Hauptseminar
SS 01

Elektronische Zahlungssysteme

Kryptographie

Daniel Würstle

Inhaltsverzeichnis

Allgemeines

Was ist Kryptographie?

Kryptographie ist ein Teil der *Kryptologi*e, der Wissenschaft der Geheimschriften und ihrer unbefugten Entzifferung. Sie ist der Teil jener Wissenschaft, der sich mit Absicherung von Nachrichten beschäftigt.

Das Gegenstück ist die *Krytoanalyse*. Sie beschäftigt sich damit, die geheimen Inhalte der Nachrichten lesbar zu machen.

Die unverschlüsselte Nachricht wird als *Klartext* bezeichnet, während die verschlüsselte Variante als *Chiffretext* bezeichnet wird.

Historie

Die Kryptologie ist eine Jahrtausende alte Wissenschaft. Sie entstand in den Anfängen parallel zu allgemeinen Schrift. Später stand ihre Entwicklung sehr stark im Zusammenhang mit jener der Mathematik. Im Folgenden werden einige Echpunkte der Entwicklung genannt. Im Internet gibt es Seiten, die ausführlich auf diese eingeht.

Die Anfänge der Kryptograohie gehen bis zu den Ägyptern 5000 v.Chr. zurück. Sie verwendeten zur Verschleierung Nichtstandard-Hieroglyphen. Damals konnten nur die Elite lesen und somit musste der Text auch nicht vor vielen geheim gehalten werden.

Der berühmteste historische Code ist der Cäsar-Code. Er bestand darin jeden Buchstaben um den zu ersetzten, der um drei weiter links im Alphabet steht.

Beim Nomenklatur-Code wurde seit 1380 Buchstaben durch zahlen ersetzt, sogar häufige Wörter und Satzteile. Dieser Code wurde sehr lange verwendet. Um 1700 hatte die Nomenklatur 2000 bis 3000 einträge.

In dieser Zeit wurden technische Hilfsmittel wie die Porta-Scheibe (1568) oder der Cryptograph von Wheatstone (1866).

Währender des zweiten Weltkrieges wurden auch Maschinen eingesetzt, die automatisch aus Klartext den Chiffretext machte und auch umgekehrt den empfangenen Chiffretext, direkt nach der Eingabe in die Maschine, in Klartext wandelte. Die bekannteste dieser Rotor-Maschinen, da der Schlüssel mit Walzen, die auch rotierten, einzustellen war, war die deutsche ENIGMA. Der Deutsche Arthur Scherbius meldete 1918 sein erstes Patent auf die ENIGMA an.

Mit der Entwicklung der Computer sind immer kompliziertere Algorithmen entwickelt worden, von denen nachher auf die wichtigsten eingegangen wird.

Anwendungsgebiete

Aus der Historie kann man erkennen, dass die Geheimhaltung von prissanten Dokumenten schon ein Thema war, seit die Schrift erfunden wurde. Da zu jener Zeit nur hohe Adlige, Priester oder Militärs richtig lesen konnten, musste die „Verschlüsselung“ nicht sehr stark sein. Diese Verschlüsselung war eher eine Verschleierung.

So kann man sagen, dass wohl die klassischen Gebiete, auf denen die Kryptographie eingesetzt wurden, diejenigen waren in denen Wissen ein Vorsprung bedeutete. Da sind vor allem die Diplomatie und das Militär zu nennen. Natürlich waren die Geheimdienste, vor allem in Kriegszeiten, immer aktiv.

Heute haben auch andere Institutionen wie Telekommunikationsunternehmen, Banken, etc. erkannt, dass bei Kommunikation über offene, unsichere Kanäle die Informationen vor unerlaubten Zugriffen und Missbrauch geschützt werden müssen.

Auch Privatpersonen haben heutzutage erkannt, dass die heutigen Kommunikationsmittel keinesfalls sicher sind. Vor allem beim Benutzen des Internets und von Computern ist. Computer sind aus unserer Gesellschaft kaum noch wegzudenken, denn sie überall eingesetzt, z.B. beim Verarbeiten unsere Banktransaktionen bis hin zum Schreiben privater Briefe und Dokumente. Aus diesem grund ist wohl der Computer, wenn auf ihm die Daten nicht richtig von fremden Missbrauch geschützt wird, eines der größten Sicherheitslöcher unserer Zeit und verlangt einen sensiblen Umgang.

Anforderungen an Kryptographie

Wenn man in der Kryptographie ein System betrachten, dann werden besondere Kriterien, welche in der Kryptologie eine wichtige Rolle spielen, zu dessen Beurteilung herangezogen. Dies sind im Wesentlichen vier Hauptkriterien.

Geheimhaltung
Der Klartext einer verschlüsselten Nachricht soll nur autorisierten Personen zugänglich sein.

Authentifizierung
Der Ersteller eines Verschlüsselten Dokuments soll von dem Empfänger zu ermitteln sein. Personen sollen sich nicht als jemanden anders ausgeben können

Integrität
Dem Empfänger soll es möglich sein, eine Nachricht zu überprüfen, ob sie von einem Eindringling gefälscht wurde, oder ob sie unverändert ist.

Verbindlichkeit
Dem Ersteller ein Nachricht soll zu einem späteren Zeitpunkt nicht leugnen können, dass er eine bestimmte Nachricht verfasst hat.

Ein Kryptosystem sicherer, je besser diese Kriterien berücksichtig wurden. Natürlich muss es einer Kryptonanalyse standhalten können, damit es nur mit

unwahrscheinlich hohem Zeit und Materialaufwand zu knacken ist. Aus diesem Grund werden alle modernen kryptographischen Systeme offengelegt und bewusst einer starken kryptongraphischen Analyse ausgesetzt, damit Schwachstellen erkannt und beseitigt werden. Da aber jeder das System kennt, ist die Geheimhaltung eines Textes nur noch von der Geheimhaltung des verwendeten Schlüssels abhängig.

