Anzahl von Teilnehmern sehr große Mengen von Schlüsseln anfallen. Dies läßt sich grafisch sehr gut verdeutlichen:



Graph der 1:1-Kommunikation für 6 Personen

Wer nachzählt, kommt auf 5 + 4 + 3 + 2 + 1 = 15 mögliche Kommunikationswege. Sollte jeder Weg abgesichert werden, müßte je ein Schlüssel in zwei Kopien bereitgestellt werden. Da zu einer Kommunikation immer zwei Teilnehmer (communicants) gehören, gibt es 30 Stellen, an denen irgendein Schlüssel geheim bleiben muß. Dazu kommt das Problem der Schlüsselverteilung. Die Schlüssel müssen nicht nur geheimgehalten werden, sie müssen auch zur Übergabe sicher transportiert (key transport) werden. Damit benötigt man zusätzlich 15 sichere Kommunikationskanäle allein für die Übermittlung der Schlüssel.

Asymmetrische Schlüssel als Lösung

In weltumspannenden, elektronischen Netzen wächst daraus eine praktisch unlösbar scheinende Verwaltungsaufgabe. Eine elegante Lösung zur Reduktion des Verwaltungsaufwandes stellt die Benutzung der *asymmetrischen Kryptographie* mit ihren zwei Schlüsseln bereit.

Asymmetrische Kryptographie setzt auf zwei unterschiedliche Schlüssel, einen privaten Schlüssel, auch geheimer Schlüssel genannt, und einen öffentlichen Schlüssel. Letzterer erhält seinen Namen dadurch, daßer im wahrsten Sinne des Wortes *veröffentlicht*wird. Konkret bedeutet Veröffentlichung, daßpotentielle Kommunikationsteilnehmer wahlfreien Zugriff auf den Schlüssel erhalten. Der private Schlüssel mußgeheim bleiben, weshalb jeder unbefugte Zugriff darauf verwehrt sein muß.

Die Besonderheit bei asymmetrischen Verschlüsselungsverfahren besteht (s.o.) darin, daß was mit einem Schlüssel verschlüsselt wurde, nur mit dem anderen entschlüsselt werden kann. Das Problem der Geheimhaltung reduziert sich daher auf die notwendige Geheimhaltung eines -des privaten- Schlüssels an einer Stelle, beim Inhaber. Dazu kommt die authentische Übermittlung der öffentlichen Schlüssel sowie deren authentische Zuordnung zum Inhaber.

Wir verstehen an dieser Stelle unter einer authentischen Übermittlung eine solche, bei der sichergestellt ist, daß eine Kopie des `echten' Schlüssels unverfälscht beim vorgesehenen Empfänger ankommt. Die Übermittlung muß nicht geheim bleiben, wie bei der symmetrischen Verschlüsselung, da der private Schlüssel nicht transportiert wird, sondern einzig und allein dem Inhaber zur Verfügung steht. Ein geheimer Kanal ist also verzichtbar. Die Übermittlung muß jedoch unbeeinflußt bleiben.

[**Anmerkung:** Die erste Publizierung eines sicheren Verschlüsselungsverfahrens (DES 1975) und die Vorstellung der Idee der Public Key-Verschlüsselung (*Diffie* und *Hellman* 1976) folgten kurz aufeinander. Beide verkörpern auf ihre Art die Vorstellung von einer öffentlichen Kryptologie. Die Herstellung von Mitteln zum öffentlichen Einsatz dieser Technologie in öffentlich zugänglichen Computernetzen (Das Internet wurde ab 1973 entwickelt.) sind da nur eine logische Folge ... die nach zwanzig Jahren den Weg in die Praxis findet.]

Ab einer gewissen Anzahl von Beteiligten stellt die Schlüsselverteilung wieder einen Engpaßdar. Der einfachste Weg wäre jener, bei dem die Schlüsselübergabe vom Inhaber an den Empfänger direkt erfolgt. Das mag für ein paar Leute praktikabel sein, in einem weltweiten Kommunikationsverkehr ist es nicht möglich.

Der Weg der unmittelbaren Übergabe des öffentlichen Schlüssels scheidet im großen Rahmen aus. Im kleinen ist er durchaus zu empfehlen, da er einem potentiellen Angreifer (auf das Übergabeprotokoll) weniger Möglichkeiten bietet, als die indirekte Verteilung, die nun beschrieben werden soll.

[**Anmerkung:** Phil Zimmerman hat etwas Ähnliches wie die unmittelbare Schlüsselübergabe in seinem Konzept für PGP vorgesehen. Er führt sogenannte PGP-Fingerprints ein. Diese sind kurz und können z.B. auf Visitenkarten aufgedruckt werden. Anhand dieser ist eine Überprüfung des öffentlichen Schlüssels möglich. Die Fachzeitschrift c't aus dem Heise-Verlag druckt in ihrem Impressum (z.B. c't 5/98) ihren Fingerprint ab:

KeyID: 1024/BB1D9f6Dc't magazine CERTIFICATE <pgpCA@heise.de>
22 09 55 9D 72 60 87 B0 02 C3 71 9C 4E 0E 07 77]

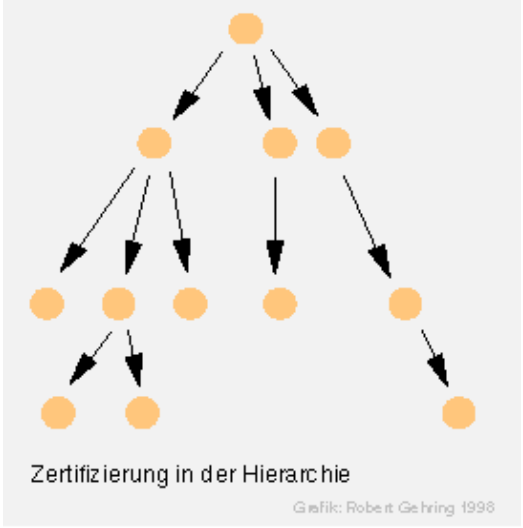
Unter indirekter Verteilung versteht man das Komplement zur direkten Verteilung, d.h. die Schlüsselübergabe erfolgt nicht durch den Inhaber, sondern aus zweiter, dritter usw. Hand. Diese Art der Schlüsselgabe ist der normale Weg in verteilten Computernetzen, wo man einen Schlüssel von irgendeiner verwaltenden Stelle (server) abruft.

Damit steht man wieder vor einer Gewissensfrage: Kann ich dem Lieferanten des Schlüssels trauen oder nicht. In unserem Sinne also: Kann ich davon ausgehen, daß der öffentliche Schlüssel, den mir Person X als den von Person Y übergibt, tatsächlich derjenige von Person Y ist? Oder wenn der Schlüssel nicht von einer Person kommt, sondern einer öffentlich zugänglichen Datenbank (trusted public directory) entnommen wird: Stimmen die Angaben über den Schlüssel in der Datenbank? Wer bürgt dafür? Wer haftet?

Direkte und indirekte Schlüsselverteilung

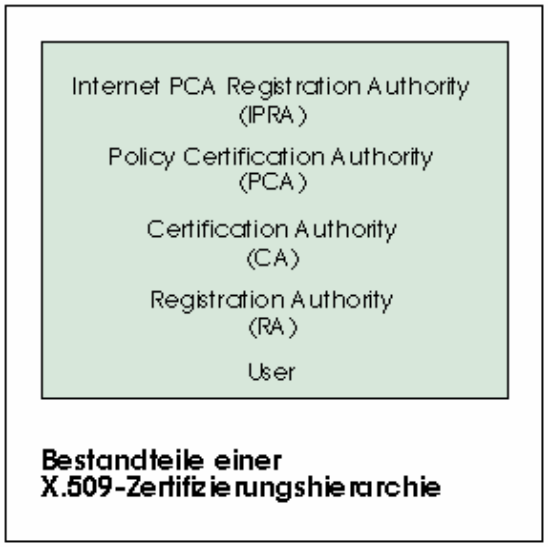
Bisher wurden zwei grundsätzlich unterschiedliche Ansätze entwickelt, die indirekte, authentische Verteilung von Schlüsseln abzusichern. Die Absicherung selbst bezeichnet man als Zertifizierung, da sie auf irgendeiner Art von Zertifikaten (Bescheinigungen, die etwas bestätigen, quasi `Ausweise') beruhen. Unterschiede finden sich in der Form, wie die Zertifizierung implementiert wird. Allgemein gefaßt, kann man Zertifizierung als Beglaubigung ``übersetzen''. In dem schon zitierten Werk zur Kryptographie von Menezes, van Oorschot und Vanstone findet sich die Definition ``*endorsement of information by a trusted entity*''([Menezes/Oorschot/Vanstone 1997], Seite 3). Wörtlich übersetzt hieße es ``*Unterschreiben einer Information durch eine vertrauenswürdige Einheit*'', was mit Beglaubigung ganz gut umschrieben ist.

Auf der einen Seite gibt es den hierarchischen Ansatz, auf der anderen Seite einen netzartigen Ansatz (auch `Digraphmodell' genannt). Jede Variante hat ihre Vor- und Nachteile. Die Hierarchie setzt auf klare Verantwortlichkeiten, die Netzstruktur auf Eigenverantwortlichkeiten. Hierarchien lassen sich effektiv realisieren, Netzstrukturen brauchen Zeit zum Wachsen. Hierarchien sind empfindlich gegen Fehler, Netzwerke sind verhältnismäßig fehlertolerant. Nicht zuletzt benötigen Hierarchien Bürokratien, wogegen Netzstrukturen weitgehend ohne solche auskommen.



Im einfachsten Falle zertifizieren die übergeordneten die jeweils untergeordneten Instanzen.

Im konkreten Fall von X.509 werden die Stellen in der Hierarchie von folgenden Elementen besetzt:



Für den Benutzer (user) müssen alle Instanzen über ihm (authorities) die Qualität vertrauenswürdiger Dritter (TTPs) haben. Nur so läßt sich eine Kette des Vertrauens bis hoch in die Wurzelinstanz aufbauen.

Zertifizierung durch Trusted Third Parties

Die Trusted Third Party (TTP)

zitat

``Vertrauen ist eine grundlegende subjektive Leistung jedes Menschen in vielen Lebenssituationen, weil der einzelne von Mal zu Mal selbst entscheiden muß, ob er es gewährt. Vertrauen reduziert soziale Komplexität, wenn Entscheidungen trotz Unsicherheit über das Verhalten anderer Menschen oder unzureichenden Wissens getroffen werden müssen."

``Die Vertrauenslücke kann mit Hilfe Dritter verkleinert werden, die die Identität von Teilnehmern zusichern oder Leistungen

garantieren." [Hammer 1995]

[**Hinweis:** Im vorliegenden Text werden die Begriffe `Trusted Third Party', `vertrauenswürdiger Dritter', `vertrauenswürdige dritte Instanz' usw. synonym gebraucht.]

Der Vertrauenswürdige Dritte

zitat

``Zwei Menschen, die sich allein und ohne Ausweis begegnen, können sich ihre Identität gegenseitig nicht beweisen. Sie brauchen dazu ein bestätigendes soziales Umfeld. Entweder sind sie von vertrauenswürdigen Instanzen, z.B. Einwohnermeldeämtern, mit Identitätsausweisen versehen worden, oder sie werden von einer vertrauenswürdigen dritten Person einander vorgestellt. Beide Verfahren setzen vertrauenswürdige Dritte ein." [Grimm 1996]

Wann ist ein `Dritter' ein `Dritter'? Und wozu wird ein `vertrauenswürdiger Dritter' benötigt?

`Trusted Third Party` ist ein englischer Begriff. Das Wort `trust' wird vom Oxford Dictionary mit Vertrauen übersetzt. Demzufolge heißt die `trusted third party' auf Deutsch `vertrauenswürdige dritte Partei'. Eine elegantere Übersetzung ist `vertrauenswürdiger Dritter'. Häufig wird auf die Übersetzung ganz verzichtet.

Gemeint ist eine Instanz mit unabhängiger Stellung gegenüber zwei Parteien, die zueinander in einer bestimmten Beziehung stehen. Für den Konfliktfall, Garantien, Interessenvertretung oder notwendige treuhänderische Aufgaben bestimmen die beiden Parteien diese Instanz zum Dritten und vereinbaren untereinander, deren Entscheidungen zu akzeptieren. Werden Regeln oder ein Protokoll vereinbart, nach dem die Parteien vorgehen wollen, wird eine unabhängige Instanz zur Überwachung der Einhaltung der Regeln bestimmt. Oft wird von ihr auch die Abwicklung der Protokolle gesteuert.

Beispiele:

Im Sport nennt man solche *``Vertrauensinstanzen"*([Hammer 1995]) Schiedsrichter. In der Rechtsprechung ist es der Richter, der nach Interessenabwägung sein Urteil fällt. Andernorts werden Vermittler und Ombudsmänner berufen.

Festzuhalten bleibt, daßeine `vertrauenswürdige dritte Instanz' in einer (interessen-) unabhängigen Position gegenüber den beiden ersten Parteien stehen muß. Besteht dagegen die Möglichkeit, daßder `Dritte' selbst in einen Interessenkonflikt bezüglich der Wahrnehmung seiner Aufgaben gerät, ist das Vertrauen schnell erschüttert. Nicht zuletzt mußdie Durchsetzung der Entscheidungen des `Dritten' gesichert sein, sonst verlieren er und seine Funktion ihre Glaubwürdigkeit. Dies sind keine neuen Erkenntnisse. Trotzdem sollte im Vorfeld der folgenden Ausführungen noch einmal klargestellt werden, was die herkömmliche Auffassung über Aufgabe und Stellung einer `Trusted Third Party' ist.

Im Zusammenhang mit `digitalen Signaturen' sollen Trusted Third Parties die Funktion der Certification Authorities in einer Schlüsselverwaltungsinfrastruktur (key management infrastructure) übernehmen. Dies wird später genauer ausgeführt werden.

Authentizität von Kommunikation

Seit den 70'er Jahren vollzieht sich eine Entwicklung hin zur elektronischen Vernetzung. Diese Entwicklung hatte Vorläufer in anderen Kommunikationsnetzen: Post, Zeitungswesen, Rundfunk, Telefonnetz und Welthandel. Dieses waren in den letzten Jahrhunderten (national-) staatliche Netze. Erst im Zeitalter des Internet werden die Grenzen für die Kommunikation aus nationalstaatlicher Perspektive aufgehoben. Gleichzeitig geht damit auch der Schutz verloren, den der Staat als Nationalstaat bieten kann: nationale Gesetze und Behörden zu deren Durchsetzung. Datenschutz und Versicherungsschutz seien hier nur als Stichworte genannt. Auch wachsen auf dem Weg in die Informationsgesellschaft die Begehrlichkeiten aller möglichen Institutionen -staatlicher und nichtstaatlicher-, an die Ressource Information zu gelangen - länderübergreifend (siehe z.B. [Ruhmann/Schulzki-Haddouti 1998]).

Die Grenzen öffnen sich noch in einem anderen Sinne: Materie wird ersetzt durch elektrische Impulse und Ladungen, durch Magnetflüsse und -felder, wandelbarer in Raum und Zeit, als Papier, Medium der letzten zwei Jahrtausende. Damit ermöglichen sie eine Beschleunigung und Vervielfachung der Kommunikation ohnegleichen. Aber auch diese Grenzöffnung hat ihren Preis: die Sicherheit und Haltbarkeit, die

Papier bieten kann, finden in elektronischen Welten kein Pendant.

Die moderne Kommunikation kann ohne Kopien gar nicht mehr existieren. Permanent werden Daten zwischengespeichert, in papierner oder in elektromagnetischer Form. Längst schon ist nicht mehr überschaubar, wer wo und wie die Gelegenheit hat, elektronische Kommunikation zu belauschen, zu verfälschen und zu verhindern. Und daß solche Möglichkeiten weidlich ausgenutzt werden, zeigen z.B. die Berichte über das von der NSA installierte Echelon-System (z.B. [Ruhmann/Schulzki-Haddouti 1998]).

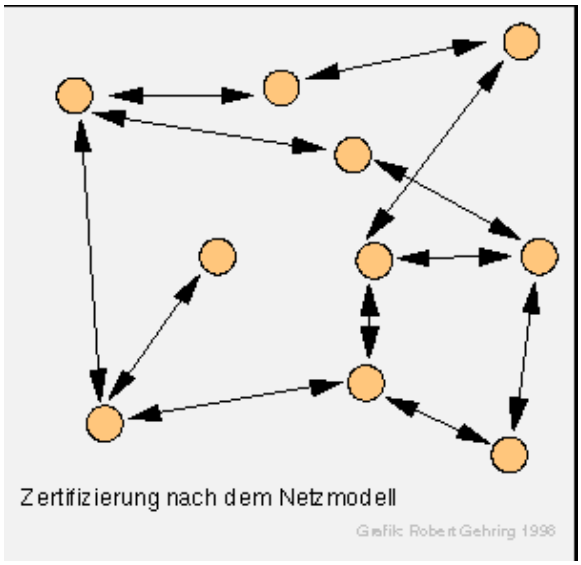
Ein Mittel, Inhalte von Kommunikation erstens abzusichern (d.h. ihre authentische Übermittlung sicherzustellen) und zweitens geheimzuhalten, ist die Verschlüsselung. (Ein anderes, deutlich aufwendigeres Mittel ist die Installation abgeschlossener Kommunikationskanäle, wie z.B. das `rote Telefon` zwischen Weißem Haus und Kreml.)

