Nachrichten-Verschlüsselung

Vortrag Tom Novacek, 03.02.2014

1 Das Prinzip der Übertragung geheimer Nachrichten

Der Absender A möchte eine Nachricht über eine *unsichere Verbindung* dem Empfänger E so zusenden,

1. dass niemand außer E sie verwenden kann (sie wäre – wenn kopiert oder irregeleitet - unverständlich, unbrauchbar),
2. dass die Nachricht unverfälscht ankommt oder eine Verfälschung zumindest erkennbar ist (Integrität) und
3. dass der Empfänger sicher sein kann, dass die Nachricht vom angegebenen Absender stammt (Authentifizierung).

Damit wäre zwar der Inhalt einer solchen Nachricht geheim und sie würde zuverlässig übertragen, wichtige Informationen können aber aus der unleserlichen Nachricht trotzdem gewonnen werden:

- Hinweise auf Absender und Empfänger,
- Zeitpunkt der Übertragung, Korrelation mit anderen Ereignissen,
- Vermutung kausaler Zusammenhänge zwischen Nachrichten,
- Länge der Nachricht (militärische Wettermeldungen, Befehle...),
- Vorkommen ähnlicher Nachrichten
- …

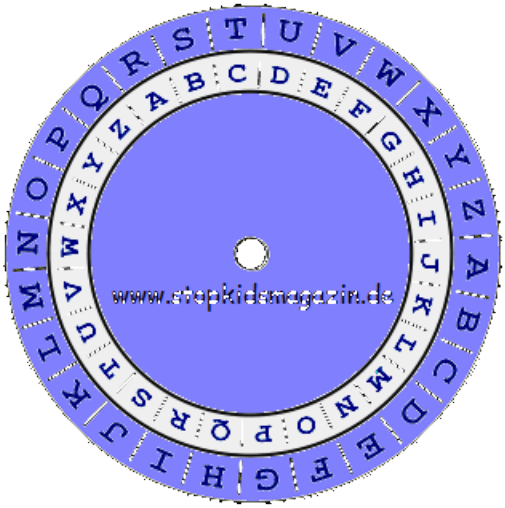
Punkt 1, mit Einschränkungen auch 2 und 3, können erfüllt werden, wenn der Absender die Nachricht in etwas übersetzt, das niemand außer dem gewünschten Empfänger sie rückübersetzen kann.

> Das Ergebnis der Übersetzung kann durchaus auch eine existierende Sprache sein. Die US-Armee verwendete im 2. Weltkrieg dafür die Sprache der Navajo-Indianer. Als Kodierer und Dekodierer wurden Angehörige dieses Stammes rekrutiert. Die Sprache wurde gewählt, da seit über 20 Jahren kein deutscher Wissenschaftler die Navajos besucht hatte und die Sprache keine Ähnlichkeit mit anderen hat (Grammatik, Syntax). Zum Beispiel wird die Endung eines Zeitwortes von der Art des Objekts bestimmt, ob es lang ist (Pfeife, Stift), schlangenförmig, körnig usw.

Praktische Bedeutung haben heute nur Computer-Programme als elektronische Übersetzer, die mit mathematischen Algorithmen Texte in Zeichenketten ohne nutzbare innere Struktur wandeln (und zurück).

2 Der Anfang: Cäsar Verschlüsselung

PCSENIOREN ↔ YLBNWRXANW



Eine solche Nachricht ist leicht zu entschlüsseln, wenn

- die Sprache bekannt ist
- Worte der Nachricht aus dem Wörterbuch stammen (nicht Code, Schlüssel...)