Was ist dann ein perfekt sicheres Kryptosystem? Sicherlich nicht wenn es nur die vier Hauptkriterien erfüllt. Die perfekte Sicherheit ist dann gegeben, wenn die Wahrscheinlichkeit, dass ein bestimmter Schlüssel und ein bestimmter Klartext zu einem verschlüsselten Text auftritt, gleichverteilt über den gesamten Werteraum ist. Dies bedeutet, dass ein Angreifer, der die verschlüsselte Nachricht analysieren will, keinerlei Rückschlüsse auf Klartext oder verwendeten Schlüssel machen kann.

Wie gerade erwähnt, hängt die Sicherheit bei modernen kryptographischen Systemen davon ab, wie viele Leute einen Schlüssel kennen. Je mehr Leute einen Schlüssel haben, desto eher ist es Wahrscheinlich, dass er geklaut werden kann. Außerdem ist man nicht sicher in wieweit man den anderen vertrauen kann.

Wenn bei einem System der gleiche Schlüssel für Chiffrierung und Dechiffrierung verwendet wird, spricht man von Symmetrischer Verschlüsselung. Bei diesen Verfahren braucht jeder Teilnehmer den gleichen Schlüssel und man muss jedem Vertrauen, dass er sorgfältig mit dem Schüssel umgeht.

Einen Anderen Weg beschreiten die asymmetrischen Verschlüsselungen. Man hat einen öffentlichen Schlüssel mit dem jeder eine Nachricht an einen verschlüsseln kann, jedoch kann man diese verschlüsselten Nachrichten nur mit dem passenden privaten Schlüssel wieder lesbar machen.

Angriffe auf kryptograhische Systeme

Es gibt zwei Arten von Angriffen: technische und nicht-technische Angriffe. Die technische, benötigen immer technische Hilfsmittel.

Zu den nicht-technischen Angriffe gehört Bestechung, denn wenn ein Mitarbeiter die Informationen für Geld weitergibt, dann nützt auch die beste Verschlüsselung nichts. Ein Mitarbeiter kann auch aus Unzufriedenheit und Unmut gegenüber seinen Vorgesetzten, weil er sich schlecht behandelt fühlt oder entlassen wurde, Informationen sozusagen freiwillig, um seiner Firma eins auszuwischen, weitergeben.

Unachtsamkeit oder mangelnde Sensibilisierung der Mitarbeiter gegenüber der Geheimhaltung der Informationen kann ein Kryptosystem unwirksam machen. Da Mitarbeiter die Information achtlos auf den Arbeitsplätzen herumliegen lassen, kann ein Fremder (z.B. aus Putzkolonne) diese Dokumente einfach kopieren.

Bei höheren Mitarbeiter wäre es möglich, je wertvoller die Informationen sein können, dass dieser erpresst wird. Wenn der Mitarbeiter darauf eingeht ist es auch klar, dass die Geheimhaltung durch ein Kryptosystem nichts nutzt.

Bei technischen Angriffen handelt es sich um Angriffe, die in der Kryptoanalyse auch angewandt wird. Hier geht man davon aus, dass ein Angreifer Dokumente, meist durch Abhören der Kommunikationswege, in die Hände bekommt oder sich allgemein Zugang zum Kryptosystem verschafft. Nun versucht er durch Analyse der so erhaltenen Informationen einzelne Dokumente oder gar den Schlüssel zu knacken.

Beim Chippertext-Only Attacken kennt der Angreifer nur die chiffrierte Variante eines Textes und versucht nun Klartext oder Schlüssel zu ermitteln.

Wendet er einen Known-Plaintext Angriff an, so besitzt er zu irgend einer Nachricht sowohl Klar- als auch Chiffretext und versucht nun den dazugehörigen Schlüssel zu ermitteln.

Bei Chosen-Plaintext Attacken kann er sich selbst die Klartexte und dazugehörigen Chiffretexte aussuchen, indem er sich Zugang zum System verschafft, ohen den Schüssel zu kennen und selbst verschlüsseln kann. Nun versucht er den Schlüssel zu ermitteln oder andere Chiffretexte zu entschlüsseln.

Chosen-Chippertext Attacken werden dann angewandt, wenn der Angreifer selbst texte entschlüsseln kann ohne den Schlüssel zu kennen. Er sucht nun den verwendeten Schlüssel.

Wenn ein Angreifer alle möglichen Schlüssel ausprobiert bis einer passt, dann spricht man von einem „Brute Force“ Angriff.

Steganographie

Die Steganographie ist die Kunst eine Nachricht in einer anderen zu verstecken. Man möchte versuchen die bloße Existenz der geheimen Botschaft zu Verbergen. Die Trägernachricht in der die Botschaft versteckt ist nach Außen hin harmlos. Es ist eine Kunst des verschleierten Übermittelns von Botschaften.

Eine Art der Steganographie kann sein, dass man mit unsichtbarer Tinte schreibt oder die Nachricht in einem Bild versteckt. Beim Computer kann man z.B. das unterste Bit in den Bytes eines Bildes verwenden um eine Nachricht zu verstecken.