Unabhängig von der Wahl des Schlüsselverwaltungsmodells mußeine Zertifizierung vorgenommen werden. Deren Sinn und Zweck ist es, Glaubwürdigkeit und Vertrauenswürdigkeit abzusichern und Beweissicherheit herzustellen.

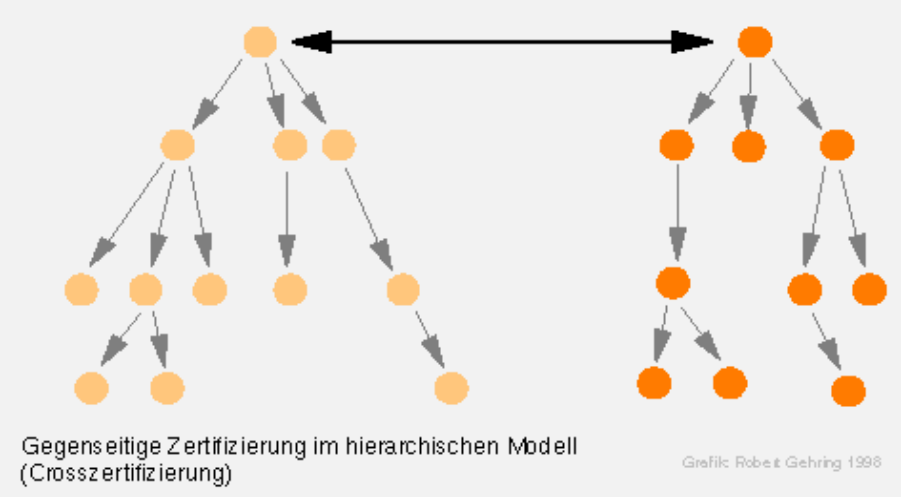
In der Hierarchie stellt die übergeordnete Instanz das Zertifikat für die ihr nachgestellte Stufe aus und gibt damit Garantien. Im Netz stellen sich die Teilnehmer gegenseitig Zertifikate aus. Diese Zertifikate haben die Aufgabe, die Zuordnung von Personen und öffentlichen Schlüsseln auszuweisen (ggf. noch weitere Angaben).

Die Aufgabe der Zertifizierung kommt in einem hierarchischen Modell dem ``vertrauenswürdigen Dritten'' (trusted third party) zu. Nur unter dem Primat der Vertrauenswürdigkeit wird einerseits der Schlüsselinhaber bereit sein, seinen öffentlichen Schlüssel zertifizieren (beglaubigen) zu lassen und andererseits ein möglicher Kommunikationspartner der Beglaubigung durch die Zertifizierungsinstanz trauen. Im Englischen wird das unter dem Begriff ``*establishing trust between users in distinct [security] domains*'' ([Menezes/Oorschot/Vanstone 1997], Seite 571) zusammengefaßt.

In einem netzartigen Modell zur Zertifizierung entscheidet dagegen jeder Teilnehmer selbst über Vertrauen oder Ablehnung, unmittelbar. Die Zertifizierung erfolgt, wie z.B. bei PGP, gegenseitig. Damit ist einem möglicherweise in betrügerischer Absicht handelnden Dritten sein Vorhaben erschwert, die Schlichtung im Streitfalle jedoch ebenfalls. Ein Betrug zeigt nicht so gravierende Folgen wie in einer Hierarchie. In jener zieht die Kompromittierung des Schlüssels einer höheren Stufe lawinenartig die Wertlosigkeit der Zertifikate aller ihr untergeordneten Stufen nach sich. Im Netz verfügt jeder einzelne Teilnehmer nur über eine relativ geringe Anzahl von Schlüsseln. Manipulationen daran können nie so große Auswirkungen haben wie in einer Hierarchie.



Weiterhin verbleibt die Frage nach der Vertrauenswürdigkeit der obersten Instanz in der Hierarchie. Eine mögliche Antwort ist die sogenannte gegenseitige Zertifizierung mehrerer Zertifizierungsinstanzen (cross certification, CA-certification), bei der zwei Instanzen sich wechselzeitig Zertifikate ausstellen. Damit läßt sich das Vertrauen in die eigene Zertifzierungsinstanz herstellen und zusätzlich auf die andere Hierarchie übertragen. In gewisser Weise handelt es sich um die Anwendung des Netzmodelles auf die Hierarchie. Zusätzlich läßt sich auf diesem Wege die Interoperabilität zu den Mitgliedern einer anderen Zertifizierungsdomäne einrichten. Voraussetzung ist natürlich eine Implementierung verträglicher Verfahren oder besser ein einheitlicher Standard (z.B. X.509).



Von beiden Zertifizierungsmodellen (Netz und Hierarchie) gibt es noch Varianten. So gibt es bidirektionale Hierarchien, bei denen jede Stufe die unter ihr liegenden Stufen zertifiziert, sowie von ihnen zertifiziert wird. Ebenfalls gibt es Netze mit abgestuften Graden des Vertrauens (wie z.B. im Web of Trustvon PGP).

Verwaltung der Zertifikate und Schlüssel

[**Hinweis:** Insofern nicht explizit von privaten Schlüsseln die Rede ist, sind immer öffentliche Schlüssel gemeint, auch wenn es bloß Schlüssel heißt.]

Für eine abgesicherte und authentische Kommunikation sind also zwei Dinge nötig: Erstens ein Verfahren und die Infrastruktur zur Verwaltung der Schlüssel und zweitens Verfahren und Infrastruktur für die Zertifikatsverwaltung. Im Netzmodell fällt das alles weitgehend zusammen: Der Inhaber gibt die Schlüssel weiter und zertifiziert die empfangenen Schlüssel. Später verteilt er seinerseits die zertifizierten Schlüssel. So `wandern' Schlüssel und Zertifikate durch das Netz und auf die Festplatten der Teilnehmer.

In der Hierarchie sieht das anders aus. Es bietet sich scheinbar an, die hierarchische Infrastruktur für Schlüssel und Zertifikate gleichzeitig zu benutzen. Warum? Beide erfordern die Speicherung in Datenbanken sowie die Möglichkeiten des externen Zugriffs. Die öffentlichen Schlüssel müssen ebenso abgerufen werden können wie die zugehörigen Zertifikate, in der Regel gleichzeitig. Eine gekoppelte Verwaltung von Schlüsseln und Zertifikaten würde diesen Ablauf erleichtern.

Es gibt auch die Möglichkeit, Zertifikate und Schlüssel nicht auf Abruf zu liefern (pull model), sondern in gewissen Zeiträumen automatisch an die Anwender zu versenden (push model), quasi im Abonnement ([Menezes/Oorschot/Vanstone 1997], Seite 577). Zusätzlich wären Zertifikatswiderrufe (certificate revocation) zu verschicken, falls Schlüssel kompromittiert oder Zertifikate manipuliert worden sein sollten. In der Praxis ist dies für kleine, geschlossene Gruppen durchführbar. Im weltweiten Verbund, mit Millionen Teilnehmern, wird die notwendige Datenmenge zu groß.

Welche Argumente könnten dagegen sprechen, Schlüssel und Zertifikate gemeinsam zu verwalten? Eine Grundregel der Sicherheitspolitik lautet, das Risiko zu verteilen (``Doppelt hält besser!''), um es zu minimieren. Und Risiken gibt es viele, wenn es um Technik geht. Technik, die zentralisiert wird, ist bei einem Ausfall nicht oder nur sehr schwer ersetzbar. Die Gefahr des Mißbrauches wächst, wenn die Möglichkeiten dazu vereinfacht werden. Und ein zentraler Zugriff ist leichter zu bewerkstelligen als mehrere dezentrale Zugriffe. (Was gleichzeitig auch ein Argument für die gemeinsame Verwaltung ist.)

Große und komplizierte Systeme haben die Tendenz, unflexibel zu werden. Im Krisenfall fällt es ihnen meist schwer, schnell und adäquat zu reagieren. Sie neigen eher dazu, die Bekanntwerdung eines Problems zu verhindern, als sofortige Abhilfe zu schaffen. Auch sind viele Fälle denkbar, in denen Zertifikate gar nicht benötigt werden, sondern lediglich die Schlüssel. Oder es kann Fälle geben, in denen nur interessant ist, ob es ein Zertifikat für eine Person gibt. Vielfach wollen Anwender auch ihre Anonymität gesichert wissen. Sie werden dann eher einer Instanz vertrauen, die ihre persönlichen Angaben gar nicht erst erfahren hat, als einer Instanz, die beteuert, keine Daten weiterzugeben, die sie gespeichert hat. Datenschutzgesetz hin oder her; Beispiele für Mißbrauch oder Fahrlässigkeit gibt es immer wieder.

Die Abwägung der Sicherheitsanforderungen gegen die Bequemlichkeiten bei der Benutzung werden letztendlich ausschlaggebend für die

Entscheidung pro oder contra gemeinsame Verwaltung von Schlüsseln und Zertifikaten sein. Wenn es um Rechtsverbindlichkeit geht, kommt man in vielen Fällen sowieso nicht umhin, sich nach den Vorgaben des Signaturgesetzes (SigG), der zugehören Verordnung (SigV) und des Maßnahmenkatalogs des BSI zu verhalten. Was aber seinerseits keine Garantien für die Sicherheiten bietet. Im Signaturgesetz geht es um die Schlüssel für digitale Signaturen. Diese könnten jedoch auch für andere Zwecke eingesetzt werden, wie zum Beispiel zur Datenverschlüsselung in hybriden Verfahren, ... *wenn sie denn zugänglich sind*.

Standardisierung von Authentifizierungs- und Zertifizierungsverfahren

Maßgeblich ISO/IEC haben diverse Authentifizierungsverfahren standardisiert ([Fumy 1995], [Menezes/Oorschot/Vanstone 1997]):

- **ISO/IEC 9796** Digitale Signaturen mit *message recovery*

- **ISO/IEC 9798** Authentifizierung
- **ISO/IEC 9798-1** Einführung
- **ISO/IEC 9798-2** (1994) Mechanismen, basierend auf symmetrischen Techniken
- **ISO/IEC 9798-3** (1993) Mechanismen, basierend auf asymmetrischen Techniken. *Die Mechanismen in ISO/IEC 9798-3 finden in X.509 eine Entsprechnung.*
- **ISO/IEC 9798-4** (1995) Mechanismen mit kryptographischer Prüffunktion
- **ISO/IEC 9798-5 (*Working Draft*)** Mechanismen, basierend auf Zero-knowledge-Funktionen

- **ISO/IEC 11770** Schlüsselverwaltung und Schlüsselinstallation
- **ISO/IEC 11770-1** Schlüssellebenszyklus, Schutz für Schlüssel, Trusted Third Parties
- **ISO/IEC 11770-2** Schlüsselinstallation mit symmetrischen Techniken
- **ISO/IEC 11770-3** Schlüsselinstallation mit asymmetrischen Techniken

- **ISO/IEC 13888 (*Draft*)** Dienste für Unabweisbarkeit
- **ISO/IEC 13888-1** Modell und Überblick
- **ISO/IEC 13888-2** Mechanismen, basierend auf symmetrischen Techniken
- **ISO/IEC 13888-3** Mechanismen, basierend auf asymmetrischen Techniken und digitalen Signaturen

- **ISO/IEC 14888 (*Draft*)** Signaturen mit Anhang
- **ISO/IEC 14888-1** Definitionen, Überblick und Modelle
- **ISO/IEC 14888-2** Mechanismen mit Signaturen, basierend auf der Identität des Benutzer
- **ISO/IEC 14888-3** Mechanismen mit Signaturen, basierend auf Zertifikaten
- **ISO/IEC 9594-8 (ITU-T X.509)** Authentifizierungstechniken

Es gibt viele weitere, konkrete Vorschläge für hierarchische Zertifizierungsstrukturen von nationalen und internationalen Institutionen. Auch Firmen haben eigene Entwürfe vorgestellt, wie z.B. PKCSNr. 6 von RSADSI.

Im Vergleich: der X.509-Vorschlag für Zertifikate (nach [Breilmann 1996]) und die Festlegungen des Signaturgesetzes [SigG]:

Allen Entwürfen gemeinsam sind öffentlich zugängliche Datenbereiche (trusted public directories, trusted public files), aus denen die Zertifikate online abgerufen werden können. Die Verwaltung dieser Datenbereiche obliegt einer vertrauenswürdiger Authorität, was lediglich ein anderer Name für `trusted third party' ist. Dieser Instanz gegenüber mußsich derjenige identifizieren, der ein Zertifikat zu erhalten wünscht. Ebenfalls mußer seinen öffentlichen Schlüssel vorlegen. Entsprechend den vorgelegten und nachgewiesenen Angaben wird ein Zertifikat erstellt. Aus dem erteilten Zertifikat gehen dann ein Identitätskennzeichen (nicht notwendig ein echtes, Pseudonyme sind ausreichend), der öffentliche Schlüssel und die Bestätigung der Übereinstimmung durch die Zertifizierungsauthorität hervor. Weitere, optionale Informationen können angefügt werden.

Die Zertifizierungsinstanz legt die Zertifikate so ab, daßsie von Außenstehenden nicht manipuliert werden können. Die Computer im Netzwerk, die für diese Aufgabe bereitgestellt werden, kann man als Schlüsselserver (key server) oder auch Zertifikatsserver bezeichnen. Der Zugriff auf die Zertifikate erfolgt über genau spezifizierte Protokolle und Verbindungen. Darunter fallen sowohl die klassische, schriftliche Übermittlung (offline), als auch die elektronische Übermittlung (online). In beiden Fällen mußdie Übermittlung selbst wieder authorisiert werden. Dazu lassen sich Siegel bzw. digitale Signaturen -durch die Zertifizierungsinstanz- einsetzen. Die Bestätigung der Authorität der Instanz selbst erfolgt durch die ihr in der Hierarchie übergeordnete Instanz bzw. durch Crosszertifizierung.

Wesentliche Unterschiede gibt es im Umgang mit ungültigen Zertifikaten. X.509 verlangt die Gültigkeit sämtlicher Zertifikate in der Zertifikatskette, d.h. von der Wurzelinstanz bis zum Benutzer, um eine gültige Signatur zu erzeugen. Die Umsetzung der Signaturverordnung zum Signaturgesetz ist hier weniger strikt. Zur Verringerung des Verwaltungsaufwandes können Zertifikate auch dann anerkannt werden, wenn übergeordnete Zertifikate ungültig sind ([SigB]).

Historische Entwicklung der Zertifizierung

Das Konzept der öffentlichen Verzeichnisse (trusted public file, trusted public directory) geht auf *Diffie*und *Hellman*(1976) zurück. *Merkle* (1979) hatte die Idee von der hierarchischen (für Informatiker: baumartigen) Authentifizierungsstruktur. Zertifikate für öffentliche Schlüssel wurden von *Kohnfelder*vorgeschlagen (1978). Sein Vorschlag sah für ein Zertifikat vor, den Namen des Inhabers, seinen öffentlichen Schlüssel und Angaben über Authentifizierung einzutragen. Er orientierte sich dabei am RSA-Verfahren. ([Menezes/Oorschot/Vanstone 1997], Seite 587) In ihrer Kombination ergeben die drei Ideen die notwendige Infrastruktur für ein System der Zertifikatsverwaltung, wie es u.a. für digitale Signaturen zur Anwendung kommt. (Alternativen sind denkbar, z.B. nach dem Netzmodell nach *Zimmerman*. [2])

Schlüsselverwaltung und Zertifikate im Signaturgesetz

Im deutschen Signaturgesetz finden sich die entsprechenden Umsetzungen der erläuterten Konzepte in Paragraph 2 (*Begriffsbestimmungen*), Paragraph 5 (*Vergabe von Zertifikaten*) und Paragraph 7 (*Inhalt von Zertifikaten*). Leider folgt das Gesetz nicht der internationalen Norm X.509, so daßeine weltweite Interoperabilität der Anwendungen zukünftig nicht garantiert ist.

> [**Anmerkung:** Dies mag sogar beabsichtigt sein. Die Beschränkung der gesetzlichen Anerkennung von digitalen Signaturen auf einen nationalen Rahmen läßt das Haftungsproblem -mehr dazu weiter unten- bei internationalen, geschäftlichen Transaktionen unbehandelt. Das Risiko verbleibt bei den Geschäftspartnern. Man könnte darin die

Konsequenz aus einem gewissen Unbehagen bei der Einführung dieser neuen Technologie sehen.]

Die Regelungen im Gesetz gehen zum Teil über die technisch sinnvollen Forderungen hinaus. So findet sich in Paragraph 5 Absatz 4 die folgende Aussage:

zitat

> ``*(4) Die Zertifizierungsstelle hat Vorkehrungen zu treffen, damit Daten für Zertifikate nicht unbemerkt gefälscht oder verfälscht werden können. Sie hat weiter Vorkehrungen zu treffen, um die Geheimhaltung der privaten Signaturschlüssel zu gewährleisten. Eine Speicherung privater Signaturschlüssel bei der Zertifizierungsstelle ist unzulässig. "* [SigG], §5 (4)

Der erste Satz ist einsichtig, Fälschungen sind zu verhindern. Der zweite Satz steht dem ersten dann in gewisser Weise entgegen. Zertifizierung meint in Bezug auf digitale Signaturen, d.h. asymmetrische Verschlüsselung, immer die Zertifizierung der öffentlichen Schlüssel. Die zugehörigen privaten Schlüssel müssen unter allen Umständen geheim bleiben, soll die Kommunikation gesichert werden [3].