Entschlüsselungsverfahren: durchprobieren, Buchstabenhäufigkeit Buchstabengruppen

3 Die Verbesserung: Vigenère-Verschlüsselung

Für jeden Buchstaben wird eine andere Verschiebung benutzt
Beispiel: Vigenère-Quadrat

```
Text:                   geheimnis
Schlüssel: AKEF         AKEFAKEFAKEFAKEF
Ergebnis Geheimtext:    GOLJIWRNS
```

	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	**L**	M	N	O	P	Q	**R**	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	**J**	K	L	M	**N**	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	**O**	P	Q	R	S	T	U	V	**W**	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
…	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.

4 Das Grundprinzip aller digitaler Ver/Entschlüsselungsverfahren:

- Es gibt ein **Verfahren** zum Ver- bzw. Entschlüsseln (Methode, Formel, Anweisung o.ä.). Es muss **nicht geheim** gehalten werden.
- Der Ablauf der Ver/Entschlüsselung ist durch das Verfahren nur *im Prinzip* festgelegt.
- Der *genaue* Ablauf wird erst durch einen **wählbaren Schlüssel** (Parameter, Code...) bestimmt.

  Beispiel: "Ersetze jeden Buchstaben durch den n-ten Nachfolger im Alphabet"
  Erst mit dem Schlüssel n = 3 wird das Verfahren eindeutig: a ↔ d, b ↔ e ...
- Wird der Schlüssel z. B. vom Absender der Nachricht festgelegt
  - benutzt er ihn zum Verschlüsseln und teilt ihn dem Empfänger **geheim** mit
  - Der Absender verschlüsselt damit die Nachricht und sendet sie an den Empfänger.

- Der Empfänger entschlüsselt die Nachricht mit dem ihm bekannten (nicht geheimen) Verfahren unter Verwendung seines (geheimen) Schlüssels
- Mit demselben Verfahren und demselben Schlüssel können auch mehrere Nachrichten und Antworten in beiden Richtungen verschlüsselt werden.

Die **Schwachstelle** ist bei all diesen "symmetrischen" Verschlüsselungsverfahren der **geheime Austausch des gemeinsamen Schlüssels.**

Überlegung: Wenn das ohne Schwierigkeit möglich wäre, könnte man denn nicht gleich die Nachricht selbst geheim übertragen und sich die Mühe mit dem Verschlüsseln sparen?
Bei einer einzigen kurzen Nachricht stimmt das schon, aber im Normalfall

- kann man einen Schlüssel mehrfach benutzen, also mit demselben Schlüssel eine Zeit lang Nachrichten übertragen und muss
- nur die (seltenere) **Schlüsselübertragung mit besonders hohem Aufwand** absichern.

5 Die Lösung des Problems "Schlüsselübertragung"

Erste Ideen: Kassette mit Anhängeschlössern

- A legt Dokument in Kassette, verschließt mit Anhängeschloss A und sendet sie an E
- E fügt Anhängeschloss E hinzu, sendet zurück
- A entfernt Anhängeschloss A, sendet an E
- E entfernt Anhängeschloss E und öffnet Kassette

Die Umsetzung auf ein Verfahren zur direkten Text-Verschlüsselung ist nicht brauchbar, weil die Entschlüsselung die umgekehrte Reihenfolge der Verschlüsselungen benutzen muss und *s*olche **reihenfolgeunabhängige Verfahren –** dazu gehört auch die Caesar-Verschlüsselung **- grundsätzlich relativ leicht zu entschlüsseln** sind.
Die meisten Vorgänge im täglichen Leben sind nicht reihenfolgeunabhängig! Zum Beispiel
Strumpf anziehen → Schuh anziehen → Strumpf ausziehen → Schuh ausziehen: gwht so nicht.
Das Beispiel mit den Kassetten würde auch nicht funktionieren, wenn E die empfangene Kassette in eine größere steckt und diese mit seinem Anhängeschloss E verschließt. A kann sein Anhängeschloss nicht entfernen, es ist ja im Inneren der größeren, mit Anhängeschloss E verschlossenen Kassette!