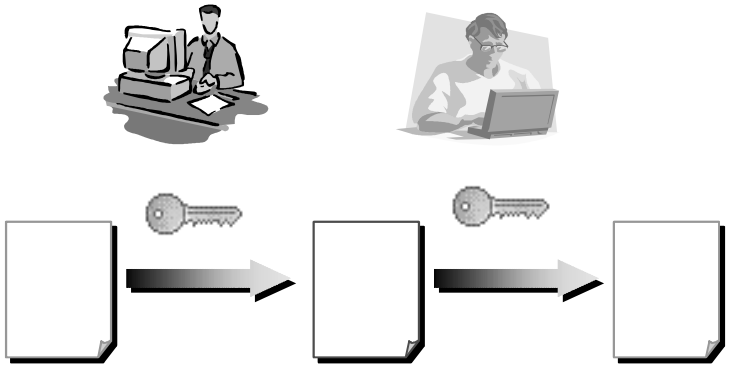
Bei Handschriften kann man bestimmte Buchstaben anders schreiben oder bei Schreibmaschinentext Buchstaben von Hand markieren. Dies kann mittels Strichen und Punkten geschehen oder mit kaum merklichen Vertiefungen.

Bei der Verschleierung sind der Fantasie kaum Grenzen gesetzt.

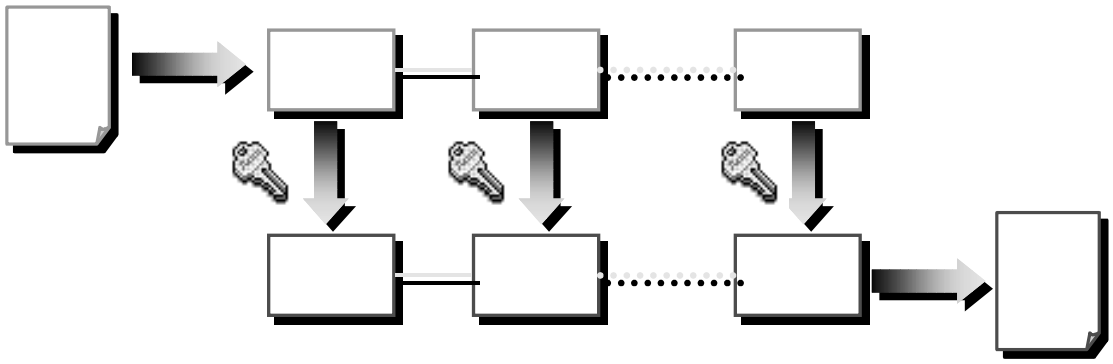
Symmetrische Verschlüsselung

Wenn symmetrische Verschlüsselung angewandt wird, so haben beide Kommunikationspartner den gleichen Schlüssel. Mit ihm wird der Klartext in Chiffretext umgewandelt, und danach auf der Gegenseite wieder zurück. Der

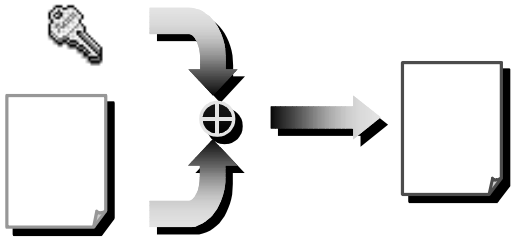
Schlüssel muss zwischen den Kommunikationsteilnehmern über einen gesonderten, sicheren Kanal den Schlüssel austauschen.



Blockchiffre sind die wichtigsten Verschlüsselungsverfahren. Zuerst wird der text in Blöcke fester Länge aufgeteilt (diese hängt vom Verfahren und Schlüssellänge ab). Diese werden dann nacheinander verschlüsselt. Es gibt viele Varianten der Blockchiffre, die sich in Berücksichtigung des Kontextes (als vorhergehender Blöcke) oder der Übertragungs- und Manipulationssicherheit unterscheiden.



Bei Stromchiffre wird ein kontinuierlicher Schlüsselstrom erzeugt. Dieser wird dann bitweise auf die Nachricht zu Verschlüsselung angewandt. Dieser Strom soll möglichst zufällig sein. Auf der Gegenseite wird der selbe Schlüsselstrom erzeugt und zu Entschlüsselung des Chiffrestroms benutzt.



Im folgenden werde ich nun einige symmetrische Verfahren zeigen

DES (Data Encryption Standard)

Der Schlüssel ist ein 64 Bit langer String. Teilt man den String in acht Teile so ist das letzte Bit des Teilstringes immer so gesetzt, dass die Quersumme aller Bits ungerade ist. Da nur je sieben Bits frei wählbar sind, ist ein DES-Schlüssel 56 Bits lang. Der Schlüssel wird für Ver- und Entschlüsselung eingesetzt.