Der zweite Satz räumt jedoch die Möglichkeit ein, daß die Zertifizierungsstelle an die privaten Schlüssel gelangt. Ein Aufdecken (Kompromittieren) der privaten Schlüssel ermöglicht die beliebige Manipulation jeglicher damit verschlüsselter Kommunikation und *muß* daher *prinzipiell ausgeschlossen werden*.

Der dritte Satz des Absatzes schließlich, der eine Speicherung der privaten Schlüssel untersagt, ist nur notwendig, wenn es überhaupt eine Möglichkeit der Speicherung und damit der Kompromittierung gibt. Satz 1 des Absatzes steht also in eklatantem Widerspruch zu den Sätzen 2 und 3. Und nicht nur dazu, sondern insbesondere zu jedem Sicherheitsmodell für digitale Signaturen.

In der vorliegenden Form wird der Umgang mit privaten (geheimen) Schlüsseln kryptologisch unsicher gemacht.

Handelt es sich um ein Versehen? Im Gesetz wird nichts darüber gesagt, woher die Schlüssel, auf die Bezug genommen wird, stammen. Noch ein Versehen? Ein Blick in die amtliche Begründung klärt nicht auf. Dort findet sich folgende Aussage:

zitat

> ``*Die jeweils einmaligen Schlüsselpaare (privater und öffentlicher Schlüssel) werden durch anerkannte Stellen natürlichen Personen fest zugeordnet. Die Zuordnung wird durch ein Signaturschlüssel-Zertifikat beglaubigt."* [SigB]

und an anderer Stelle:

zitat

> ``*Der private Schlüssel sowie die Signiertechnik ist in der Regel auf einer Chipkarte gespeichert, die erst in Verbindung mit einer Personenidentifikationsnummer (PIN) eingesetzt werden kann."* [SigB]

Die Schlüsselgenerierung selbst wird nicht behandelt. Wie kommt der private Schlüssel auf die Chipkarte? Wieso mußdie Zertifizierungsstelle die privaten Schlüssel geheimhalten, wo sie diese doch nicht speichern darf? Wie kommt sie überhaupt in den Besitz der privaten Schlüssel, den sie geheimhalten soll? Warum werden PINs gegenüber biometrischen Verfahren priorisiert, wird doch damit der Schlüsselraum erheblich eingeschränkt? Biometrische Merkmale zur Identifizierung heranzuziehen ist zwar möglich, nach der Signaturverordnung (§16 Abs. 2 Satz 3). Es ist jedoch nicht zwingend vorgeschrieben. Warum? Fragen, die zu stellen sind. Mit der Sicherheit der Schlüsselgenerierung und -verwaltung steht und fällt das ganze System der Verschlüsselung mit Public Key-Verschlüsselung, wie es z.B. für digitale Signaturen eingesetzt wird.

Worin die Intention der unklaren gesetzlichen Aussagen zu sehen ist, kann man sich bei aufmerksammer Lektüre von Gesetz, Verordnung und insbesondere amtlicher Begründung zusammenreimen.

Unter der Überschrift ``Wirksamer Informationsschutz'' findet sich in der Begründung zum Gesetz der Absatz:

zitat

> ``*Ob unabhängig davon unter besonderen Aspekten spezielle >>Kryptoregelungen<< erforderlich sind, ist nicht Gegenstand des Gesetzentwurfs. Die Funktionen Signatur und Verschlüsselung sind technisch wie rechtlich völlig eigenständig zu betrachten. "* [SigB]

Aus juristischer Perspektive mag ein solcher Satz, wie der zweite des zitierten Absatzes, sinnvoll sein. Bei der Interpretation des Wortes `technisch' mußman stutzig werden. Wie bei der Erläuterung der kryptologischen Grundlagen für digitale Signaturen beschrieben, erzeugt man digitale Signaturen, in dem man das Resultat der Anwendung einer kryptographischen Hashfunktion auf eine Nachricht -den Hashwert- *verschlüsselt*. In diesem (mathematisch-technischen) Sinne kann von einer Eigenständigkeit keine Rede sein. Verbleibt also, das `technisch' als `implemtierungstechnisch' zu lesen. Dann würde die Aussage so zu verstehen sein, daßdie Implementierung zwar die Erzeugung digitaler Signaturen, nicht aber Verschlüsselung anderweitig gestatten soll - ein Schritt auf dem Wege zum `Kryptoverbot'.

Andere Passagen im Gesetz und in der Begründung lassen ähnliche Vermutungen zu. In der Begründung zu Paragraph 5 findet sich folgende Aussage:

zitat

> ``*... da davon ausgegangen werden kann, daß der Markt jedem Interessenten die Möglichkeit eröffnen wird, bei einer Zertifizierungsstelle einen Signaturschlüssel zu erwerben.''* [SigB]

Wohl fast jedem Kryptographen werden gewisse Zweifel an der Sicherheit eines so konzipierten Systems kommen, wird doch ein elementarer kryptologischer Grundsatz -Geheimhaltung des Schlüssels- verletzt, wenn dritte Personen Zugriff auf den privaten Schlüssel haben. Und diese Personen haben nicht bloßZugriff darauf, sie entscheiden sogar darüber, welche Schlüssel an wen vergeben werden! Dieses Verfahren hätte gewisse Ähnlichkeiten mit der Vergabe der PINs für EC-Karten, die in letzter Zeit stark in Verruf geraten ist.

> [**Anmerkung:** Noch aus einem anderen Grunde ist diese Aussage als bedenklich anzusehen: Im Hinblick auf den intendierten Einsatz digitaler Signaturen (u.a. als digitalem Ausweis) werden hoheitliche Aufgaben privatisiert. Damit wird die Möglichkeit eingeräumt, daß die Qualität zu einer Preisfrage gerät, was die Gleichbehandlung der Bürger in Frage stellt. Wie solches In-Frage-Stellen aussehen kann, läßt sich anhand der Behandlung von Kunden, die mit EC-Karte bargeldlos bezahlen wollen, ablesen: Inhaber von EC-Karten der Sparkassen können Beträge bis zu 400,-DM begleichen. Inhaber von EC-Karten, die durch die Deutsche Bank ausgegeben wurden, dürfen dagegen auch 2000,-DM begleichen. In manchen Geschäften wird die Angelegenheit so gehandhabt, muß man einschränken.]

Da beruhigt es auch nicht, wenn in der Begründung zu Paragraph 5 Absatz 4 steht:

zitat

> ``*Die in Satz 2 geforderte Geheimhaltung des Signaturschlüssels ist absolut. Es soll keine Person (auch nicht der Signaturschlüssel-Inhaber) Kenntnis vom privaten Signaturschlüssel erhalten, da andernfalls ein Mißbrauch des Signaturschlüssels nicht auszuschließen ist.''* [SigB]

Inwiefern ein berechtigter Schlüsselinhaber seinen eigenen Schlüssel mißbrauchen könnte, bleibt offen.

Es folgt gleich darauf, in der Erläuterung von Satz zwei, die Aussage:

zitat

> ``*Technisch unvermeidbare temporäre Zwischenspeicherungen beim gesicherten Ladevorgang sind damit nicht ausgeschlossen.*''[SigB]

Daraus ist wohl zu folgern, daßder private Schlüssel außerhalb der Chipkarte erzeugt (key generation) und anschließend darauf gespeichert werden soll (key installation). Mindestens im Schlüsselgenerator (key generator) wird er für eine gewisse Zeit zwischengespeichert werden, wenn dieser nicht auf der Chipkarte integriert wird.

Zieht man nun noch in Betracht, welche Anwendungen für digitale Signaturen vom Gesetzgeber u.a. vorgesehen werden, nämlich ``*digitaler Ausweis*'' ([SigB]) oder ``*automatische Feststellung der Urheberschaft elektronischer Post*'' ([SigB]) muß man befürchten, daß das Recht auf informationelle Selbstbestimmung der Bürger weiter ausgehöhlt wird. Dem Gesetzgeber ist das durchaus bewußt, findet sich in der Begründung zu Signaturgesetz doch die Aussage:

zitat

> ``*Signierte Daten in Dateien und Netzen können das Erstellen von Persönlichkeitsprofilen ... erleichtern.*'' [SigB]

Haftung der Trusted Third Parties

zitat

> ``*Mögliche Haftungsfragen sind aus den jeweiligen Verantwortlichkeiten und dem allgemeinen Haftungsrecht zu beantworten (jeder haftet für sein schuldhaftes Handeln oder Unterlassen).*''[SigB]
>
> ``*Hinsichtlich der Haftung der Zertifizierungsstellen gegenüber Dritten kann sich im Einzelfall eine Haftungslücke ergeben.*'' [SigB]

Im Prinzip ist das alles, was sich in der Begründung des Signaturgesetzes zum Thema Haftung findet. Der Gesetzestext selbst enthält keinerlei Haftungsregeln oder -beschränkungen. Das ist um so verwunderlicher, als vergleichbare Gesetze in den USA auf detaillierte Haftungsrichtlinien nicht verzichten (s. z.B. [UDSA]).

Die Adäquatheit bestehender Haftungsregelungen zu den Bedürfnissen, die aus dem neuen Gesetz erwachsen, ist zu bezweifeln. Zum einen fehlt es an einer passenden Rechtsprechung, zum anderen an ausreichenden Praxiserfahrungen mit vergleichbarer Technologie. Die vorliegenden Erfahrungen im breiten Einsatz von Chipkarten (Telefonkarten, EC-Karten, Krankenkassenkarten) sprechen eher gegen die Annahme, daß die Haftung bereits ausreichend geregelt sei.

Die implizierte Klarheit der Verantwortlichkeiten läßt sich meines Erachtens aus dem Gesetz nicht ableiten. Zwar läßt sie sich für die (behördliche) Wurzelinstanz erkennen. Für die nachgeordneten, privaten Zertifizierungsstellen bleibt dagegen offen, welche Haftungsbestimmungen greifen. Was geschieht, wenn sich die Genehmigungen der behördlichen Wurzelinstanz oder des amtlich bestellten Prüfinstituts als Fehler herausstellen, sei es in technischer oder in organisatorischer Hinsicht? Greift dann die Staatshaftung für die Behörde oder sind die Verträge zwischen Benutzer und Zertifizierungsstelle maßgeblich? Der Vergleich mit Kernkraftwerken, wie ihn Wendelin Bieser in der Begründung zum Signaturgesetz ([SigB]) anstellt, wirkt in dieser Hinsicht nicht sehr beruhigend.

Patente

Und noch etwas wird übersehen oder ignoriert: Alle bedeutsamen Verfahren für digitale Signaturen sind irgendwo patentiert. Und die Patente werden verwertet.

Die Patente schließen üblicherweise die Schlüsselgenerierung ein (siehe RSA). Die Folgerung lautet, daß Schlüsselpaare nicht kostenlos erhältlich sein werden. Da es nur sehr wenige praktikable Signaturverfahren gibt, haben die Patentinhaber praktisch eine Monopolstellung inne. Das Gesetz sieht diesbezüglich weder Beschränkungen, noch Öffnungsmaßnahmen vor. Der Einsatz von digitalen Signaturen kann somit schon an der Kostenfrage scheitern.

Fazit aus der Analyse des Gesetzes

(A)Es besteht die Gefahr, daßdas Grundrecht auf informationelle Selbstbestimmung weiter eingeschränkt wird. Inwieweit ist eine solche Einschränkung, durch unmittelbare oder mittelbare Einschränkung von Verschlüsselung, zu befürchten? Folgende Punkte sind mindestens zu nennen:

1. Der Schlüsselinhaber hat nicht die vollständige Autonomie über den privaten, d.h. den geheimen Schlüssel. Die Wahl des Verschlüsselungsverfahrens ist nur eingeschränkt möglich. Die vorgegebenen Verfahren der Schlüsselerzeugung und Schlüsselinstallation sehen keine individuelle Schlüsselwahl als zwingend vor. Die gleichzeitige Verwendung mehrerer, alternativer Verschlüsselungsverfahren scheint nicht möglich zu sein. Das Gesetz bleibt in diesem Punkte unklar.

2. Der vorgesehene Umgang mit den privaten Schlüsseln ist aus kryptologischer Sicht zumindest bedenklich (z.B. temporäre Zwischenspeicherung). Verfahren, bei denen der geheime (private) Schlüssel zeitgleich nur an einer einzigen Stelle existiert, sind nicht zwingend vorgeschrieben. Der Schlüsselraum wird durch den Einsatz von PINs (mit verhältnismäßig geringer Länge) anstelle von einmaligen biometrischen Merkmalen stark eingeschränkt.

3. Die künstliche Trennung zwischen Signatur und Verschlüsselung legen den Schluß nahe, daß Kryptographie später -in einem anderen Gesetz- von staatlicher Seite eingeschränkt werden soll. Aussagen des Bundesinnenministers und seines Staatssekretärs weisen in dieselbe Richtung. (s. [Kanther 1997])

4. Eine Infrastruktur für Schlüsselverwaltung und Zertifizierung im Sinne des Gesetzes kann jederzeit für ein umfassendes `key recovery'/`key escrow'-Programm eingesetzt werden. Damit kann die Wahrnehmung des ``Grundrechts auf Verschlüsselung'' ([Koch 1997]) behindert oder gar verhindert werden.

5. Schlüsselverwaltung und Signaturen im Sinne des Gesetzes können zur Erstellung von Benutzer- und Bewegungsprofilen ohne Kenntnis des Schlüsselinhabers benutzt werden. Der vorgeschlagene Einsatz von Chipkarten als digitalem Ausweis gestattet dies. In der automatischen Absenderkontrolle bei elektronischer Post liegt das Risiko einer De-Anonymisierung. Eventuell gewünschte oder notwendige Vertraulichkeiten sind so u.U. gefährdet.

6. In der Verordnung zum Signaturgesetz wird in §13 verlangt, eine Kopie vom Ausweis oder eines anderen Identitätsnachweises des Antragstellers anzufertigen und aufzubewahren - für 35 Jahre. Diese Bestimmung verstößt meines Erachtens gegen das Bundesdatenschutzgesetz, da mehr Daten erhoben werden, als für die Durchführung der Geschäftstätigkeit notwendig sind (vgl. BDSG §13 - Datenerhebung). Art und Weise der Kopie sind nicht genau spezifiziert, könnten demnach auch elektronisch (z.B. durch Einscannen) angefertigt werden. Einer unzulässigen Auswertung steht danach nichts mehr im Wege, außer der Datenschutz.

7. Das Signaturgesetz sieht eine flache, zweistufige Hierarchie mit einer Genehmigungsbehörde oben und lizenzierten Zertifizierungsstellen unten vor. Die Behörde erteilt der Zertifizierungsstelle [4] die Lizenz nach einer Evaluierung (z.B. durch das BSI) [5]. Das Kontrollrecht liegt ausschließlich bei der Behörde. Den Betroffenen (Schlüsselinhabern und Zertifkatsnachfragern) ist eine Kontrolle nicht möglich. Es steht zu befürchten, daß im Streitfalle der Bürger oder die Firma der Zertifizierungsstelle wird nachweisen müssen, daß diese versagt hat (analog dem Verfahren bei EC-Kartenvorfällen [6]). Ohne Einblick in die internen Vorgänge und Abläufe wird das nicht möglich sein und so geraten Bürger oder Firma in eine Ohnmachtsposition. Erfahrungen dazu gibt es vom EC-Kartenbetrug und den Fällen überhöhter Telefonrechnungen der Telekom in den letzten Jahren. Simulationsstudien haben ihrerseits Schwachstellen nachgewiesen [7]. Im übrigen kehrt sich das Beweisverfahren um: Wo bei der einzelnen Unterschrift im Zweifelsfalle nachgewiesen werden muß (z.B. durch gutachterliche Untersuchungen), daß derjenige, von dem sie zu stammen scheint, tatsächlich der Urheber ist, steht der Schlüsselinhaber bei der digitalen Signatur in der Pflicht, da gemutmaßt wird, daß er die Signatur erstellt hat. Eine klare Schwächung der Bürgerposition.

(B)Detaillierte Haftungsregelungen fehlen gänzlich. Der grundgesetzlich verankerte Schutz des Eigentums ist für den Fall gefährdet, daßsich bei Fehlern die Verantwortlichkeiten nicht identifizieren lassen. Bei komplizierten technischen Abläufen, wie sie Zertifizierung und Authentifizierung erfordern, gibt es diesbezüglich ein großes Risikopotential, das nicht kompensiert wird.

(C) Die Stellung der Patentinhaber wurde nicht genügend beachtet. Zertifizierungsinstanzen kommen nach dem vorliegenden Gesetz nicht umhin, Patente in Anspruch zu nehmen (mangels alternativer Verfahren). So werden sie gezwungen sein, entsprechende Gebühren zu zahlen. Die faktische Monopolstellung der Patentinhaber stellt den neuralgischen Punkt dar. Ein fairer Wettbewerb zwischen ihnen ist nicht

erkennbar.

(D) Das technische Fundament für die im Gesetz festgeschriebene asymmetrische Verschlüsselung hat seine Tragfähigkeit auf Dauer noch nicht unter Beweis gestellt. Bei einer unbeschränkten Einführung digitaler Signaturen im großen Rahmen besteht die Gefahr einer ernsthaften Gefährdung des Rechtsgefüges, sollten sich die den Verfahren zugrundeliegenden kryptologischen Annahmen in näherer oder fernerer Zukunft als falsch erweisen. Die Möglichkeit einer Rücknahme der Entwicklung dürfte in wenigen Jahren nicht mehr bestehen.

(E) Einer Internationalisierung des elektronischen Handels steht entgegen, daß das Gesetz die einschlägigen internationalen Standards nicht als (rechts-)verbindlich vorsieht, sondern statt dessen eine nationale Regelung schafft.