Der erste erfolgreiche Ansatz von Diffie, Hellmann und Merkle (1976)

- A erzeugt einen geheimen Schlüssel A, verändert ihn durch eine bekannte, nicht geheime "**Einwegfunktion"**, sendet das "Resultat A" an E
- E macht es mit seinem geheimen Schlüssel E ebenso, sendet das "Resultat E" an A
- Jeder der beiden setzt das empfangene Resultat und den eigenen geheimen Schlüssel in eine (bekannte, nicht geheime) Formel ein
- Beide erhalten - ein mathematisches Kunststück! - als **Ergebnis dieselbe neue, lange Zahl** und verwenden sie als Schlüssel. Dieser Schlüssel wurde nie übertragen.
- Die Einwegfunktion stellt sicher, dass sich die geheimen Schlüssel nicht aus den Resultaten errechnen lassen. Werden die Resultate gestohlen, kann der Dieb damit nichts anfangen.
- Was blieb noch zu tun? Die Einwegfunktion musste gefunden werden, Die Lösung

lag in der **Primzahlzerlegung.** Sie ist weiter unten unter "Der nächste Schritt: Rivet, Shamir und Adleman – RSA Verfahren, 1977" kurz beschrieben.

Verdeutlichung mit Farbeimern:

- A kauft einen 3-liter-Eimer, vermischt darin 1 Liter einer geheim zusammengemischter Farbe (z.B. ein bestimmtes Rot) und 1 Liter der Farbe gelb vom Baumarkt(nicht geheim), das ergibt 2 Liter eines bestimmten Orange
- E kauft einen 3-Liter-Eimer, vermischt darin 1 Liter seiner geheime Farbe (z. B. Ein bestimmtes Blau) und 1 Liter derselben gelben Farbe gelb, das ergibt 2 Liter eines bestimmten Grün
- A und E tauschen ihre Eimer per Post aus
- Beide fügen 1 Liter ihrer geheimen Farbe hinzu. Jeder Behälter enthält also eine Mischung von 1 Liter Geheimfarbe A, 1 Liter Geheimfarbe E und 1 Liter gelber Farbe – das ergibt eine **neue, gemeinsame Mischfarbe** = der gemeinsame "Schlüssel".
- Ein Böser, der die Eimer klaut und den Inhalt mischt, kann diese Mischfarbe nicht erzeugen, denn die Mischung enthielte zwar je 1 Liter der beiden Geheimfarben, aber **2 Liter** Gelb! Er müsste aus einer der beiden Mischungen entmischen und das Gelb entfernen. Das ist aber nicht möglich, denn das Mischen ist eine "Einwegfunktion" und kann nicht rückgängig gemacht werden.

Das Diffie-Hellmann Verfahren wird bei den heutigen digitalen Verschlüsselungen in verwendet.

Der nächste Schritt: Rivet, Shamir und Adleman – RSA Verfahren, 1977

Whitfield Diffie hatte schon die Idee der **asymmetrischen Verschlüsselung.** Rivet, Shamir und Adleman haben sie weiter entwickelt und die dazu nötige **Mathematik** gefunden**.**

- Bei diesem Verfahren gibt es **zwei Schlüssel**, einen zum Verschlüsseln und einen anderen zum Entschlüsseln. Sie werden gemeinsam durch eine mathematische "Einweg-Formel" erzeugt aus Zufallszahlen erzeugt.
- Der "Entschlüssel" ist geheim (geheimer, privater Schlüssel), der "Verschlüssel" wird veröffentlicht (öffentlicher Schlüssel)

Verdeutlichung mit Einschnappschlössern:

- E sendet A ein Anhängeschloss. Es wird durch Einschnappen geschlossen und nur E kann es mit seinem Schlüssel wieder öffnen. Es ist so gebaut, dass man auch durch Zerlegen des Schlosses den zugehörigen Schlüssel nicht rekonstruieren kann ("Einwegfunktion")
- A legt das geheime Dokument in eine Kassette, verschließt sie mit dem Einschnappschloss und sendet sie an E.
- Niemand kann die Kassette auf dem Weg öffnen, auch A nicht
- E empfängt die Kassette und öffnet sie mit seinem Schlüssel
- E könnte das offene Anhängeschloss auch an mehrere Leute verteilen, es in Postagenturen oder Amazon zur Verfügung: Jeder kann damit eine Sendung an E schützen.