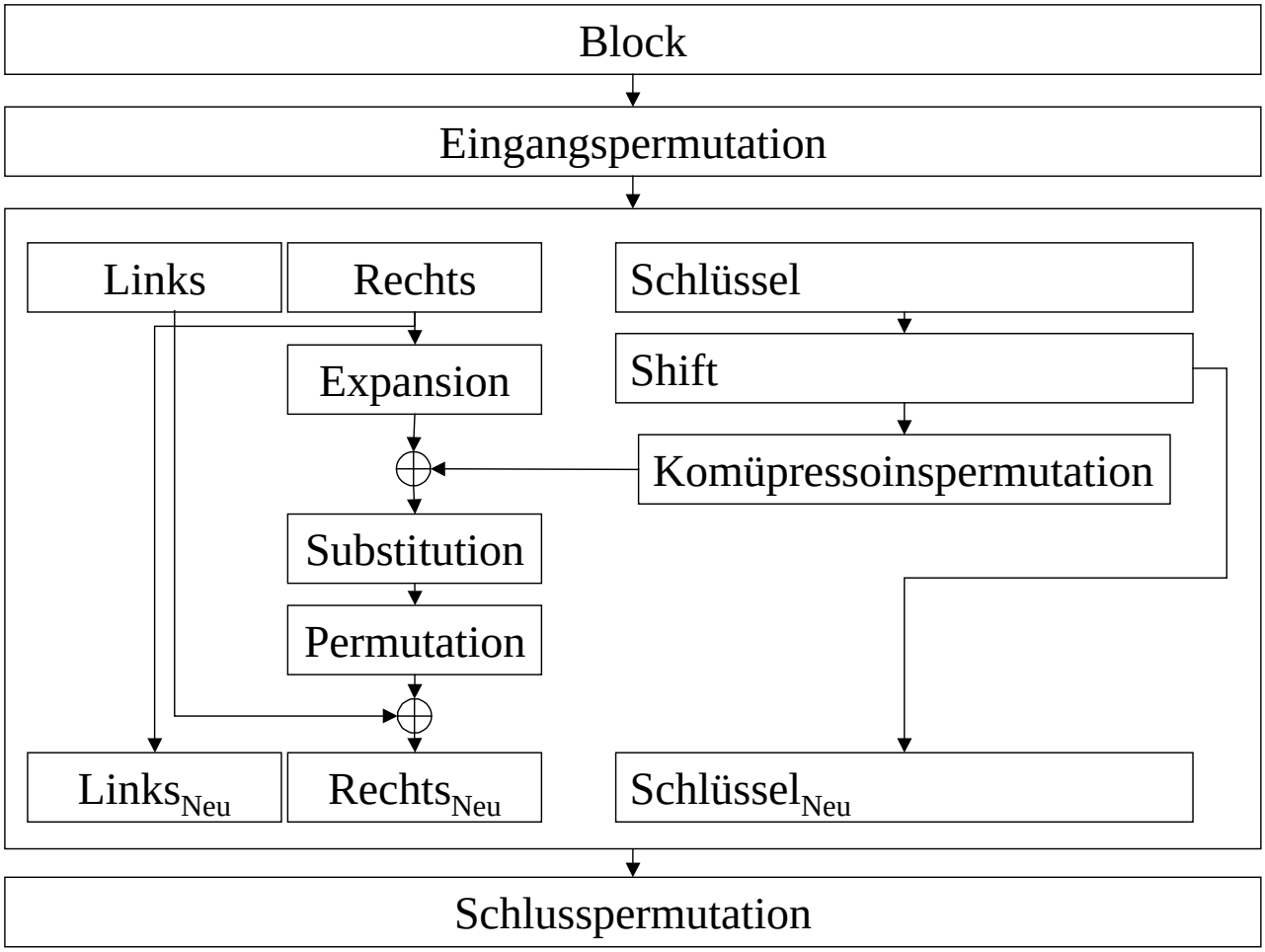
Der DES-Algorithmus arbeitet in drei Schritten. Im ersten Schritt wird eine im Verfahren feste initiale Permutation angewandt.

Danach wird der Block in zwei 32Bit Blocke in der Mitte geteilt. Nun wird auf den gesamten Block 16 Runden lang die identischen Operationen ausgeführt, wobei bei jeder Runde die Bits des Schlüssels verschoben werden.

In einer Runder wird die rechte Hälfte per Algorithmus auf 48 Bit verbreitert und mit XOR auf ausgewählte Bits aus dem Schlüssel kombiniert. Danach werden feste Substitutionen darauf ausgeführt, die wieder 32 Bit erzeugen. Schließlich wird noch einmal fest permutiert. Das Ergebnis wird über XOR mit der linken Hälfte kombiniert.

Die rechte Hälfte wird für die nächste Runde die linke, während das berechnete Ergebnis die neue rechte Hälfte ergibt.

Die Schlusspermutation ist die Inverse zur Eingangspermutation.



AES (Advanced Encryption Standard)

Jahrelang war DES der Standard in der Verschlüsselung, jedoch hat 1997 die NIST („National Institut for Standard and Technology“) gesagt, dass DES bei der jetzigen Entwicklung der Technik, in Zukunft nicht mehr sicher genug sei. Deshalb hat sie einen internationalen Wettbewerb ausgeschrieben, in dem ein neues Verschlüselungsverfaheren ausgewählt werden soll, welches DES als Standard ablösen soll.

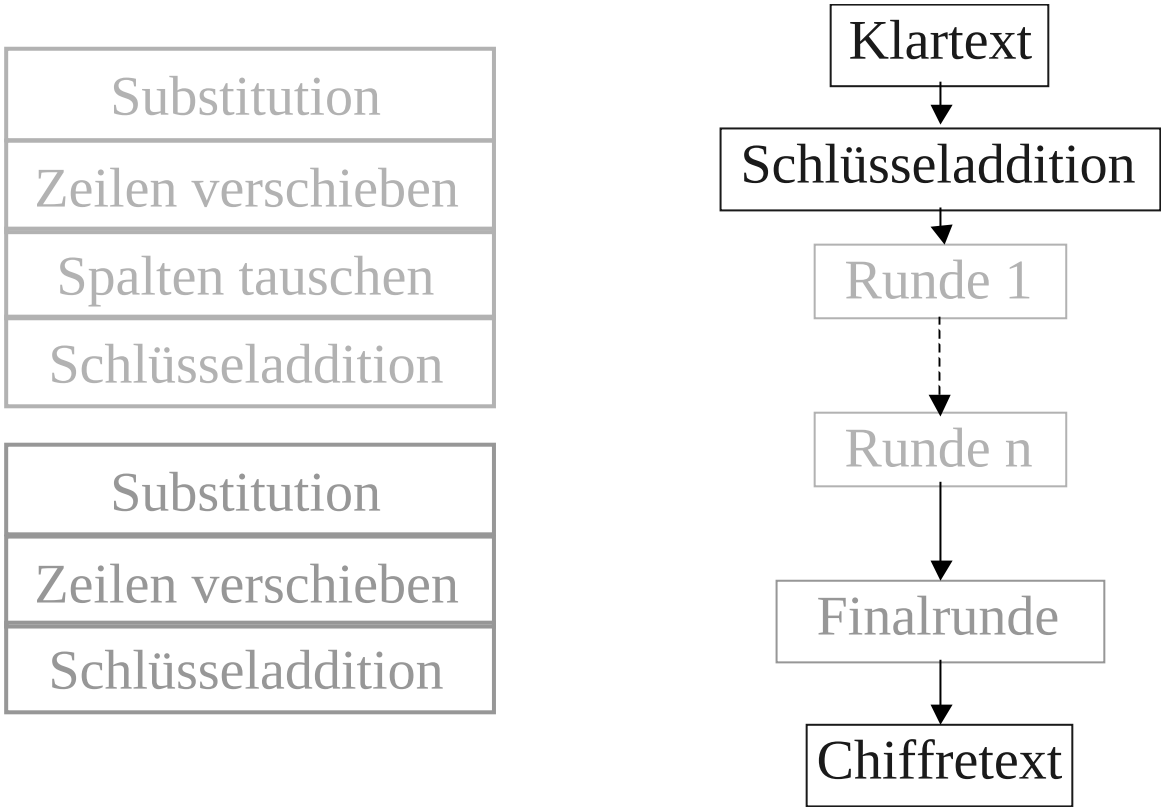
Das Verfahren sollte symmetrisch und Rundenbasiert sein, wie es DES auch ist. Zudem sollen Schlüssel mit 128, 194, 256 Bit Länge verwendet werden können.