Digitale Signaturen

zitat

> *``For practical applications, digital signatures are one of the two most important cryptologic primitives. In particular with the rise of electronic commerce on the Internet and the World Wide Web, they may become even more important than the better-known schemes for message secrecy.''* [Pfitzmann 1996], Preface

Konzepte für authentischen und beweisbaren Dokumentenaustausch

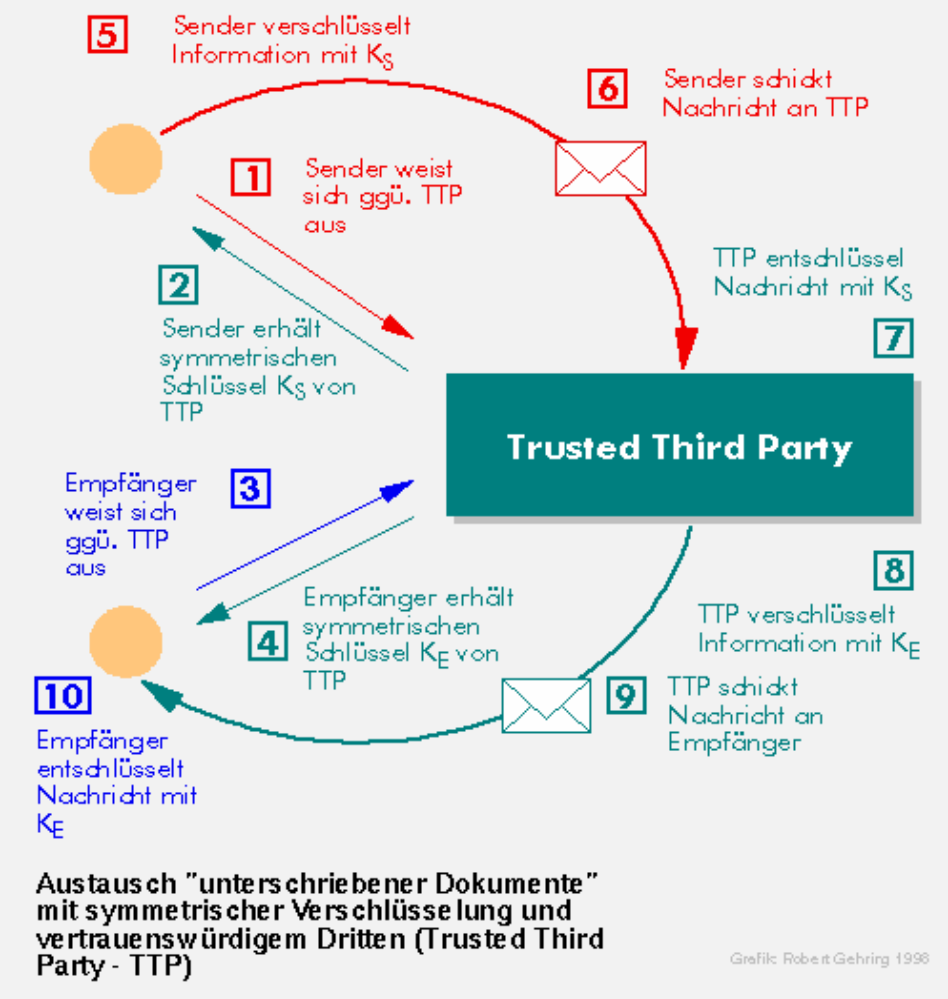
Zum authentischen Dokumentenaustausch zwischen zwei Kommunikationspartnern greift man auf Verschlüsselungsverfahren zurück. Gründe dafür wurden im Verlauf des voranstehenden Textes an verschiedenen Stellen diskutiert. Wenn es darum geht, solchen Dokumentenaustausch beweisbar zu machen, müssen die Protokolle, wie sie bisher vorgestellt wurden, teilweise erweitert werden. Die Ziele, die es zu erreichen gilt, wollen wir noch einmal zusammenfassen.

- Identifikation des (Ab-)Senders des Dokuments.
- Absicherung der Integrität des Dokuments.
- Beweisbarkeit des Dokumententransfers.

Historisch bedingt gibt es mehrere Ansätze, digitale Signaturen zu implementieren. Solange die Qualität der Public Key-Kryptographie noch schwer einzuschätzen war, wurde vorrangig an symmetrischen Verfahren zur authentifizierten Kommunikation gearbeitet. Später wurde klar, daßPublic Key-Verfahren zumindest für den breiten Einsatz vorteilhafter sind. Ob sich deren Weiterentwicklung, sogenannte Fail-Stop-Signaturen werden durchsetzen können, läßt sich aus der Perspektive der Gegenwart noch nicht abschätzen. Wir werden alle drei Stufen der Entwicklung beschreiben.

Dokumentenaustausch mit symmetrischer Verschlüsselung

Bei diesen Verfahren geht es nicht um eine ``Unterschrift'' im Sinne des Alltagsgebrauchs. Vielmehr sollen einige Funktionen der Unterschrift nachgebildet werden. Ziel ist es, Dokumente auf elektronischem Wege mit vergleichbarer Sicherheit wie bei der digitalen Signatur, auszutauschen. Im Zentrum des Geschehens agiert eine Trusted Third Party als Vermittler. Die folgende Grafik zeigt das Ablaufschema.



Sender und Empfänger einigen sich auf eine vertrauenswürdige Instanz, die sie als Vermittler einsetzen. Von dieser erwerben beide je eine Kopie eines symmetrischen Schlüssels, wozu sie ihre Identität belegen müssen. Eine Kopie der vergebenen Schlüssel bleibt im Besitz der Trusted Third Party. Die von der Trusted Third Party vergebenen Schlüssel müssen sich unterscheiden. Im Prinzip ist es auch möglich, daßSender und Empfänger unterschiedliche Verschlüsselungsverfahren einsetzen. Dazu mußdie Trusted Third Party (TTP) jedoch in der Lage sein, beide Verfahren anzuwenden.

Der Sender erzeugt dann ein Dokument und verschlüsselt es mit seinem symmetrischen Schlüssel. Die resultierende Nachricht übermittelt er der Trusted Third Party zusammen mit der `Adresse' des Empfängers.

Sobald die Trusted Third Party eine Nachricht erhält, entschlüsselt sie diese mit dem Duplikat des Senderschlüssels. Eine erfolgreiche Entschlüsselung zeigt die Authentizität der Nachricht an. Sodann nimmt sie das Duplikat des Empfängerschlüssels und verschlüsselt die Information damit. Dadurch bekommt sie eine Nachricht, die sie zusammen mit einem Vermerk über den Absender an den Empfänger schickt.

Der Empfänger entschlüsselt die Nachricht von der Trusted Third Party und vertraut dieser, daß die Nachricht wirklich vom angegebenen Absender stammt und authentisch ist.

Ohne volles Vertrauen in die Trusted Third Party läßt sich das Verfahren in der beschriebenen Form nicht abwickeln. Ohne Trusted Third Party selbstverständlich auch nicht. Diese garantiert die Authentizität der Kommunikation und die Sicherheit der geheimen (symmetrischen) Schlüssel. Da die Trusted Third Party weiß, wann von wem an wen welche Nachricht geschickt wurde, kann keine der Parteien ihre Beteiligung abstreiten oder den Inhalt des Dokuments in Frage stellen. Sender oder Empfänger können mit Hilfe der Trusted Third Party gegenüber Außenstehenden nachweisen, welche Kommunikation stattgefunden hat. Voraussetzung ist, daß Außenstehende die Trusted Third Party ihrerseits als glaubwürdig akzeptieren.

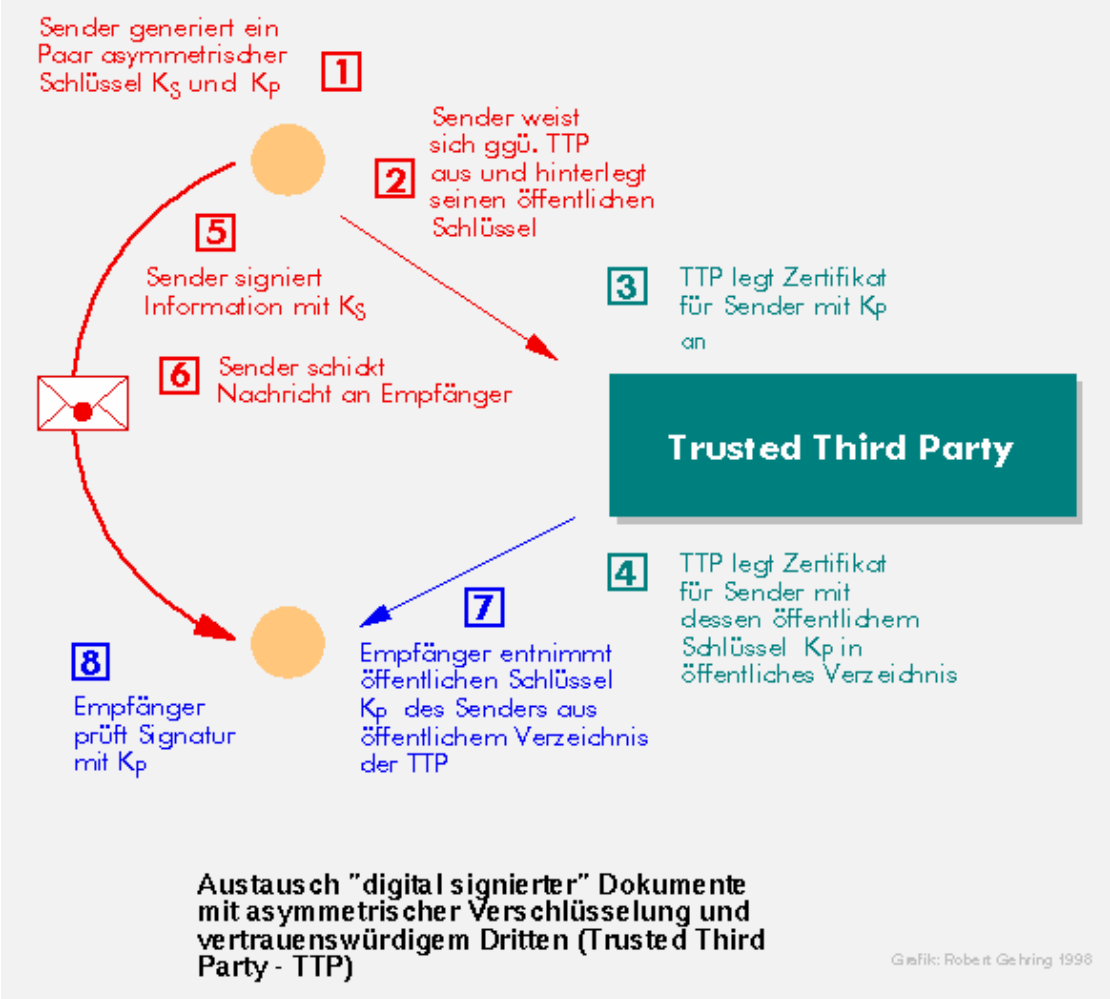
Um ihre Aufgabe zu erfüllen, muß die Trusted Third Party einen ziemlich hohen Aufwand für die Schlüsselverwaltung, die Kommunikation mit den Teilnehmern und die Archivierung von Nachrichten leisten. Die zentrale Verwaltung von Schlüsselkopien wird darüber hinaus Begehrlichkeiten bei Unbefugten wecken. Viele Leute werden auch nicht damit einverstanden sein, daß eine zentrale Stelle von ihren

Dokumenten Kenntnis erlangen kann, so sie will. Man sieht, für den praktischen Einsatz weist diese Methode einige Unzulänglichkeiten auf.

Im weiteren werden wir den Ansatz untersuchen, der nicht nur die größte Verbreitung gefunden hat, sondern auch durch das Signaturgesetz vorgesehen ist ([SigG §2(1)]).

Digitale Signaturen mit Public Key-Verschlüsselung

Digitale Signaturen mit Public Key-Verschlüsselung kommen nicht ohne Trusted Third Party aus. Darin ähneln sie dem zuerst beschriebenen Verfahren für authentischen, beweisbaren Dokumentenaustausch. Der Umfang der Dienste, auf die man angewiesen ist, kann dagegen drastisch reduziert werden. Die nächste Grafik zeigt den schematischen Ablauf:



Im Bild ist K_S der geheime Schlüssel (secret key) und K_P der öffentliche Schlüssel (public key).

Den ersten Schritt seitens des Senders stellt die Schlüsselgenerierung dar. Wie oben erläutert, handelt es sich um ein Paar Schlüssel, von denen einer geheim und nur dem Sender zugänglich bleibt. Der öffentliche Schlüssel aus dem Paar wird vom Sender bei der Trusted Third Party hinterlegt. Dort läßt man sich vom Sender die Identität bescheinigen und zertifiziert den öffentlichen Schlüssel.

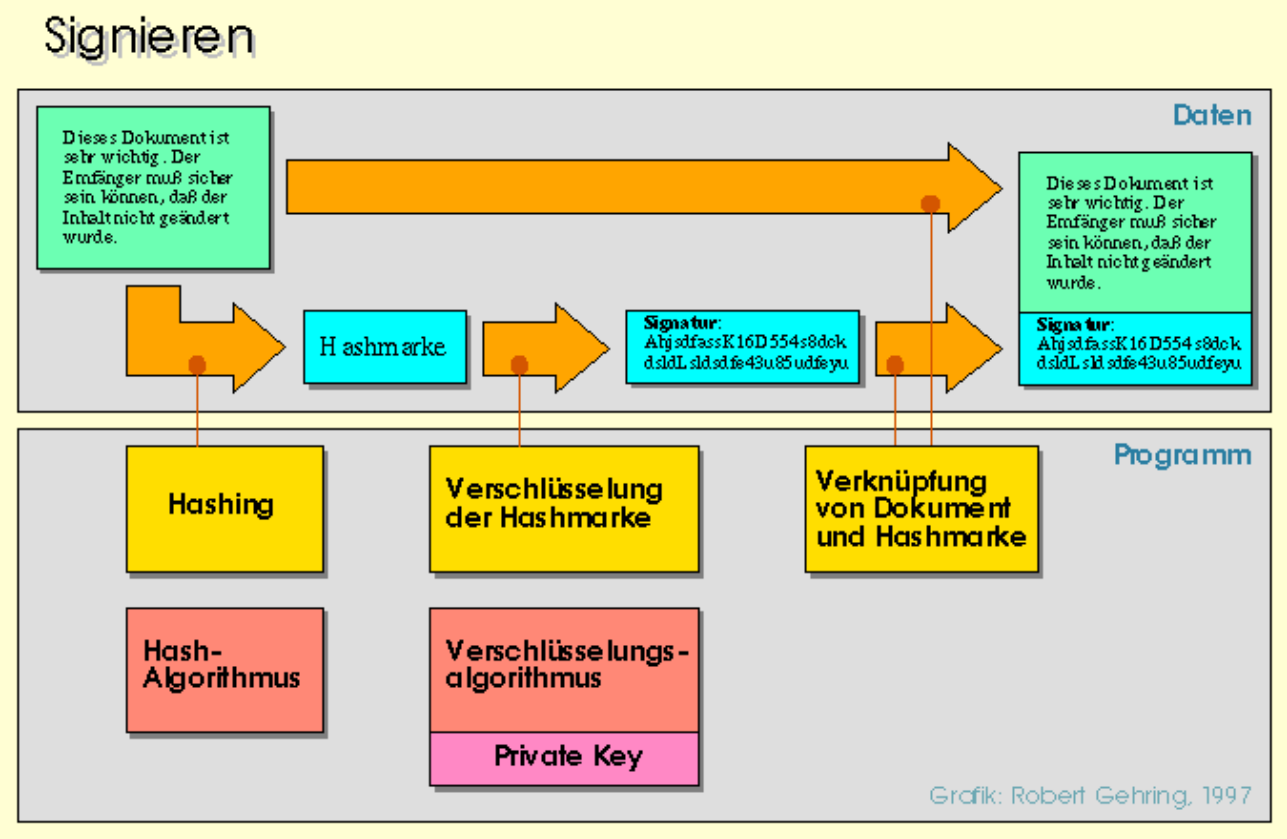
Um sicherzustellen, daß der Sender nicht einen fremden öffentlichen Schlüssel als den seinigen ausgibt, testet die Trusted Third Party den öffentlichen Schlüssel. Dazu wird z.B. eine Zufallszahl mit dem öffentlichen Schlüssel verschlüsselt. Anschließend muß der Antragsteller, d. h. der Sender, der ein Zertifikat beantragt, die verschlüsselte Zufallszahl wieder entschlüsseln. Schafft er das, so ist bewiesen, daß er über den geheimen Schlüssel zu dem von ihm vorgelegten öffentlichen Schlüssel verfügt.

Nach der Überprüfung des Senders wird das Zertifikat mit dem öffentlichen Schlüssel in ein öffentlich zugängliches Verzeichnis auf dem Server der Trusted Third Party gelegt. Je nach Struktur der Zertifikate werden Zeitmarken, Gültigkeitsbeschränkungen etc. zusätzlich darin vermerkt.

Der Sender kann nun eine Nachricht mit seinem geheimen Schlüssel signieren und an den Empfänger schicken. Will der Empfänger überprüfen, ob die Nachricht vom vorgeblichen Sender stammt und auch unverändert ist, verschafft er sich den öffentlichen Schlüssel des Senders bei der Trusted Third Party. Damit testet er die Signatur des Dokuments. Diesen Test kann er auch einem Außenstehenden vorführen und diesem gegenüber die Herkunft der Nachricht beweisen.