Für die asymmetrische Verschlüsselung gibt es zwei Anwendungen

- Ein Besitzer des öffentlichen Schlüssels verschlüsselt mit diesem (und dem dazugehörigen Berechnungsverfahren) eine Nachricht, nur der Besitzer des geheimen Schlüssels kann sie entschlüsseln und öffnen → **sichere Übertragung**
- Der Besitzer des geheimen Schlüssels verschlüsselt eine Nachricht mit diesem

geheimen Schlüssel, **jeder** Besitzer des öffentlichen Schlüssels kann sie **entschlüsseln und öffnen. D**ie Nachricht ist also nicht geheiem, jeder Empfänger der Nachricht kann aber sicher sein, dass sie **von dem Besitzer des geheimen Schlüssels** stammt – **Authentifizierung.**
Ob allerdings der Besitzer des geheimen Schlüssels als Absender in der Nachricht angegeben ist und nicht irgend jemand anderer, muss noch extra abgesichert werden durch ein **Zertifikat**, mit dem nachgewiesen wird, dass der öffentliche Schlüssel wirklich dem Absender (Person, Firma, Institution usw.) gehört.
Im Bankgeschäft ist die Authentifizierung wichtiger als die sicher Übertragung!

Das asymmetrische Verfahren benutzt die **Zahlentheorie**, eine hochkarätige Sparte der Mathematik, die sich mit den ganzen Zahlen beschäftigt. Sie fand in der "Kryptologie", mit der wir uns hier beschäftigen, die erste praktische Anwendung. Benutzt werden dabei **Primzahlen**

Primzahlen sind ganze Zahlen, die sich durch keine Zahl ohne Rest dividieren lassen (außer durch sich selbst und 1).
2, 3, 5, 7, 11, 13, 17 usw. sind Primzahlen. Jede beliebige Zahl lässt sich in Primzahlen zerlegen., z. B. 728 = 2 x 2 x 2 x 7 x 13. Trotz jahrhundertelanger Bemühungen aller Mathematiker gibt es kein Verfahren, diese Zerlegung zu *errechnen*, man kann nur Schritt für Schritt durch eine Primzahl nach der anderen versuchsweise dividieren. Bei dreistelligen Zahlen geht das mit Papier und Bleistift, bei 6-stelligen Zahlen mit dem Taschenrechner, bei 130 Dezimalstellen würde ein PC Monate brauchen, der neue NSA Rechner aber nur Sekunden. Praktisch verwendet werden Zahlen mit über 300 Dezimalstellen! Da die Primzahlverschlüsselung ein mathematischer Vorgang ist und für beliebig große Zahlen funktioniert gibt es auch kein Problem, wenn die **Rechner immer schneller** werden: Man benutzt einfach **noch längere Zahlen**, davon gibt es ja unendlich viele.
Eine Grenze setzt vielleicht einmal der Quantencomputer, aber es gibt schon Vorschläge zu einer **Quantenverschlüsselung**, gegen die auch der machtlos sein wird.