Die Entscheidung fiel im Herbst 2000 für den Rijndael-Adglorithmus von Joan Deamen und Vincent Rijmen aus Belgien.

Bei diesem Algorithmus hängt die Anzahl der Runden von der Länge des verwendeten Schlüssels ab. Vor der Ersten Runde wird eine Schlüsseladdition ausgeführt, d.h. der Schlüssel wird binär auf den Klartext addiert. Nach diesen

normalen Runden wird eine Finalrunde durchgeführt, welche sicherstellt, dass Ver- und Entschlüsselung mit dem gleichen Algorithmus durchgehführwerden können.

In einer normalen Runden werden nacheinander fest vorgeschriebene Substitutionen, Zeilenverschiebungen und Spaltentausch durchgeführt. Dabei ist auch die Reihenfolge vorgeschrieben. Danach erfolgt immer eine Schlüsseladdition. In der Finalrunde wird der Spaltentausch aus symmetrischen Gründen des Algorithmuses weggelassen.



One-Time-Pads

One-Time-Pads sind, im Gegensatz zu DES und AES, Stromchiffre. Ihre Stromschlüssel gehen oft über mehrere Seiten und sind immer länger als die zu verschlüsselnde Nachricht. Jeder dieser Schlüssel wird nur einmal zu Verschlüsselung verwendet, dies macht dieses System sehr sicher. Nach der Verschlüsselung wird der Stromschlüssel vernichtet und nur der Empfänger kann die Nachricht mit seiner „Kopie“ des Stromschlüssels lesen.

Ohne das Pad kann keiner die verschlüsselte Nachricht lesen, denn die Wahrscheinlichkeit dass ein bestimmter Klartext dahinter steht ist gering und man kann auch keinen Rückschlüsse über den Schlüssel machen.

Asymmetrische Verschlüsselung

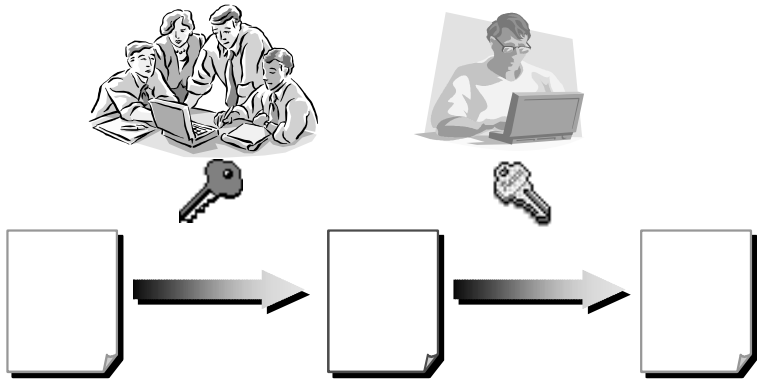
Der Nachteil bei symmetrischer Verschlüsselung ist, dass der gleiche Schlüssel für Ver- und Entschlüsselung genommen wird. Dieser muss natürlich geheim gehalten werden. Da er über einen sicheren Kanal ausgetauscht werden muss ist dies ein entscheidendes Sicherheitsloch.

Einfacher wäre dies, wenn jeder Teilnehmer seinen eigenen Schlüssel hätte, mit dem er Nachrichten an Ihn lesen kann – und nur er. Symmetrische Schlüssel können einem in diesem Punkt keine Sicherheit geben.

Zu jedem privaten Schlüssel (Private Key) gibt es dann eine öffentliches Gegenstück (öffentlicher Schlüssel oder Public Key), das jeder sehen und benutzen kann. Jede Nachricht an eine Person wird mit deren öffentlichen Schlüssel verschlüsselt und diese kann die Nachricht mit ihrem privaten Schlüssel lesen.

Da die Sicherheit des Systems nur noch von privaten Schlüssel abhängt müssen die Schlüssel ein zusätzliches Kriterium zu denen eines symmetrischen erfüllen. Nämlich dass aus dem Öffentlichen Schlüssel nicht der private Schlüssel herleitbar ist. Asymmetrische Schlüssel sind einiges länger als ihre symmetrische Gegenstücke.