Dieser Beweis hängt von der Qualität der Signatur und der Zuverlässigkeit der Trusted Third Party ab. Erstere wird durch das Signierverfahren abgesichert. Letztere hängt von angemessenen technischen Maßnahmen und deren Kontrolle ab.

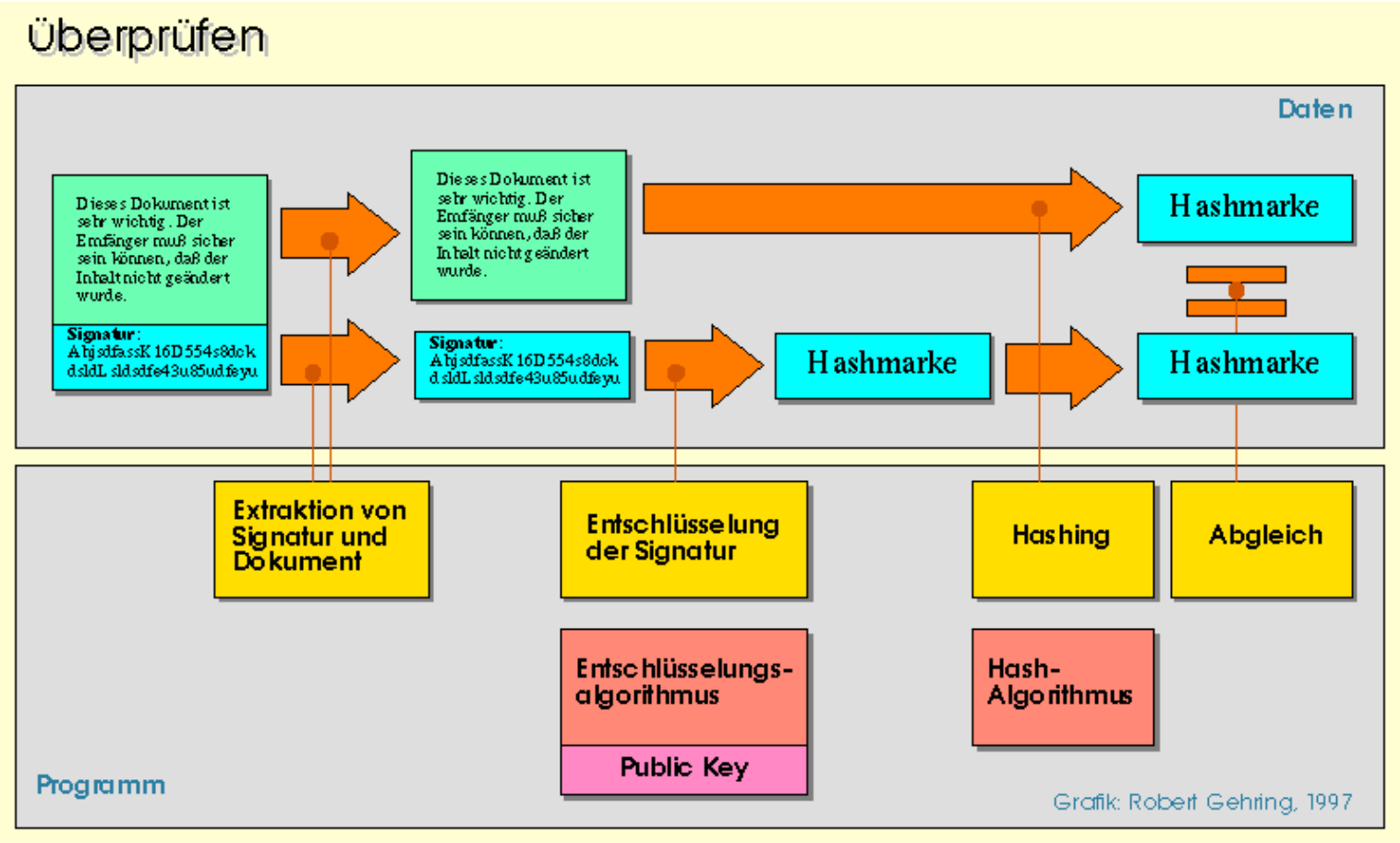
Folgende, schematische Darstellung zeigt den Vorgang der Erzeugung einer digitalen Signatur zu einem Dokument.



Zuerst wird vom Sender der Hashwert(Hashmarke- hash mark) des Dokuments erzeugt. Dazu verwendet er den Dokumententext als Eingabe für einen kryptographischen Hashalgorithmus (z.B. MD5). Der resultierende Hashwert ist in fast allen Fällen kürzer als das Dokument (z.B. 128 Bit bei MD5).

Der Hashwert wird dann mit einem Public Key-Verfahren verschlüsselt, wozu der private Schlüssel des Senders herangezogen wird. Das Ergebnis der Verschlüsselung des Hashwertes stellt die digitale Signatur des Dokumentes dar. Vom Sender wird diese Signatur an das Dokument angefügt und der entstehende Verbund an den Empfänger geleitet.

Ist die Sendung beim Empfänger angekommen, überprüft jener, was er erhalten hat, auf seine Richtigkeit:



Die Überprüfung beginnt mit der Abtrennung des Signaturteils vom eigentlichen Dokument. Darauf erfolgt die Entschlüsselung mit dem öffentlichen Schlüssel des Senders. Im Ergebnis hat der Empfänger die unverschlüsselte Hashmarke extrahiert. Der nächste Schritt ist die erneute Anwendung der Hashfunktion auf das Dokument. Die dabei entstehende Hashmarke wird mit der entschlüsselten Hashmarke verglichen. Falls die Hashmarken sich völlig gleichen, kann der Empfänger zufrieden sein. Er hat wirklich das Dokument bekommen, das der Sender ihm geschickt hat. Nicht ein einziges Bit daran hat sich geändert.

Den schrittweisen Ablauf des Protokolles kann man etwas formaler so beschreiben:

Vor der Kommunikation:

- Vereinbarung eines Public Key-Verfahrens;
- Generierung eines zugehörigen Schlüsselpaares;
- Veröffentlichung/Zertifizierung des erzeugten öffentlichen Schlüssels;

Während der Kommunikation:

Sender

- Erzeugen des Dokuments;
- Hashen des Dokuments;
- Verschlüsseln des Hashwertes mit privatem Schlüssel;
- Anhängen des verschlüsselten Hashwertes an den Dokumententext;
- Versenden des Dokuments über einen beliebigen Kanal;

Empfänger

- Zerlegen der erhaltenen Sendung in Dokument und Signatur;
- Entschlüsseln der Signatur;

- Hashen des Dokuments;
- Vergleich des erhaltenen Hashwerts mit der entschlüsselten Signatur (Gleichheit bedeutet korrekten Erhalt des Dokuments, Ungleichheit bedeutet, daß das Dokument auf seinem Weg verändert wurde);

Nach der Kommunikation:

- (ggf.) Quittierung oder Neuanforderung des Dokuments;

Randbedingungen

Erst eine Vielzahl von Restriktionen macht digitale Signaturen zu dem, was sie sind. Was sie sein könnten, sollte man vorsichtiger formulieren. Ihren praktischen Wert müssen sie in einem breiten Einsatz erst noch nachweisen. Die Sicherheit des Einsatzes wird wesentlich von der Erfüllung der Randbedingungen bestimmt.

Zu den Randbedingungen gehören in erster Linie die Verwendung kollisionsfreier Hashfunktionen, exakte Zeitangaben, gute Schlüssel und nachweisbar sichere Zertifikate.

Kollisionsfreie Hashfunktionen

zitat

> *``Hash functions ... are important tools to protect information integrity. Together with digital signature schemes, they play an important role for securing our electronic interactions, ..."*
> [Preneel 1997]

Eine Schlüsselstellung hat bei digitalen Signaturen die Hashfunktion inne. Es handelt dabei sich nicht um eine gewöhnliche Hashfunktion, sondern um eine kollisionsfreie Einweg-Hashfunktion (collision-free one-way hash function, CFOWHF) mit fester Länge der Ausgabe.

Einweg-Hashfunktion wurden bereits bei den Definitionen eingeführt. Kollisionsfreiheit der Hashfunktion bedeutet, daßes nicht möglich ist, in vertretbarer Zeit zwei Eingaben für die Hashfunktion zu finden, die denselben Hashwert haben. Diese Eigenschaft wird gefordert, um es einem Angreifer oder betrügerischen Sender unmöglich zu machen, eine falsche Nachricht unterzuschieben. Unterscheiden sich zwei Dokumente auch nur in einem Bit, was einem unaufmerksamen Betrachter leicht entgehen kann, so werden unübersehbar unterschiedliche Hashmarken errechnet.

DaßHashfunktionen überhaupt verwendet werden müssen, ist dem Umstand geschuldet, daßPublic Key-Kryptographie sehr langsam ist. Um die zu verschlüsselnde Datenmenge klein und damit die Rechenzeit kurz zu halten, werden die Dokumente der Komprimierung durch einer Hashfunktion unterworfen. Selbst sehr lange Dokumente bekommen nur einen ziemlich kurzen Hashwert (etwa 128 oder 160 Byte). Den zu verschlüsseln verursacht keine störende Zeitverzögerung.

Dadurch, daßder Hashwert mit dem privaten Schlüssel verschlüsselt wird, kann der Sender später nicht abstreiten, die Nachricht signiert zu haben. Die Überprüfung der Signatur mit dem zugehörigen öffentlichen Schlüssel zeigt, ob eine Nachricht mit dem entsprechenden privaten Schlüssel signiert wurde.

Auf die Hashfunktion entfallen demnach drei Aufgaben:

- Datenumfang für die Verschlüsselung und Übertragung möglichst gering halten;
- Integrität der Daten sicherstellen;
- Unwiderrufbarkeit des Dokumentes sichern (Beweisbarkeit der Zuordnung zum Absender);

[**Anmerkung:** Bei sehr kurzen Nachrichten kann auf eine Hashfunktion verzichtet werden, da der Hashwert unter Umständen länger als die Nachricht ausfällt. Statt dessen wird das Dokument direkt verschlüsselt und das Resultat an das unverschlüsselte Dokument angehangen. Bei geeigneter Wahl der Verschlüsselungsfunktion erfüllt dieser Appendix die Funktion des verschlüsselten Hashwertes ebensogut. In der Praxis werden die Anwendungsmöglichkeiten dafür beschränkt sein.]

Sichere Zertifizierung des öffentlichen Schlüssels

Beide Kommunikationsteilnehmer müssen mit absoluter Sicherheit über die Identität des anderen im Bilde sein. Gleiche absolute Sicherheit wird für die Authentizität der Schlüssel gefordert. Dazu bedienen sich die Kommunikationspartner entweder der unmittelbaren Schlüsselübergabe, einer `Trusted Third Party' oder eines `Web of Trust'. Die Auswahl bestimmt der Zweck. Die Verfahrensweisen wurden oben vorgestellt. Die Beweissicherheit ist bei Einbeziehung einer verläßlichen Trusted Third Party sicher am größten.

Um an öffentliche Schlüssel gelangen, sowie die Zertifikate abfragen zu können, müssen online-Zugänge zur TTP eingerichtet werden.

Die Aufgaben der Zertifizierung lauten:

- Identität der Kommunikationspartner absichern;
- Öffentliche Schlüssel zugängig machen;
- Authentizität der öffentlichen Schlüssel garantieren;

Exakte Zeitangaben

Sinnvoll kann es sein, jede Aktion mit einer Zeitangabe zu versehen. So ist in einem später möglicherweise folgenden Streitfall eine Rekonstruktion des zeitlichen Ablaufs durchführbar. Bedingung ist, daßbeide Partner über dieselbe Zeitangabe verfügen. Am leichtesten läßt sich diese per Funkuhr einstellen. Jede einzelne Transaktion kann mit einem Zeitstempel versehen werden, der analog dem Hashwert verschlüsselt und dem Dokument hinzugefügt wird. Die Systemzeit der meisten Rechner ist in der Regel ungeeignet.

Durch die Integration von Zeitmarken ins Protokoll kann verhindert werden, daß der Sender nach Absendung des Dokuments seinen geheimen Schlüssel veröffentlicht, d.h. mutwillig kompromittiert, und anschließend behauptet, nicht der Absender des signierten Dokuments zu sein. Anhand der Zeitmarke läßt sich herausfinden, ob der `Schlüsselverlust' vor oder nach der Signierung stattfand.

Gute Schlüssel

zitat

> ``*... in all publications in theory, it is assumed that participants generate their own secret keys, so that the keys deserve the attribute "secret". This procedure is also strongly recommended for practical applictions."* [Pfitzmann 1996], S.17

Wer wirklich sicher sein will, daßsein geheimer Schlüssel tatsächlich ein *geheimer*Schlüssel ist, kann und darf nicht darauf verzichten, den Schlüssel mit einem sicheren Verfahren selbst zu generieren. Der dazu nötige Rechenaufwand hält sich in Grenzen. Selbst auf einem langsamen PC handelt es sich bloßum Sekunden oder Minuten. Und sollte es wesentlich länger dauern, ist der Computer für Verschlüsselung ohnehin nicht geeignet.

Zu jedem Verschlüsselungsverfahren werden bestimmte Schlüsselgenerierungsalgorithmen empfohlen. Insofern diese Empfehlungen von Kryptologen ausgesprochen werden und in der Fachliteratur gutgeheißen werden, kann man darauf zurückgreifen. Mißtrauen ist gegenüber als ``neu und besonders sicher" angepriesenen Verfahren ohne entsprechende Referenzen angebracht.

Fail-Stop-Signaturen

zitat

> ``*Forging a signature is as hard as in the most secure ordinary digital signature schemes, but if, for all that, someone succeeds in forging, the supposed signer can prove that this happened ..."* [Pfitzmann 1996], Preface

Noch relativ neu sind Fail-Stop-Signaturen, die auf *Birgit Pfitzmann* und *Michael Waidner* zurückgehen. Ihrem Design liegen zusätzlich zu den allgemeinen Sicherheitsansprüchen digitaler Signaturen noch weitere zugrunde:

- Signaturen sollen mit minimalem Aufwand getestet werden können.
- Fälschungen sollen feststellbar und nachweisbar sein.
- Das Protokoll soll möglichst ohne Trusted Third Party auskommen.

[**Anmerkung:** Außer in dem Buch von B. Pfitzmann ([Pfitzmann 1996]) finden sich in der aktuellen kryptologischen Fachliteratur nicht sehr viele Darstellungen zu Fail-Stop-Signaturen. Insbesondere findet sich keine gute, kompakte Darstellung.]

Bruce Schneier gibt in [Schneier 1996] auf den Seiten 102 und 103 einen kurzen Abriß der Idee (*Zusammenfassung*):

> Man benötigt einen Public Key-Verschlüsselungsalgorithmus, der zu jedem öffentlichen Schlüssel eine sehr große Anzahl geheimer Schlüssel benutzen kann. Der Aufwand, ein Paar aus geheimem und öffentlichem Schlüssel zu generieren, darf nicht wesentlich größer als bei anderen Signaturverfahren sein. Die Möglichkeit, einen bestimmten geheimen Schlüssel aus dieser großen Menge gezielt auswählen zu können, muß dagegen sehr klein, praktisch Null sein. Der Aufwand, aus einem signierten Dokument und einem öffentlichen Schlüssel einen passenden geheimen Schlüssel zu errechnen, sollte in die Komplexitätsklasse NP fallen. Jeder mögliche geheime Schlüssel führt zu einer anderen Signatur.
>
> Der Sender generiert ein Paar aus geheimem und öffentlichen Schlüssel. Der öffentliche Schlüssel wird wie üblich seiner Bestimmung zugeführt und veröffentlicht. Auch die Kommunikation wird wie gewöhnlich vorgenommen, d.h. signiert wird mit dem geheimen Schlüssel, getestet mit dem öffentlichen Schlüssel.
>
> Falls es einem Angreifer gelingen sollte, zu dem öffentlichen Schlüssel einen passenden geheimen Schlüssel zu finden, so ist die Wahrscheinlichkeit, daß der gefundene Schlüssel derselbe ist wie der geheime Schlüssel des Senders, sehr gering. Praktisch ist es ausgeschlossen, denselben Schlüssel zu finden. Wenn mit dem gefundenen Schlüssel Dokumente signiert werden, so wird eine andere Signatur erzeugt, als mit dem richtigen (echten), geheimen Schlüssel des Senders. Das kann der Sender gegenüber Außenstehenden vorführen und so beweisen, daß die Signatur eine Fälschung ist. Eine Trusted Third Party zur Identifizierung ist deshalb verzichtbar.

Fußnoten

[1] Der Begriff der *Authentifizierung* geht auf den der *Authentizität* zurück und hat in unserem Zusammenhang die Feststellung von Identität zum Gegenstand.

Bruce Schneier definiert ihn so:

zitat

> ``*Es sollte dem Empfänger möglich sein, die Herkunft einer Nachricht zu ermitteln; ein Eindringling sollte sich nicht als andere Person ausgeben können.* "[Schneier 1996], S. 2 (!)

Menezes/Vanstone/van Oorschot unterscheiden zwischen `` *data origin authentication*" und ``*entity authentication*". Erstere stellt auf die Identität und Integrität der Daten ab (``*Data origin authentication implicitly provides data integrity ... if a message is modified, the source has changed.*''), letztere auf die Identität der Kommunikationsteilnehmer. [Menezes/Vanstone/Oorschot 1997], S. 4 (!) Deren Integrität allerdings kann mit Authentifizierung nicht sichergestellt werden.