Beim Verschlüsseln wird der Text als Zahlenfolge interpretiert und in eine Formel eingesetzt. Eine Nachricht mit ein paar hundert Zeichen ergäbe eine mehr-hundertstellige Dezimalzahl, die bei der Umrechnung noch viele größere Zahlen erzeugen würde – zu viel für einen PC, der ja das Ver- und Entschlüsseln besorgen muss. **Das asymmetrische Verfahren** wird daher vorwiegend nur dazu verwendet, eine kurze Nachricht sicher zu übertragen, nämlich einen zufällig erzeugten **Schlüssel für ein symmetrisches Verschlüsselungsverfahren. Dieses wird dann zur Verschlüsselung der eigentlichen Nachricht benutzt.**

6 Zufall?!

An mehreren Stellen kommt in dieser Beschreibung der Begriff "Zufall" vor. Bei allen Verschlüsselungen muss ein Schlüssel verwendet werden und natürlich nicht immer derselbe. Es müssen also ständig neue Schlüssel erzeugt werden. Die dürfen aber nicht durch ein Berechnungsverfahren entstehen (es könnte wie jedes Verfahren nicht geheim gehalten werden) sondern müssen "zufällig" sein. Und der Computer soll das möglichst alleine machen, ohne dass wir unsere Phantasie anstrengen müssen. *Wir* halten leicht etwas für zufällig, bloß weil wir die Kausalität dahinter nicht erkennen, aber ein erfahrener "Krypt-Analytiker" fällt darauf nicht herein.

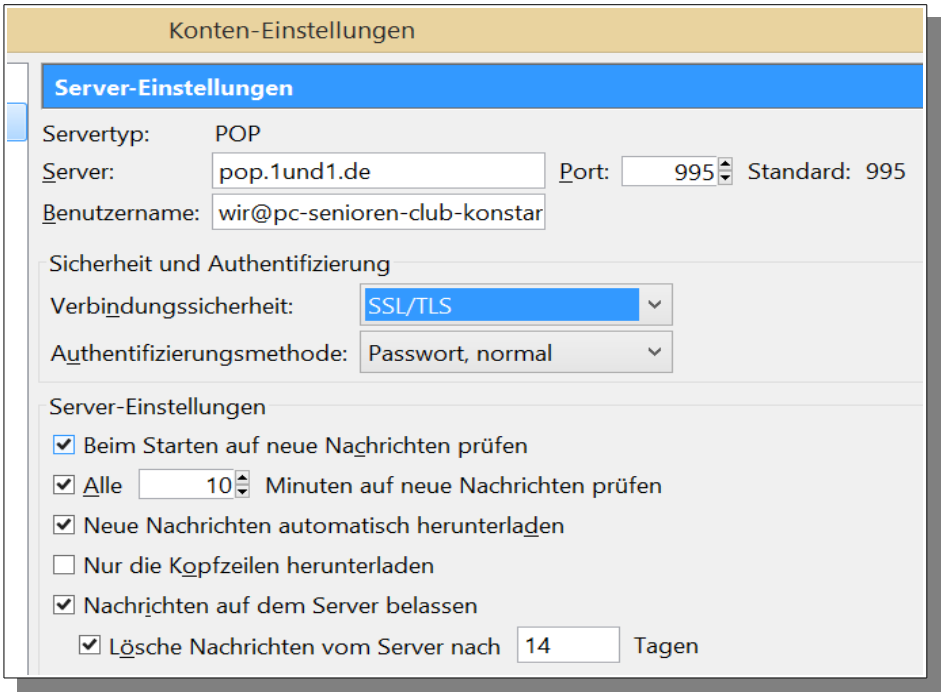
Computer und Zufallszahl: Das ist gar nicht selbstverständlich! Denn der Computer soll ja aus vorgegebenen Anfangsbedingungen mit höchster Präzision Ergebnisse errechnen, aber Anfangsbedingungen zu erzeugen ist nicht seine Sache. So kann der Computer (mit unserer Hilfe) einen riesigen Text gestalten, formatieren, übertragen, mit anderen Texten vergleichen – aber einen kreativ Text erzeugen kann er nicht. Und mit der "Kreation" von Zufallszahlen hat er auch Schwierigkeiten und benutzt daher oft dazu den chaotischen Menschen. Zum Beispiel werden Sie aufgefordert, die Maus frei herum zu bewegen und der Computer benutzt die Koordinaten des Mauspfeils zur Erzeugung einer Zufallszahl.