Asymmetrische Verfahren sind deutlich aufwendiger in den Berechnungen als symmetrische. Die Verfahren sind oft auf mathematische Spezialfälle aufgebaut (z.B. Rucksackproblem, große Primzahlen). Der Schritt der bei der Asymmetrischen Verschlüsselung wesentlich erschwert wurde ist die Entschlüsselung, da dies nur mit dem privaten Schlüssel geschehen darf und dieser nicht herleitbar ist.



Ein entscheidender Vorteil der asymmetrischen Verschlüsselung gegenüber der symmetrischen ist, dass nicht für jedes Teilnehmerpaar ein eigener Schlüssel benötgit wird, wenn jeder mit jedem sicher kommunizieren will; sondern nur pro Teilnehmer ein öffelntlicher Schlüssel (n(n-1) Schlüssel vs. n Schlüssel).

RSA

RSA ist der erste vollständige Public-Key Algorithmus, der sich auch für Digitale Signaturen (siehe unten) geeignet ist. Er ist auch der am einfachsten zu implementierende aller bisher veröffentliche Algorithmen.

Die Sicherheit beruht auf der Schwierigkeit, große Zahlen zu fakorisieren. Die Schlüssel hängen von sehr großen Primzahlen ab.

Zur Schlüsselerzeugung wählt man zwei zufällige, groß Primzahlen p und q aus. Man errechnet das Produkt n.

Wähle danach ein e das prim zu (p-1)(q-1) ist. Dies ist unser Chiffrierschlüssel.

Aus den erweiterten Euklidischen Algorithmus bekommt man dann den Dechiffrierschlüssel d (ed = 1 mod (p-1)(q-1)).

Die Verschlüsselung:

$$c = m^e \bmod n$$

Die Entschlüsselung:

$$m = c^d \bmod n$$

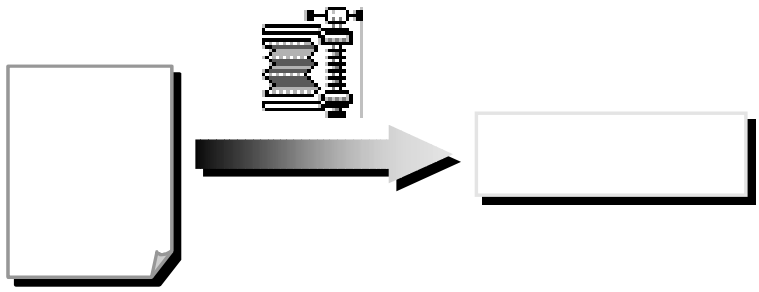
Einweg-Hashes

Hashes sind Funktionen, die einen beliebig langen Text über eine mathematische Funktion auf eine fest Länge kürzt. Sie sollen einen Fingerabdruck (Fingerprint) eines Textes ergeben. Damit aus dem Hash nicht wieder der Originaltext hergestellt werden kann oder man auf dessen Aufbau aus dem Hashwert schließen kann, werden sogenannte Einweg-Hasches eingesetzt, des Funktion einfach ist, aber eine Unhehrfunktion zu bilden fast unmöglich ist.

Bei solchen Kompremierungen kann es vorkommen, dass zwei Texte den gleichen Hashwert haben. Dies ist ein Standardproblem der Statistik, genannt das Geburtstags-Paradoxon.

Dieses Paradoxon stellt die Frage, ab wie viel Personen die Wahrscheinlichkeit mehr als 50% bträgt, da jemand am selben Tag Geburtstag hat wie ich. Die Antwort ist 253. Frag man jedoch ab wann die Wahrscheinlichkeit größer 50% ist, dass zwei bleibige Peronen ein Gruppe am selben Tag Geburtstag haben, ist die Antwort 23.

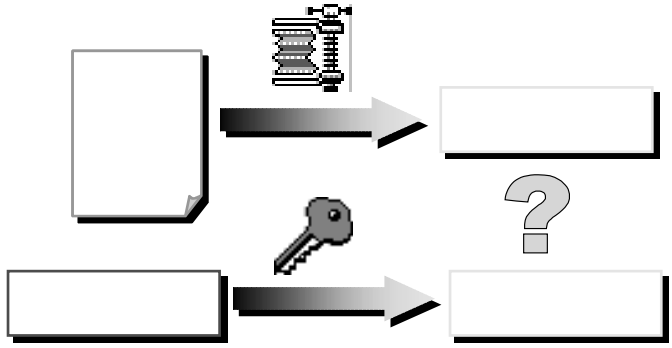
Auf die Hashes übertragen kann man sagen, dass relativ wahrscheinlich ist, dass zwei inhaltlich sinnvoll nachrichten den gleichen Hash haben, es aber nicht sehr wahrscheinlich ist eine Nachricht mit den selben Hash zu finden, wie diejenige, die ich sende. Um zwei Nachrichten zu finden sind $2^{m/2}$ zufällige Nachrichten nötig. Bei einer Hashlänge von 160 Bit beträgt die Wahrscheinlichkeit eine Nachricht mit den selben Hashwert zu finden also $1:2^{80}$.



Digitale Signatur

Die Digitale Signatur ist die Unterschrift unter ein elektronisches Dokument. Dort kann man nicht, wie auf Papier, mit der Füller unterschreiben. Des halb wurde über legt, was man machen kann, damit ein Dokument auch für den Unterzeichne r rechtsverbindlich wird. In Deutschland gab es seit dem 22. Juli 1997 ein Signaturgesetz, die wurde in der jetzigen Legislaturperiode am 15. Februar 2001 geändert.

Bei der digitalen Signatur wird ein Hash aus der Nachricht gebildet und mit dem privaten Schlüssel des Erstellers verschlüsselt. Dieser kann mit dem Öffentlichen Schlüssel des Erstellers entschlüsselt und dann verglichen werden mit dem der mitgesendeten Nachricht.