CRISIS bietet vielleicht die umfassendste Betrachtung:

zitat

> *``... individuals in an information age may wish to be able to:*
>
> *...*
>
> *Ensure that a party with whom they are transacting business is indeed the party he or she claims to be. Likewise, they may seek to authenticate their own identity ... In an electronic domain without face-to-face communiations or recognizable indicators such as voices and speech patterns (as used today in telephone calls), forgery of identity becomes increasingly easy."* [CRISIS 1997], S. 42

Zu Problemen der Echtheit und Authentizität siehe auch: Anntotation zu Walter Benjamin - Das Kunstwerk im Zeitalter seiner elektronischen Reproduzierbarkeit.

[2] Zur netzartigen Struktur der Zertifizierung bei PGP siehe z.B.: [Grimm 1996], [Wobst 1997 (I)]

[3] Dazu ein Zitat:

zitat

> *``Die Sicherheit von Aussagen zur Identität des Urhebers von elektronischen Signaturen wird durch vier Faktoren beeinflußt:*
>
> *- Unikat des Schlüsselpaares[42]*
> *- Zugriffssicherung zum Trägermedium*
> *- Sperrdienste*
> *- Sicherheit der Ausgabeverfahren und Verzeichnisdienste*
>
> *Der Nachweis der Unikatssicherung von Schlüsselpaaren und der korrekten Ausgabeverfahren und Verzeichniseinträge ist gleichermaßen ein Validierungs- wie Revisionsproblem. ...*
>
> *[42] Zielkonflikte ergeben sich dafür aus Interessen der inneren Sicherheit. ..."* [Hammer 1993]

[4]Anwärter für Zertifizierungsstellen sind derzeit (März 1998) die Telekom und das Gespann debis/Bundesdruckerei. Als Aspiranten in spe dürften fast alle großen Banken und Versicherungsgesellschaften in Frage kommen. Den maßgeblichen Antrieb bildet die Hoffnung auf Großgeschäfte mit Behörden.

[5] Eine solche Zertifizierung stellt allerdings keine Garantie dar, daß ein System wirklich sicher ist. Siehe z.B. [Versteegen 1997].

[6] Zu den ``Schwierigkeiten" mit der Sicherheit beim EC-Verfahren und ihren Konsequenzen siehe z.B.:
[OLG Hamm (31 U 72/96)] , [Rossa 1997(I)], [Rossa 1997(II)], [Pausch 1997], [Heine 1997], [SPIEGEL 36/1997]

[7] Siehe z.B. den Bericht zur provet/GMD-Simulationsstudie von *Volker Hammer*:

zitat

> *``Im Rahmen der Simulationsstudie Rechtspflege und in ihrem Umfeld wurden eine Reihe von Angriffen durchgeführt. Obwohl den sachverständigen Testpersonen dieses Versuchsziel bekannt war, gelang es unter anderem, Dokumente zu manipulieren, Chipkarten mit PIN zu entwenden und beliebige oder teilweise veränderte Dokumente zum Signieren unterzuschieben. Die Angriffe gelangen völlig unabhängig vom mathematischen Teil des Signaturverfahrens ..."*
>
> *``Werden dagegen elektronische Signaturen mit Chipkarten gefälscht, gibt der Augenschein keinerlei Hinweis auf deren Unechtheit. Ein betroffener Chipkarteninhaber kann allenfalls versuchen, z.B. durch Zeugen zu belegen, daß die Signatur nicht von ihm stammen kann."* [Hammer 1993]

key revocation

key revocation (engl.) - Schlüsselwiderrufung, Schlüsselrückruf

key backup

key backup (engl.) - Schlüsselsicherungskopie

Geschichte digitale signaturen

diplomarbeit · robert gehring

Inhaltsverzeichnis

[**Lesehinweis:** Abschnittsüberschriften werden mit einer einfachen Markierung eingeleitet. Teilabschnitte beginnen mit einer doppelten Markierung und Unterabschnitte von Teilabschnitten haben eine dreifache Markierung. Art und Weise der Markierung entsprechen derjenigen im Inhaltsverzeichnis. Jeder Teilabschnittsüberschrift werden die `übergeordneten' Überschriften klein vorangestellt, um die Orientierung zu erleichtern. Am Ende jedes Abschnittes findet sich -optisch hervorgehoben- eine sehr kompakte Zusammenfassung. Absätze werden mit einem Kästchen beendet. Zitate sind kursiv gedruckt. Fußnoten werden durch Zahlen in eckigen Klammern markiert und finden sich am Ende des Dokumentes. Die Fußnoten sind gelinkt.]

Prolog

Grundsätzlich gibt es zwei Methoden, Geschichtsschreibung zu betreiben. Die eine erkennt das Ziel und zeigt die

Kausalitäten, die zu seiner Erreichung führten. Die andere begreift Geschichte als durch menschliches Handeln realisierte Möglichkeiten, wobei im Vollzug einer Handlung nicht notwendig eine bestimmte Konsequenz angelegt ist. In diesem Sinne ist jede Geschichte Interpretation und der Schluß von der Gegenwart auf die Vergangenheit eine Idee, keine Wahrheit. Bildhaft gesprochen könnte man sagen, man befinde sich in einem Delta mit vielen Zu- und Abflüssen.

Im folgenden Text sollte der Leser sich auf eine Geschichtsdarstellung nach dem zweiten Modell einlassen. Wir suchen nach verschiedenen Spuren in der Geschichte, die in engerem Bezug zum Sujet stehen. Den Bezug zwischen ihnen stellt unsere Frage nach der Geschichte her. Eine Schwierigkeit solcher Beschreibungen besteht darin, zeitgleiche Entwicklungen nur sequentiell besprechen zu können. Daraus ergeben sich Irritationen. Abhilfe kann man schaffen, indem man die Bausteine des Textes als Mosaik versteht und zusammensetzt, um sich ein Bild zu machen.

Wenn man über die Geschichte digitaler Signaturen schreiben will, steht man vor einem Dilemma der Art, wie es häufiger auftritt, wenn die Technik in die Lebenswirklichkeit eingreift. Gewohnte Kategorien werden ``unscharf'', Begriffe bekommen neue Namen und bekannte Namen neue Bedeutungen. Und wo die Geschichte anfängt und wo sie hinführt ... ? So ist es auch im Falle digitaler Signaturen.

Da gibt es auf der einen Seite die Unterschrift -vornehm: *Signatur*-, die man schon als Schulkind übt und die einen lebenslang als Resultat persönlichen Handelns begleitet. Jetzt soll diese zuerst ergänzt, später vielleicht ersetzt werden durch die sogenannte digitale Unterschrift -technisch: d*igitale Signatur*-; ein Begriff, unter dem sich wohl nur wenige etwas vorstellen können. Das ist die andere, abstrakte Seite der Münze. Ist die Geschichte der einen auch die der anderen? Irgendwie schon und andererseits auch nicht. Das ist das Dilemma.

Digitale Signaturen haben eine relativ kurze Geschichte; Unterschriften eine lange. Digitale Signaturen haben etwas mit dem Computer zu tun; die gibt es noch nicht so lange und suspekt sind sie sowieso. Unterschriften sind Handarbeit und schon uralt. Und: Wer vertraut schon einem Computer? Einer Unterschrift vertraut dagegen eigentlich jeder. Zu Recht?

Eine kurze Geschichte der Unterschrift

zitat

> *``Die Unterschrift ist grundsätzlich mit dem Familiennamen zu leisten. ... Sie muß individuelle Züge tragen, nicht aber unbedingt lesbar sein. ... Sie muß ferner eigenhändig vollzogen werden; ... Die Unterschrift muß - ihrem Wortlaut gemäß - regelmäßig unter das Schriftstück gesetzt werden, d.h. dessen Inhalt decken ... Eine "Oberschrift" ... genügt regelmäßig nicht ..."* [Creifelds]

[**Hinweis:** Es gibt leider kein deutschsprachiges Buch, das einen Titel wie ``Geschichte der Unterschrift'' trägt. Man findet hier und da in der wissenschaftlichen Literatur einzelne Hinweise, die man unterschiedlich interpretieren kann. Diese Darstellung ist ein vorsichtiger Versuch der Zusammenfassung der mir bekannten Fakten.]

Im Wort `Signatur' steckt das alte `signum', das Zeichen. Unterzeichnen klingt zwar amtlicher, meint aber dasselbe wie unterschreiben. Signieren klingt schon nach einem Staatsakt. In allen Fällen geht es aber darum, ein Zeichen anzubringen, das als Beleg dient. Solche Zeichen sind in verschiedenen Formen als Siegel bereits aus alten Zeiten bekannt, in denen die Schrift noch einigen wenigen vorbehalten war.

[**Anmerkung:** Auch im alten China wurden Siegel, in Form von Stempeln, eigenständig entwickelt und verbreitet. Ich beschränke mich an dieser Stelle aber auf die europäische Kultur.]

Es hat sich sogar eine ``Hilfswissenschaft'' namens Sphragistik herausgebildet, die sich mit der rechtlichen Bedeutung der Siegel beschäftigt. [Microsoft LexiRom]

Die ersten siegelartigen Objekte finden sich bereits um 3200 v.u.Z., in Mesopotamien, der Wiege Europas. Es handelte sich um geschnitzte Knochen oder Steine, deren Abdrücke im Ton Muster hinterließen. Diese konnten Verzierungen, aber auch Markierungen darstellen. [Funk & Wagnalls]

Mit der Ausbreitung der Schrift wurden auch Siegel vermehrt eingesetzt. Ihre Gestaltung wurde mit größerem künstlerischen Anspruch vorgenommen. Neue Materialien, wie Metalle und Edelsteine, kamen zum Einsatz. In der griechischen und römischen Antike gipfelte diese Entwicklung in Siegelringen mit dem Abbild des Inhabers (Gemmen). [Funk & Wagnalls]

Die Römer handelten viel mit anderen Völkern, ihre Keramik war weltberühmt, begehrt und wurde bis nach Indien gebracht. An diesem Erfolg wollten viele teilhaben, der Handel florierte und mit ihm der Betrug. Und wer wollte in Asien unterscheiden, welche Vase aus Rom stammte und welche nicht?

Um solchem Betrug vorzubeugen, kamen die Römer auf die Idee, ihre Keramik mit einem Siegelabdruck zu markieren. Wie erfolgreich diese Methode war, ist nicht überliefert. Bezeichnet wird die Keramik diesen Typs als `*terra sigillata*' (Verbreitung: ca. 50 v.u.Z. bis 50), wobei unklar bleibt, ob sich das `*sigillata*' auf die Reliefverzierungen oder die Herstellersiegel bezieht. Jedenfalls handelt es sich um eine neuzeitliche Bezeichnung. [Neuburger 1919]

Solch ein Siegelabdruck enthielt üblicherweise den Namen des Fabrikbesitzers (von lat.: *fabricae*) und den des Arbeiters, stellte also eine Art individuelles Warenzeichen dar. [Antike 1982]

Die Antike ging vorüber, das Mittelalter kam und mit ihm die Vorherrschaft der katholischen Kirche. Die Siegel wurden kaum noch zu Handwerkszwecken eingesetzt. Die Römer hatten der Welt ein umfangreiches Justizwesen hinterlassen, in dem Verträge eine dominierende Rolle spielen. Um dieser Bedeutung auch formell Ausdruck zu verleihen, wurden unter wichtigen Verträgen die Siegel der Vertragspartner angebracht. Dies war sowohl auf weltlichem, als auch auf geistlichem Gebiet etabliert. [Funk & Wagnalls]

Auch in der Kirche als (Auf-)Bewahrer der antiken Schriften spielten Siegel eine wichtige Rolle. Abschriften von Originalen wurden mit einem Siegel beglaubigt. Diese Abschriften bekamen den Namen `*Authentik*'. [Microsoft LexiRom]

Die Handwerker verzichteten ihrerseits auch nicht darauf, ihre Werke zu markieren. Allerdings war es den angeseheneren Handwerkern -z.B. Meister und Gesellen der Steinmetze- vorbehalten, Markierungen an Werkstücken anzubringen. Aus dem hohen und späten Mittelalter sind viele solche Zeichen an Kirchenbauten überliefert. Es handelt sich bei diesen um handgefertigte Markierungen. Deren genauer Zweck ist umstritten. Zum einen werden sie als `persönliche Zeichen' interpretiert, zum anderen als Hinweise für den Zusammenbau der Teile. Sie lassen sich verstärkt ab dem 13. Jahrhundert nachweisen, aber auch aus der Spätantike sind Zeichen überliefert (z.B. in der Kirche von Ravenna), so daßeine gewisse Tradition in der Antike vermutet werden kann. [Conrad/Mertens 1990]

Die Grafik stellt einige Steinmetzzeichen dar. Ein individueller Charakter ist deutlich erkennbar.

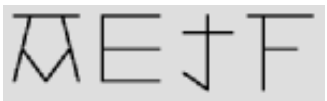


Abb.: Steinmetzzeichen nach *G. Binding*: ``Baubetrieb im Mittelalter'' [Binding 1993]

Ab wann Daumenabdrücke zum Unterzeichnen zum Einsatz kamen, läßt sich nicht feststellen. Man kann aber annehmen, daßes nicht vor der Erfindung der formellen Verträge, also zu römischen Zeiten, geschah. Später kamen die berühmten `drei Kreuze' hinzu, zu denen jeder fähig war, auch wenn er nicht schreiben konnte.

Mit der Ausbreitung des Schrifttums und der Bürgerrechte trat an die Stelle des Siegels die persönliche, eigenhändige Unterschrift. Funk &Wagnalls New Encyclopedia [Funk & Wagnalls]gibt das Jahr 1536 für das Auftauchen der Wortes `*signature*' an. (*Zur Einordnung:* Johannes Gutenberg druckte seine Bibel um 1450.) Das Wort `*signify*', aus dem sich das `*sign*' für `*unterschreiben*' entwickelt hat, weist Webster's Dictionary als aus dem 13. Jahrhundert stammend aus [Webster's].

Das Erstarken des Bürgertums in der Renaissance und die Ausbreitung der Schrift in größeren Teilen der Bevölkerung beförderte diese Entwicklung sicherlich. Nach [Menezes/Oorschot/Vanstone 1997]wurde die verbindliche Unterschrift ins englische Rechtssystem im 17. Jahrhundert eingeführt. Siegel kamen mehr und mehr aus der Mode, ganz verschwunden sind sie aber bis heute nicht. Insbesondere zu Staatsakten und in der Verwaltung (Amtssiegel, Stempel) werden sie immer wieder gerne eingesetzt.

Wir sehen, in gewisser Weise haben Siegel, Stempel, Handelsmarke und Unterschrift einen gemeinsamen Ursprung. Sie alle haben etwas mit individuellen Zusicherungen verschiedenster Art zu tun: *Herkunft, Stand, Identität, Authentizität, Exklusivität, Verbindlichkeit*. Mit der Etablierung der Unterschrift im Recht wurde dem formal Rechnung getragen.

Zusammenfassung

Siegel und Stempel waren die Vorläufer der Unterschrift. Sie sind seit Jahrtausenden im Gebrauch. Ein wichtiger Grund für ihren Gebrauch war der Beleg der Authentizität. Unterschriften entstanden, als sich das Schrifttum in größeren Teilen der Bevölkerung ausbreitete und das Bewußtsein der eigenen Individualität zunahm.

Geschichte digitaler Signaturen

zitat

> ``*... the essential direction for the future development of what is still called `Public-Key-Cryptography' ist rather that of preserving trust than that of preserving secrecy, only!*'' [Beth/Frisch/Simmons 1991]

Am Ende der Entwicklung zur Unterschrift standen einige Eigenschaften fest, die digitale Signaturen auch werden aufweisen müssen, sollen sie eine vergleichbare Qualität haben und Akzeptanz finden. Dazu gehören *Individualität, Falsifizierbarkeit, Handhabbarkeit, Unabweisbarkeit*und *Vertrauen in sie*. Diese Merkmale bildeten sich durch Gebrauch heraus und haben sich im Alltag bewährt.

Doch das ist das Ergebnis. Wie kam es dazu? Wir vollziehen jetzt einen Schritt aus der kontinuierlichen, analogen Welt des menschlichen Handelns in die diskrete, digitale Welt der Computer.

[**Anmerkung:** Über die Geschichte digitaler Signaturen wird in der Fachliteratur nicht viel gesagt. Oft lassen die Autoren sie ganz aus der Betrachtung heraus, manchmal kommt sie vor, beginnt aber erst in den 70'er Jahren (z.B.: [Pfitzmann 1996]). Ich versuche, bei den Ahnen anzufangen.]

Geschichte digitaler Signaturen

Computer und Techniker

zitat

``*Historically, computer security is related to both cryptography and access control in operating systems.*" [Pieprzyk/Sadeghiyan 1993]

In der Welt der Computer wird mit Daten operiert. Da nichts perfekt ist, auch ein Computer nicht, treten in dieser Welt Fehler auf. Als ein Mittel zur Erkennung von Fehlern in Daten wurden Prüfsummen(`computerdeutsch': Checksummen) eingeführt: Eine gewisse Menge an Daten wird mit einer Markierung versehen, die mittels einer (mathematischen) Vorschrift bestimmt wird. Nach dem Datentransport, respektive dem Wiedereinlesen nach der Speicherung, wird dasselbe Verfahren wieder angewandt und das Resultat mit der Markierung verglichen. Ergibt sich dabei keine Differenz, geht man davon aus, daßdie Daten unverändert sind. Die Markierung, als redundante Information, belegt dabei weniger Speicherplatz bzw. Bandbreite, als die Daten selbst.