Dieser Zwang zum Zufall birgt eine Gefahr. Wenn sich beim Zufall irgend eine *Systematik* einschleicht und erraten werden kann, hilft die beim Erahnen des Schlüssels. Schließlich: Was nützt

die sichere Übertragung eines Schlüssels, wenn der sich leicht erraten lässt? Tatsächlich gibt es etliche Beispiele für automatisch generierte, nur scheinbar zufällige Schlüssel und Codewörter.

Genau wie bei der Primzahlzerlegung, die im Kapitel "Der nächste Schritt: Rivet, Shamir und Adleman – RSA Verfahren, 1977" erwähnt ist hilft der Wettlauf mit der Zeit. Je besser die Zufallszahlen sind (Länge, keinerlei Systematik, häufige Änderung) desto länger würde die Kryptanalyse dauern. Der geheime Vorgang wäre dann evemntuell schon abgeschlossen und nicht mehr beeinflussbar.

7 TLS Verschlüsselung bei E-Mails



TLS bedeutet **Transport Layer Security** (**TLS**; deutsch *Transportschichtsicherheit*) und ist auch bekannt unter der Vorgängerbezeichnung **Secure Sockets Layer** (**SSL**). Die "Transportschicht" ist ein Teil des außerordentlich komplexen Programmpaketes für den Datenaustausch über das Internet und sorgt dafür, dass Datenpakete wieder in die richtige Reihenfolge gebracht werden, wenn sie auf unterschiedlich schnellen Wegen übertragen wurden, es fordert die Wiederholung verlorener oder verstümmelter Datenpakete an und kann vorübergehend unterbrochene Übertragungen wieder fortsetzen.

Eine TLS-Verschlüsselung wird heute mit **HTTPS** (Zugriff auf Internetseiten), **POP3** und **IMAP** (E-Mail empfangen) , **SMTP** (E-Mail senden), NNTP, SIP, XMPP, IRC, LDAP, MBS/IP, FTP, EAP-TLS, TN3270 und OpenVPN.
Verschlüsselte Übertragungen benutzen eigene "Ports", der Standard ist meist voreingestellt und wird *im Mailprogramm angezeigt*

SMTP auf Port 25 bzw. 587 und SMTPS auf Port 465
IMAP auf Port 143 und IMAPS auf Port 993
POP3 auf Port 110 und POP3S auf Port 995

8 WIE FUNKTIONIERT TLS?

Der **Client**, also das Mailprogramm in Ihrem PC, baut eine Verbindung zum Server, der die Mails von Ihnen und für Sie sammelt, auf. Für gewöhnlich **authentifiziert sich zuerst der Server** gegenüber dem Client mit einem **Zertifikat**. Danach schickt entweder der Client dem Server eine

mit dem öffentlichen Schlüssel des Servers verschlüsselte geheime **Zufallszahl**, oder die beiden Parteien berechnen mit dem **Diffie-Hellman-Schlüsselaustausch** ein gemeinsames Geheimnis. Aus dem Geheimnis wird dann ein kryptographischer Schlüssel abgeleitet. Dieser Schlüssel wird in der Folge benutzt, um alle Nachrichten der Verbindung mit einem **symmetrischen Verschlüsselungsverfahren** zu verschlüsseln.