Das neue Signaturgesetz lässt es nun auch zu, dass offizielle Dokume nte – außer Urkunden – in digitaler Form mit einer entsprechenden Signatur Gültigkeit haben. Die vorgaben wurden vom Gesetzgeber streng festgelegt.

Neues Signaturgesetz

1. “elektronische Signaturen” Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen
2. “Signaturschlüssel” einmalige elektronische Daten wie private kryptographische Schlüssel, die zur Erstellung einer elektronischen Signatur verwendet werden,
3. “Signaturprüfschlüssel” elektronische Daten wie öffentliche kryptographische Schlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden
4. “fortgeschrittene elektronische Signaturen”, die
    - ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind
    - .die Identifizierung des Signaturschlüssel-Inhabers ermöglichen
    - mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann
    - mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann
5. qualifizierte elektronische Signaturen”, die
    - auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen
    - mit einer sicheren Signaturerstellungseinheit erzeugt werde

Zertifizierung

Um eine digitale Signatur zu erstellen, braucht man ein nachprüfbar, gültiges Zertifikat. Dieses Zertifikat bestätigt, dass es sich hier eine bestimmte Person handelt und sich niemand für sie ausgibt. Sie sind elektronische Bescheinigungen, mit denen Signaturprüfschlüssel einer Person zugeordnet werden und die Identität dieser Person bestätigt wird.

Es gibt verschieden Klassen von Zertifikaten. Das Niedrigste sag nur, dass irgendjemand, der diesen Namen angegeben hat, mit einer bestimmten E-Mail ein Zertifikat hat. Das Höchste bestätigt, dass hinter einem Zertifikat eine bestimmte Person steht, die existiert und deren Personalien mit den im Zertifikat angegeben übereinstimmen.

Zertifizierungsdienstesanbieter sind natürliche oder juristische Personen, die qualifizierte Zertifikate herausgeben. Sie zeihen auch ungültige Zertifikate, welche sie ausgestellt haben, wieder zurück

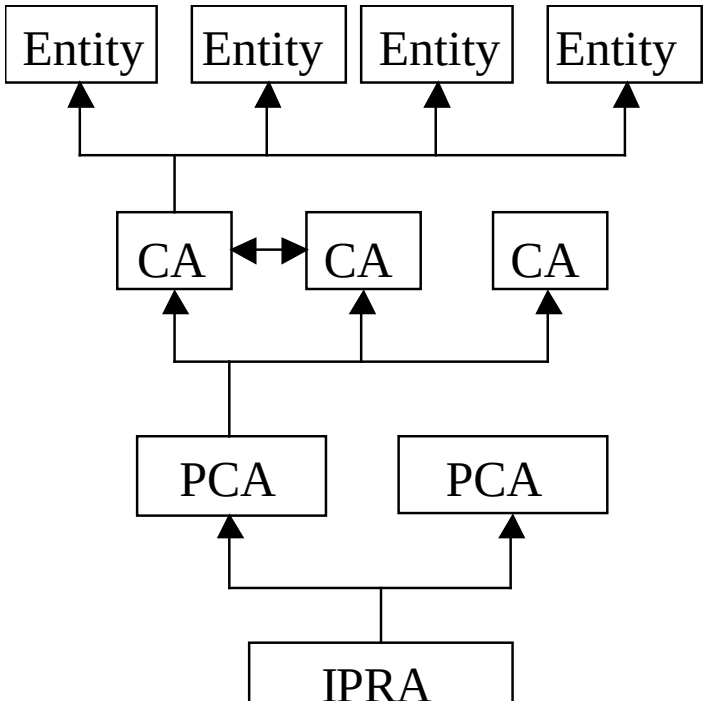
X.509

Im X509 wird eine Struktur für Public-Key-Zertifikate festgelegt. Dabei bekommt jeder Benutzer einen eindeutigen Namen von seiner CA (Certification Authority), so wie einen eindeutigen Schlüssel für Unterschriften.

Die CAs erden von einer PCA (Policy Certification Authorities) zertifizerit. Wech wiederung von einer IPRA (Internet Policy Registration Authority) zertifiziert werden. So entsteht eine Baumstruktur.

Es werden von einer Zertifizierungsstelle nur die unmittelbar darrüberliegende Schicht zertifizeirt. Cas zertifizieren sich oft gegenseitig, damit deren Benutzer die Zertifikate der anderen CA auch benutzen können.

Um ein Zertifikat zu überprfen muß man nur noch den Pfad von dem zu überprüfenden zertifikat zu einem Zertifikat, dem man vertraut zurückverfolgen. Sind alle Zertifikate in Ordnug, so kann man dem Zertifikat vertrauen. Ist ein Zertifikat dabei, dass zurückgezogen wurde, so ist auch da zu überprüfende Zertifikat ungültig.



Inhalts eines X.509-Zertifikats:

- Version
- Seriennummer
- Algorithmus/Parameter
- Aussteller
- Geltungsdauer
- Betreff
- Public Key
  Aussteller-Signatur

Die Rücknahme eines noch nicht abgelaufenen Zertifikat läuft über eines sog. CRL (Certificate Revocation List):

- Version
- Aussteller-Signatur
- Seriennummer
  Liste der Zertifikate

Das Feld „Version“ gibt in einem Zertifikat immer dessen Format an. Die „Seriennummer“ wird innerhalb einer CA eindeutig vergeben und dient der eindeutigen Identifizierung des Zertifikats. Unter „Algorithmus/Parameter“ wird Algorithmus, der zum Unterzeichnen eines Zertifikat benutzt wird, angegeben und weitere dazu notwendige Informationen. Als „Aussteller“ wir immer der Name der CA angegeben. Die „Geltungsdauer“ besteht aus zwei Daten, zwischen denen das Zertifikat gültig ist. Der „Betreff“ ist der Name des Inhabers des Zertifikates. Dessen öffentlicher Schlüssel wird unter „Public Key“ im Zertifikat angegeben. Das Zertifikat wird mit dem öffentlichen Schlüssel der CA zum Schluss unterschreiben.