Je weiter man zu den Anfängen der Computer zurückgeht, desto teurer war der Speicher. Die ersten Verfahren für Prüfsummen waren simpel, d.h. der Aufwand, sie zu berechnen, war aus heutiger Sicht gering; ihr Speicherbedarf war niedrig. Ihre Trefferquote war allerdings auch nicht sehr hoch. So gab es Verfahren, die Fehler immer nur im zweiten Bit anzeigten, d.h., mit einer Wahrscheinlichkeit von höchstens 50% wurde eine auftretende Abweichung festgestellt.

Im Widerstreit mit den Speicherbeschränkungen befanden sich die Sicherheitsanforderungen. Bei wirklich wichtigen Daten ist es nicht hinnehmbar, daßsie überhaupt verändert werden. Man stelle sich vor, ein Parameter in der Steuerung eines Kernkraftwerkes wechselt unbemerkt seinen Wert von 1 auf 0 ... Um die Daten wirklich zu sichern, müßte man immer mindestens eine Kopie vorrätig halten und ständig mit dem Original vergleichen. Das würde dann doppelt soviel Speicher verschlingen, und der war damals zu teuer. Auch wäre der Aufwand des Vergleichens oft zu hoch gewesen. Dies galt nicht für alle Informationen, aber für die meisten.

Ausgefeilte Prüsummenverfahren erlauben heute die Integration von sogenannten `error correcting codes' (ECC) direkt in die Speicherhardware. Fehler im Bereich einzelner Bits werden mittels ECC sofort korrigiert. Der Aufwand dafür ist natürlich höher als bei einem Verzicht auf eine automatische Korrektur. Das wirkt sich auf den Preis und das Kaufverhalten aus: Speicher mit ECC belegt nur einen sehr geringen Marktanteil.

Zur gleichen Zeit wurde an einem anderen, wichtigen Problem der Informatik gearbeitet, dem schnellen Sortieren und Suchen in großen Datenmengen. Dafür wurden Hashverfahren erfunden. Sie wurden bereits früh im Compilerbau und bei Datenbanken eingesetzt, um einerseits Speicher zu sparen und andererseits eine hohe Zugriffsgeschwindigkeit zu erreichen.

Die Einweg-Eigenschaft von Funktionen wurde 1977 von L. Berman erstmals definiert. [Kurtz/Mahaney/Royer 1988] Eine Weiterentwicklung der Hashfuntionen unter dem Aspekt der Einweg-Eigenschaft führte zu den kryptographischen Hashfunkionen, auch Einweg-Hashfunktionen genannt, die wiederum gut als Checksummenfunktionen einzusetzen sind.

Zusammenfassung

In den 50'er und 60'er Jahren wurde von den Technikern (Informatikern) an der Entwicklung von Verfahren gearbeitet, welche bei geringem Speicherbedarf die Integrität der Daten sicherstellen sollten, die mit dem Computer verarbeitet werden: Checksummen. Ebenfalls wurden Hashverfahren, die einen effizienten Zugriff auf Daten bei gleichzeitig geringem Speicherbedarf gestatten, entwickelt.

Geschichte digitaler Signaturen

Militär, Geheimdienste und Verschlüsselung

zitat

> ``*Within Europe all email telephone and fax communications are routinely intercepted by the United States National Security Agency transfering all target information from the European mainland via the strategic hub of London then by satellite to Fort Meade in Maryland via the crucial hub at Menwith Hill in the North York moors in the UK.*" [Electronic Telegraph 16.12.1997]

Parallel zur Entwicklung der Computer wurde auf dem Gebiet der Kryptologie geforscht. Deren Bedeutung war im zweiten Weltkrieg, der in den 50'er Jahren noch nicht allzu lange zurücklag, deutlich aufgewertet worden [Kippenhahn 1997]. [1] Die Verschlüsselung der deutschen Kommunikation mit der Enigmahatte den Alliierten erhebliche Kopfschmerzen bereitet. [2]Und auch im kalten Krieg war Kryptologie gut zu gebrauchen. Auf beiden Seiten des `*iron curtain*' (*Churchill*) arbeiteten Spione (alias Agenten, Aufklärer, ...) daran, strategische Informationen zu erlangen und diese sicher an ihre Auftraggeber weiterzuleiten. Die Verschlüsselung der Informationen spielte dabei eine entscheidende Rolle.

Die Forschungen im Bereich der Kryptologie fanden über zwanzig Jahre hinweg nahezu ausschließlich in den Geheimlabors der Militärs und Geheimdienste statt. Die Resultate blieben bis auf Ausnahmen geheim. In den USA wurde z. B. 1952 die NSA gegründet, die sich in der Hauptsache mit Ver- und Entschlüsselung beschäftigt und zu diesem Zwecke zig-Tausende Mathematiker im Dienst hat. Ziel der NSA-Aktivitäten war und ist einerseits die strategische Aufklärung der Kommunikation von Feinden und Freunden (siehe Zitat) und andererseits die Unterbindung vergleichbarer Vorhaben durch jene.

Als die Geheimdienste die Computer für sich entdeckten, oder andersherum: als die Computer für die Zwecke der Geheimdienstler interessant wurden, wurden die Erkenntnisse zu Checksummen und Hashverfahren, wie auch zur Verschlüsselung zusammengeführt. Wie fruchtbar diese Begegnung wirklich war, kann nur gemutmaßt werden, da Geheimdienstler meist verschwiegene Leute sind. *David Kahn* hat Teile davon rekonstruiert ([Kahn 1967]). Als *Diffie* und *Hellman* ihren Artikel (s.u.) veröffentlichten, monierte der Direktor der NSA, daß dort die Kryptographie mit

unterschiedlichen Schlüsseln bereits zwei Jahrzehnte zuvor entwickelt worden wäre. Das blieb aber unbewiesen ([Schneier 1996], S. 38).

Zusammenfassung

Mathematiker und Linguisten arbeiteten im Auftrag der Geheimdienste seit den 50'er Jahren verstärkt an Verfahren zur Geheimhaltung von Informationen und an Verfahren zur Gewinnung von Informationen aus verschlüsselten Daten. Die klassische (symmetrische) Verschlüsselung erlebte ihre Blütezeit.

Geschichte digitaler Signaturen

Privacy & Authentication

zitat

> ``*Regierungen haben eine Menge Geheimnisse vor ihrem Volk. ... Warum darf das Volk im Gegenzug keine Geheimnisse vor der Regierung haben?''* Philip Zimmermann, Entwickler von PGP, zitiert in [Kippenhahn 1997], S. 250

Relativ unabhängig -jedoch nicht unbehindert [3] - von der geheimdienstlichen und militärischen Forschung auf kryptologischem Gebiet hatte sich eine um Größenordnungen weniger umfangreiche akademische Forschung entwickelt. Auch in der Wirtschaft war mit dem Computereinsatz das Interesse an `*privacy and authentication*' (*Diffie* und *Hellman*) gewachsen, und die entsprechenden Anstrengungen wurden verstärkt.

Insbesondere der zunehmende internationale Austausch von Waren und Dienstleistungen machte eine sichere Informationsweitergabe unumgänglich. In unserer Zeit übersteigt die Menge an monetären Transaktionen in ihrem Wert den des Warenaustausches um das Fünfzigfache. Dieser Verkehr wird in irgendeiner Form über elektronische Kommunikationsnetzwerke abgewickelt. Ohne Authentifizierung und Schutz vor Manipulation wäre das nicht denkbar.

Erste Arbeiten zu manipulationsgeschützten Codes wurden (nach [Pfitzmann 1996], S.12) von *E. N. Gilbert*, *F. J. Mac Williams* und *N. J. A. Sloane* veröffentlicht (Codes which detect deception; The Bell System Technical Journal 53/3, 1974). Es verging noch einige Zeit, bis jemand die entscheidende Idee hatte: 1976 veröffentlichten *Whitfield Diffie* und *Martin Hellman* einen Artikel, der den Grundgedanken für die `*public key cryptography*' enthielt: New Directions in Cryptography [Diffie/Hellman 1976].

Kerngedanke war, daß man mit zwei unterschiedlichen Schlüsseln arbeitet, wobei ein Schlüssel nur für die Verschlüsselung und der andere nur für die Entschlüsselung verwendbar ist (*Sinnbildlich: Ein Schlüssel kann das Schloß verschließen, aber nicht aufschließen. Mit dem anderen Schlüssel kann man wiederum nur aufschließen, nicht jedoch abschließen.*). Dazu muß man dem Gegenspieler, dem fiktiven kryptologischen Angreifer (attacker), eine an sich unlösbare Aufgabe stellen. Für Freunde aber baut man eine Hintertür (trapdoor) ein, durch welche die

Lösung leicht zu bestimmen ist. Konkret heißt das: Die Verschlüsselung mit dem einen Schlüssel stellt den Angreifer vor das Problem, daß der Aufwand für das Brechen der Verschlüsselung in der Praxis dessen Möglichkeiten übersteigt. Dagegen kann ein Partner, der über den anderen Schlüssel verfügt eine Entschlüsselung vornehmen.

Bei *Diffie* und *Hellman* handelte es sich um theoretische Überlegungen, die erstmals von *Ronald Rivest*, *Adi Shamir* und *Leonard Aldleman* praktisch umgesetzt wurden: 1978 (1977) stellten sie das nach ihnen benannte RSA-Verfahren vor und ließen es sogleich patentieren.

Kombiniert man geeignete Hashfunktionen, sogenannte kryptographische Einweg-Hashfunktionen, mit Public Key-Verfahren und einer Schlüsselverwaltung in bestimmter Art und Weise, so erhält man digitale Signaturen, auch als digitale Unterschriften bezeichnet.

> Genauere Beschreibungen finden sich im Kapitel ``Grundlagen''.

Die erste Implementierung eines Verfahrens für digitale Signaturen wurde (nach [Pfitzmann 1996], S. 19) von *Leslie Lamport* vorgenommen (1979). Der Vorschlag, auf dem die Implementierung basierte, stammte bereits aus dem Jahre 1974, von *Roger Needham*. Der größte Nachteil des Ansatzes von *Lamport* war die Schlüssellänge, die so groß war, daß eine effiziente Verwaltung nicht möglich war. Später wurden praktikable Verfahren entwickelt.

> *F. Damm* hat in [Damm 1995] Übersichten über die wichtigsten kryptographischen Hashfunktionen und praktikablen elektronischen Unterschriftenverfahren erarbeitet, die ich graphisch aufbereitet habe.

Der Vollständigkeit halber soll an dieser Stelle daraufhingewiesen werden, daß *Diffie* und *Hellman* nicht die ersten waren, die sich mit `*public key cryptography*' beschäftigt haben, wenn auch ihre Ideen die maßgeblichen waren. Nimmt man die Zeitangaben aus der Fachliteratur, so steht *Ralph Merkle* die Ehre zu. 1974 entwickelt er im Rahmen einer Seminararbeit an der Universität Berkeley (Kalifornien) das `*knapsack*'-Problem ([Schneier 1996], S. 40). An anderer Stelle ([Menezes/Oorschot/Vanstone 1997], S. 300) werden *Merkle* und *Hellman* als Verursacher genannt. Auch die Zeitangaben differieren. Bei [Damm 1995] findet sich für das `*knapsack*'-Problem 1978 als Entstehungszeitpunkt (S. 40). Der `*knapsack*'-Ansatz wird von den meisten Autoren jedoch abgelehnt bzw. nicht empfohlen und hat praktisch keine Bedeutung.

Den modernsten Ansatz für digitale Signaturen haben Birgit Pfitzmann und Michael Waidner entwickelt und 1990 bzw. 1991 [4] vorgestellt. Sie verfolgen mit ihren Failstop-Signaturen die Idee, die Fälschung einer digitalen Signatur nachweislich zu machen und Folgefälschungen zu unterbinden, sobald eine Fälschung festgestellt wurde. Voraussetzungen für das Funktionieren sind die Geheimhaltung des privaten Schlüssels und die Gültigkeit der kryptologischen Annahme (cryptological assumption).

Zusammenfassung

In den 70'er Jahren wurden in der zivilen kryptologischen Forschung große Fortschritte gemacht, insbesondere wurde die asymmterische Verschlüsselung (*public key cryptography*) entwickelt. Durch eine Kombination mit kryptographischen Hashfunktionen erhält man Verfahren für digitale Signaturen. Die Sicherheit von der

modernen Fail-stop-Signaturen ist höher als die einfacher, herkömmlicher digitaler Signaturen.

Geschichte digitaler Signaturen

Das Gesetz zur digitalen Signatur

zitat

``Der Trend ist eindeutig: die Informationsgesellschaft wird es nur in Abhängigkeit vom sicheren und beherrschbaren Funktionieren "digitaler Signaturen" geben. Gemessen am Stand der aktuellen Debatte wird ein gerichtsverwertbarer, also rechtsverbindlicher Geschäftsverkehr - ein zentraler Baustein einer multimedialen Dienstleistungsgesellschaft - nicht ohne digitale Signaturen, dem modernsten Produkt kryptographischen Denkens, möglich sein." [Hartmann/Ulrich 1997]

Mit der Ausbreitung von Computernetzen, insbesondere des Internet, nehmen die Möglichkeiten zu ihrer geschäftlichen Nutzung zu. Geschäftsleute sind darauf angewiesen, daßihre Verträge eingehalten werden. Um sich abzusichern, lassen sie die Verträge normalerweise unterschreiben. Aus einem Stück Papier wird durch die Unterschrift eine Urkunde, die Beweiskraft hat. In Computernetzwerken gibt es jedoch kein Papier, was unterschrieben werden kann. Und ein digital signiertes, elektronisches Dokument ist nicht dasselbe wie ein unterschriebener Vertrag. Zumindest gilt dies in Bezug auf die Beweiskraft. Die vielen Formvorschriften im bürgerlichen Recht verlangen nun mal nach einem Stück Papier, wenn es um eine Urkunde geht.

Auf Drängen der Geschäftswelt wurden inzwischen weltweit einige Versuche unternommen, die digitale Signatur gesetzlich zu reglementieren, um ihr einen der eigenhändigen Unterschrift vergleichbaren Wert zu geben. Den Anfang machten die USA, wo 1995 in Utah der `Utah Digital Signature Act' (UDSA) verabschiedet wurde. Es folgten andere Bundesstaaten, wie z.B. Georgia und Kalifornien.

Auch der deutsche Gesetzgeber bemerkte die Notwendigkeit einer rechtlichen Absicherung digitaler Signaturen und reagierte. 1997 trat im Rahmen des sogenannten Multimediagesetzes (IuKDG) das Gesetz zur digitalen Signatur, kurz SigG, in Kraft. Damit sieht sich die Bundesregierung international in einer Vorreiterrolle.

Der Wert des Gesetzes ist umstritten. Einerseits wurde begrüßt, daß das Gesetz überhaupt geschaffen wurde. Auf der anderen Seite wurde seine Ausgestaltung stark kritisiert. Den Hauptangriffspunkt stellen dabei die unklaren Verantwortlichkeiten und fehlende Haftungsregelungen dar. Auch werden die in einer ergänzenden Verordnung vorgeschriebenen technischen Anforderungen als ernstes Hindernis für den breiten Einsatz der digitalen Signaturen angesehen. Die von einer Allianz aus Politikern, Geheimdienstlern und Beamten der Innenministerien von Bund und Ländern angestrebte Reglementierung der Verschlüsselung trägt ihrerseits zur Verunsicherung über den Wert digitaler Signaturen bei.

Zusammenfassung

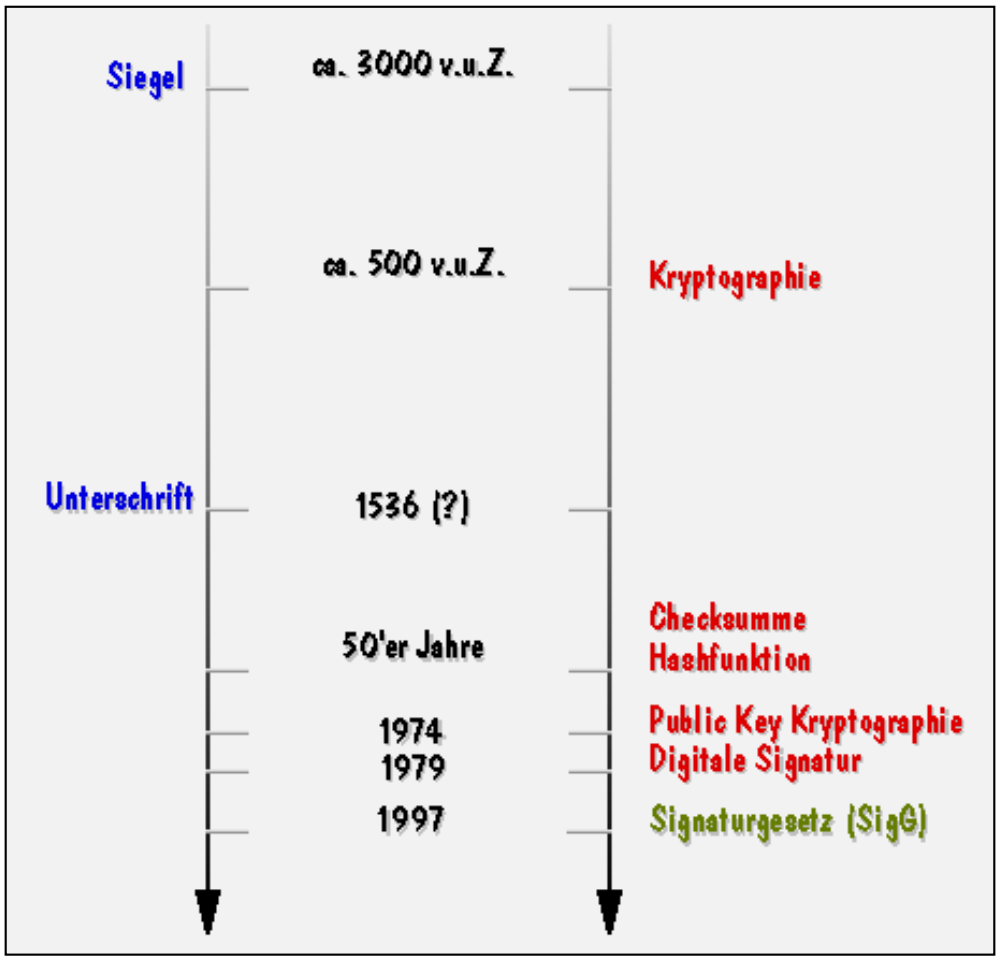
Zwanzig Jahre nach Entwicklung der technischen Verfahren wird die digitale Signatur der eigenhändigen Unterschrift rechtlich weitgehend gleichgestellt. Der praktische Wert der gesetzlichen Regelungen muß sich erst noch erweisen. Zumindest beinhalten die fehlenden bzw. unklaren Haftungsregelungen ein gewisses Risiko.

Zeittafel

zitat

> ``*Chronological Order with digital signature schemes, as with most other cryptologic subjects, means: Related to older work, someone has an informal idea, and people happily start to construct schemes.*" [Pfitzmann 1996], S.11

Den zeitlichen Ablauf der Ereignisse möchte ich zum Schlußnoch zusammenfassend in einer Grafik darstellen.



Fußnoten

[1] ``*Cryptography is intimately linked to war. In war, the forces of the nation must cooperate in order to function effectively, which requires exchange of information. At the same time this information needs to be kept hidden from the enemy.*''[Tedrick 1985]

---

[2]Die Bedeutung der Brechung der Enigma-Verschlüsselung in England (Projekt ULTRA) wird von manchen Fachleuten sehr hoch eingeschätzt:

> ``*ULTRA was indispensible during the battle of Britain, allowing the British to make optimal use of limited resources in fighting the Luftwaffe. Knowledge of enemy numbers, locations, and plans was of extreme importance.*'' [Tedrick 1985]
>
> ``*Summing up, in all theatres of war ULTRA had the most serious consequences for the German war effort. Without ULTRA Rommel should have overrun the British in North Africa and been able to carry out his plan for moving into southern Russia, the Allies should not have been able to invade Nort Africa or Europe, and the war on the Eastern front should have been at least stalemate. When Atomic weapons came into play the most uncertain consequences coul be expected.*''[Tedrick 1985]

---

[3]Siehe z.B.: *W. Diffie*im Vorwort zu [Schneier 1996]:

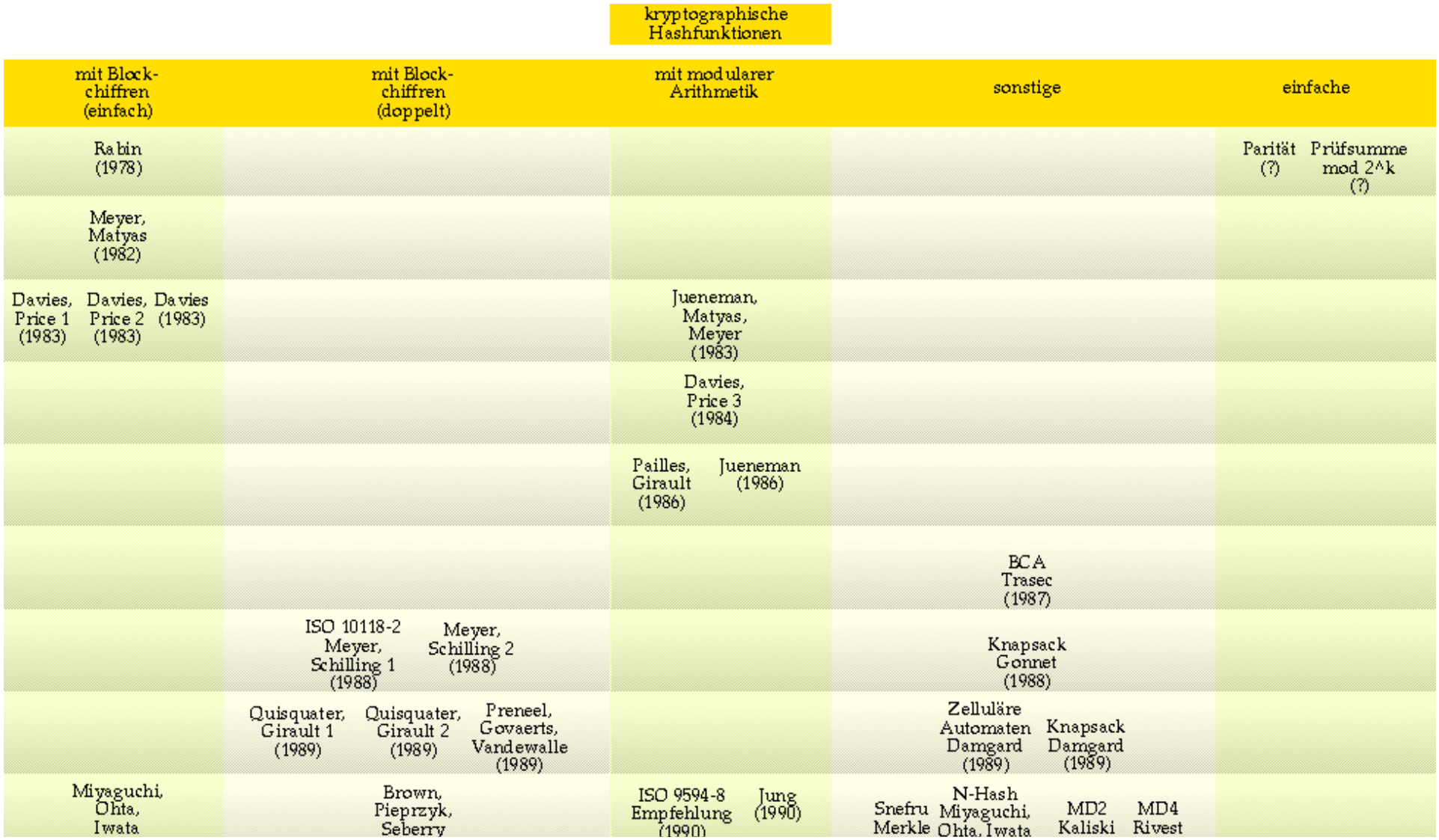
> ``*Als das öffentliche Interesse an der Kryptographie in den späten siebziger und frühen achtziger Jahren zu erwachen begann, unternahm die National Security Agency (NSA), das offizielle kryptographische Organ Amerikas mehrere Versuche, es wieder zu unterdrücken. Der erste Versuch bestand in einem Brief eines langjährigen und angeblich eigenmächtig handelnden NSA-Angestellten an die IEEE. Er wies in seinem Brief darauf hin, daß die Veröffentlichung kryptographischen Materials einen Verstoß gegen das internationale Waffenkontrollgesetz (International Traffic in Arms Regulations, ITAR) darstelle. Es stellte sich jedoch heraus, daß diese Auslegung der Vorschriften nicht korrekt war, denn diese sahen für veröffentlichtes Material ausdrücklich eine Befreiung vor.*''
>
> ``*1980 gab es einen schwerwiegenden Versuch, als die NSA das American Council on Education ins Leben rief. Dahinter steckte die Absicht, den Kongreß davon zu überzeugen, der NSA die juristische Kontrolle der Publikationen auf dem Gebiet der Kryptographie zu übertragen.*''
>
> usw. usf.

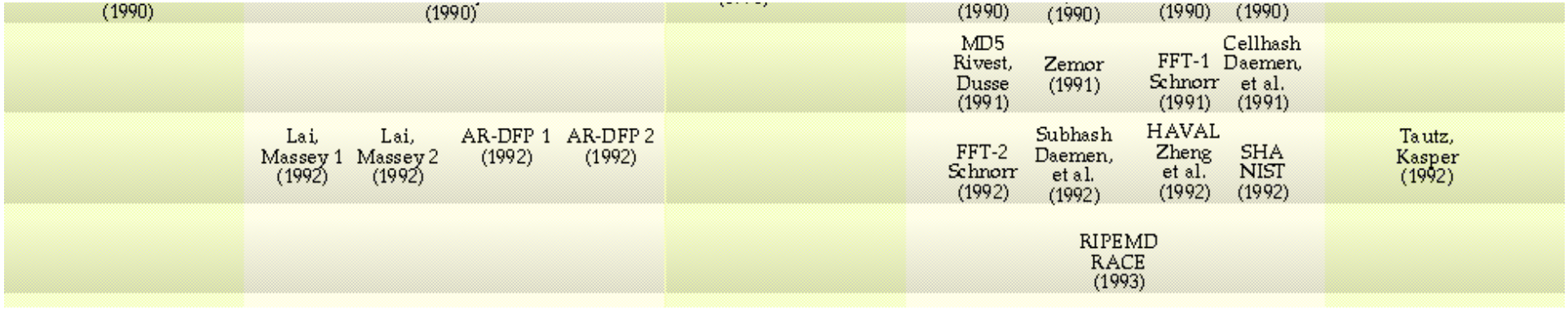
---

[4]*Birgit Pfitzmann,Michael Waidner*: **Fail-stop signatures and their applications.**Proceedings of the 9th worldwide Congress on Computer and Communications Security and Protection (SECURICOM'91), 1991

Birgit Pfitzmann, Michael Waidner: **Formal Aspects of Fail-Stop Signatures.** Report 22/90, Fakultät für Informatik, Universität Karlsruhe, 1990

Chronologie kryptographischer Hashfunktionen



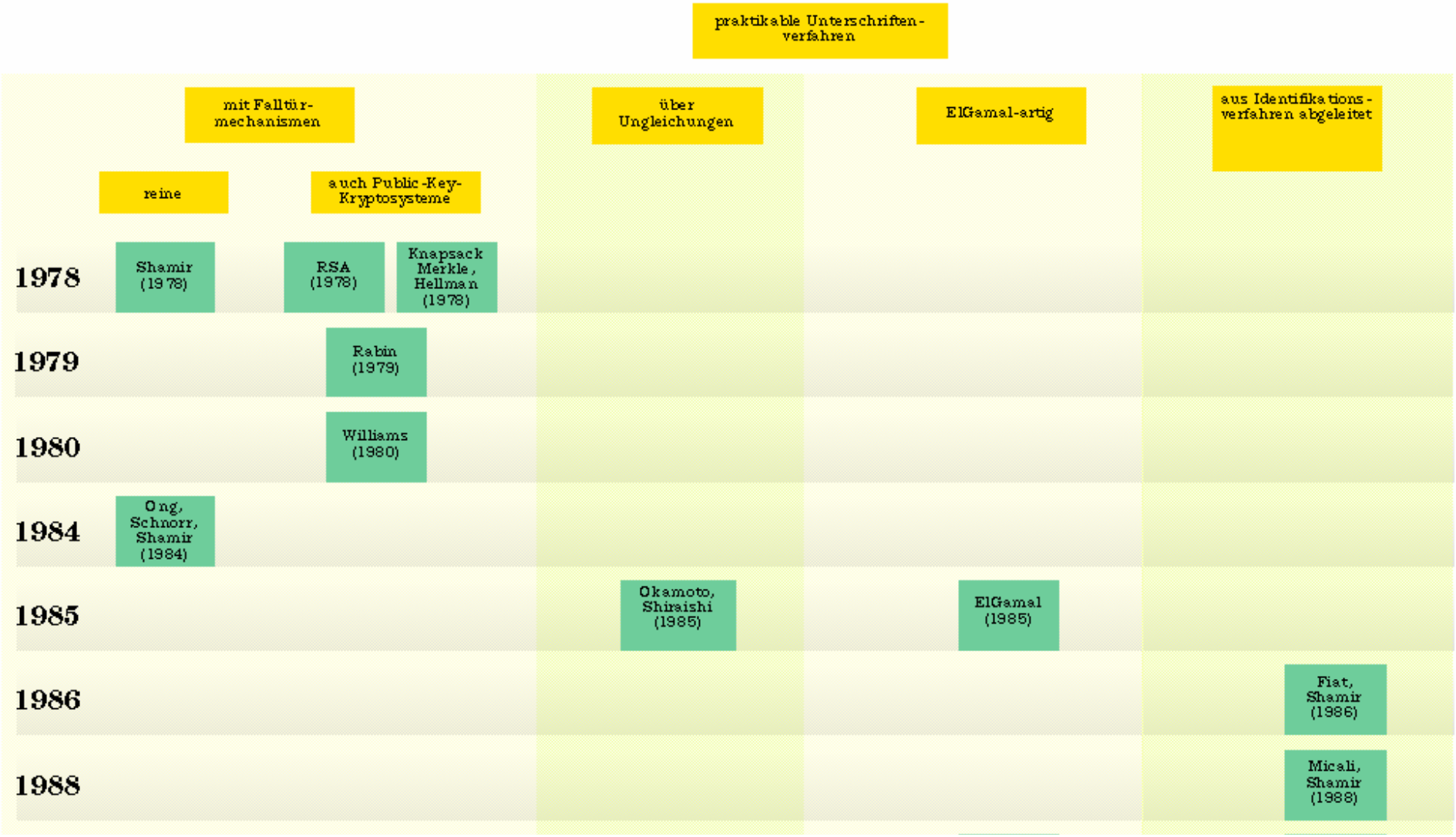


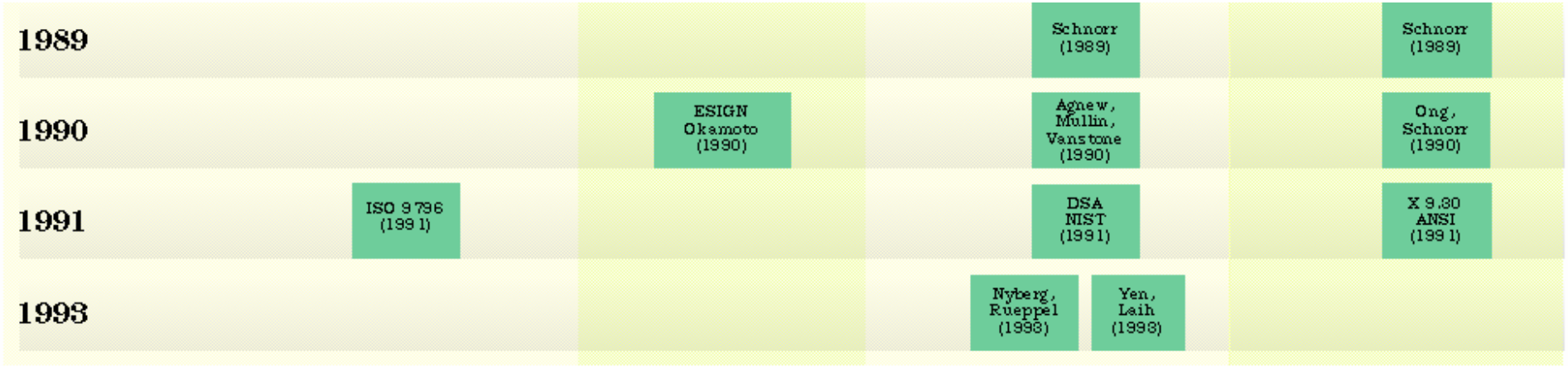
(nach [Damm 1995])

Eingangsseite Mail
digitale signaturen diplomarbeit · robert gehring

Geschichte digitale signaturen
diplomarbeit · robert gehring

Chronologie praktikabler elektronischer Unterschriftenverfahren





(nach [Damm 1995])

IEEE [*Institute of Electrical and Electronics Engineers*]

Institute of Electrical and Electronics Engineers (engl.) - Institut der Elektro- und Elektronikingenieure

Das IEEE(oft ausgesprochen als ``*I triple E*'') ist eine internationale Organisation, die 1963 gegründet wurde. Sie kümmert sich um die Entwicklung von Standards für Elektrik und Elektronik. Das deutsche Gegenstück ist der VDE.

Internet

http://www.ieee.org

VDE [Verband deutscher Elektroingenieure]

Verband deutscher Elektroingenieure - (engl.) Institute of German Electrical Engineers ???

Der VDEist das deutsche Gegenstück zur IEEEauf internationaler Ebene.

Internet

http://www.vde.de

ITAR [*International Traffic in Arms Regulations*]

International Traffic in Arms Regulations (engl.) - Internationales Waffenhandelskontrollgesetz

Das ITARist -nicht nur für Kryptologen- insofern interessant, als es in Abschnitt 121.1 folgende Festlegungen enthält:

``Sec.121.1-General. The United States Munitions List.

(a) The following articles, services and related technical data are designated as defense articles and defense services pursuant to sections 38 and 47(7) of the Arms Export Control Act ...
Category XIII Auxiliary Military Equipment. ...

(b) Information Security Systems and Equipment, cryptographic devices, software, and componentes specifically designed or modified therefor, including:

*(1) Cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information or information systems, ... "*ITAR, zitiert in [CRISIS 1996]


Vorwort
digitale signaturen
diplomarbeit · robert gehring


Eingangsseite
Mail
digitale signaturen
diplomarbeit · robert gehring