OCSP (Online Certificate Status Protocol)

Wenn man überprüfen will ob ein bestimmtes Zertifikat gültig ist, muss man nach dem X.509 Protokoll in den CRL nachschauen, ob ein Zertifikat gültig ist. Diese CRL werden oft nur in großen Intervallen erneuert. Dies bedeutet, dass eine CRL nicht sehr aktuell ist. Da die CRL sehr groß sein können, werden diese auch nicht oft (meist einmal) neu eigelesen.

Als Alternative zu den CRL des X.509 Protokolls gibt es das OCSP. Bei diesem Protokoll kann man online bei einem Provider eine Anfrage nach einem Zertifikat. starten. Man muss pro zu überprüfenden Zertifikat immer eine neue Anfrage an den Server stellen.
Der Server gibt dann den aktuellen Status des angefragten Zertifikates zurück. Dieser zurückgegebener Status des Zertifikats kann folgende Werte haben:

- „good“: Zertifikat in Ordnung
- „revoake“: Zertifikat wurde zurückgezogen
- „unknown“: Unbekanntes Zertifikat

Bei diesem Protokoll muss man manuell bis zu einer „trusted“ CA, der man vertraut, prüfen.

SCVP (Simple Certificate Validation Protocol)

Damit man nicht immer von Hand aller Zertifikate bis zu einer vertrauenswürdigen CA überprüfen will, übergibt man an einen Server die zu prüfende Zertifikate und vertauenswürdige CAs. Der Server überprüft dann, ob es einen gültigen Pfad von den zu prüfenden Zertifikate zu einer der vertrauenswürdigen CAs gibt. Nach dem der Server alle Ergebnisse hat, gibt er zurück, ob Zertifikate vertauenswürdig sind.

Man muss bei diesem Protokoll Vertrauen in Server wie eigene Software haben. Bei allen Protokollen kann man sich immer dadurch absichern, dass man jede Nachricht

signiert und auch anfordert, dass der Server alle Nachrichten signiert. Andersrum kann der Server auch nur Anfragen bearbeiten, die vom Anfragenden signiert wurden.

Krypto Debatte / Politik

Während der Debatte über das neue Signaturgesetz kam auch die Frage auf, ob nicht die Benutzung von starker Kryptographie, also hoher Verschlüsselung und lange Schlüssel, eingeschränkt oder verboten werden soll.

Befürworter bringen gerne das Argument, dass Kriminelle und organisiertes Verbrechen ihre Daten so vor Zugriff vor der Justiz schützen können. Wenn man sieht, wie diese Leute ihr Geld verdienen, werden sie wohl eventuell kleinere Strafen in Kauf nehmen, als für die restlichen Verbrechen.

Auch Militär und Staatsschutz führen gern den Begriff „Innere Sicherheit“, wenn sie starke Kryptographie verbieten will. Sie glauben, dass politische Gegner , z.B. RAF, diese benutzt um im Untergrund ungestört zu kommunizieren.

Für den freien Einsatz der starken Verschlüsselung ist vor allem Industrie und Dienstleistungsgewerbe. Denn Kunden, Forschungs- und Entwicklungsdaten wollen sie vor der Konkurrenz und evtl. Erpressern schützen. Hier stehen Milliarden auf dem Spiel.

Man kann auch starke Verschlüsselung umgehen, indem man mehre schwächere Schlüssel hintereinander verwendet. Eine andere Methode die Verschlüsselung zu umgehen ist die Steganographie. Somit hätte ein eventuelles Verbot kaum Konsequenzen.

Schlusswort

In den letzten Jahren hat die Kryptographie eine immense Entwicklung gemacht, nicht zuletzt durch die immer schneller werdende technische Entwicklung. Da Computer immer leistungsfähiger werden und dadurch ältere Algorithmen schneller knacken, ist auch anzunehmen, dass die Algorithmen immer ausgefeilter werden.

Eine weitere Entwicklung könnte auch alle bestehenden Regeln in der Kryptographie außer Kraft setzen. Die Quantencomputer können, im Gegensatz zu heutigen Computern, massiv parallel rechnen und somit „Brute Force“ Angriffe erleichtern.

Kryptographie kann wie jede andere Technologie missbraucht werden, jedoch liegt das an uns, wie wir damit umgehen.

Interessante Quellen

Bücher
Angewandte Kryptographie, B. Schneider, Addison-Wesley,1996
Entzifferte Geheimnisse(3. Aufl.), F.L. Bauer, Axel Springer Verlag, 2000
Einführung in die Kryptographie, J. Buchmann, Axel Springer Verlag, 1999

Internet
Allgemein
http://www.cs.adfa.edu.au/teaching/studinfo/ccs3/lectures/
http://www.ftech.net/%7Emonark/crypto/index.htm

Geschichte
http://www.lexiter.com/misc/ps_crypto/highlights.html
http://www.cs.adfa.edu.au/teaching/studinfo/ccs3/lectures/less02.html

AES
http://csrc.nist.gov/encryption/aes/
http://home.ecn.ab.ca/~jsavard/crypto/co040801.htm

Signatur-Gesetze
http://www.signaturrecht.de/

Zertifikate
http://www.cryptolinks.de/
http://www.ietf.org/internet-drafts/draft-ietf-pkix-scvp-05.txt
http://www.ietf.org/internet-drafts/draft-ietf-pkix-ocspv2-02.txt