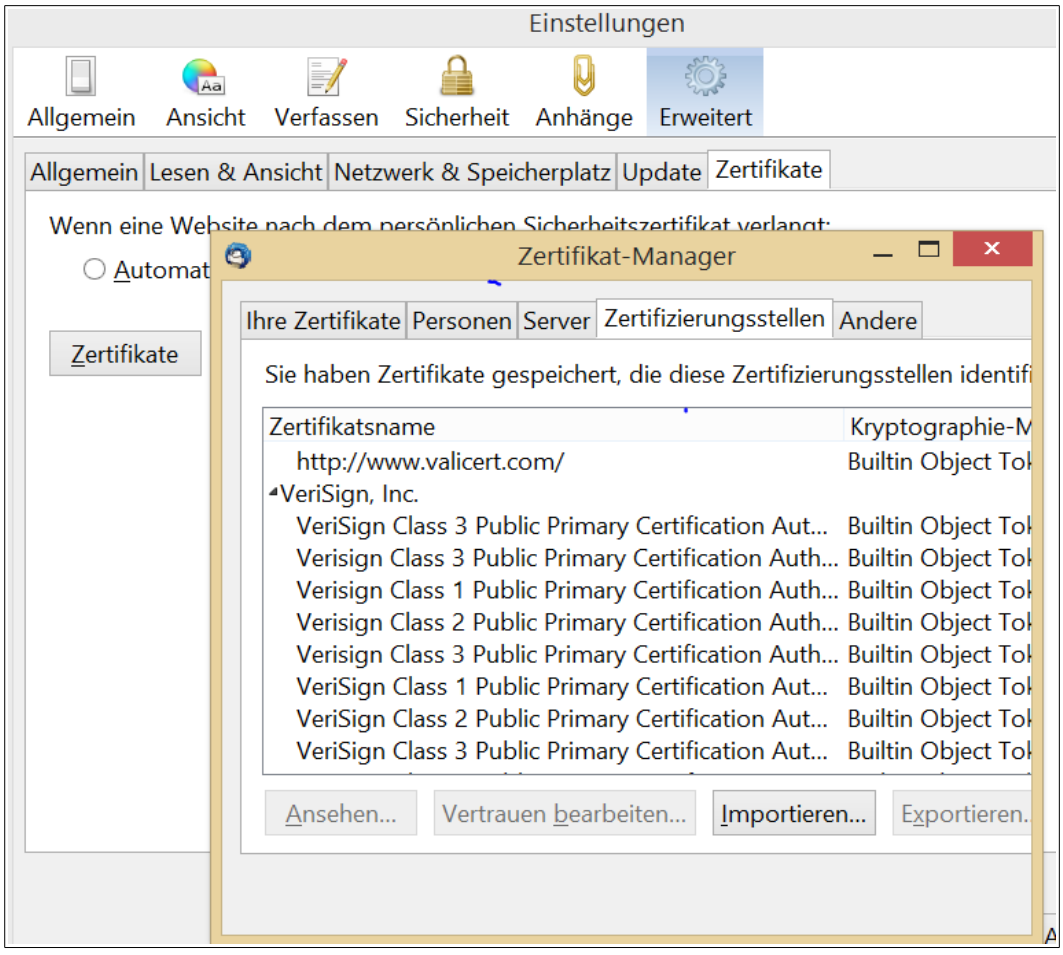
Die Authentifizierung des Absenders wird nicht durch ein weiteres asymmetrisches Verfahren sondern einfach durch das Paar Benutzername + Passwort erreicht.

9 Digitales Zertifikat

Wie wird sichergestellt, dass der öffentlicher Schlüssel von A tatsächlich von A stammt? Das wird durch ein **digitales Zertifikat** bestätigt. Es wird von **Zertifizierungsfirmen** in unterschiedlichen Qualitäten angeboten.

> Ein kostenloses Zertifikat bekommt man schon durch bloße Angabe einer Mailadresse, ein hochwertiges Zertifikat einer Bank kann den persönlichen Einsatz zweier Prokuristen mit Personalausweisen erfordern.

Zertifizierungsstellen (Beispiel Thunderbird)



Die Firma Versisign dürfte Marktführer sein.

Interessant ist es, die im Zertifikat Manager angegebenen Firmen anzusehen. Ein Doppelklick auf einen Eintrag enthüllt vielerlei, z. B. Name und Ort der Firma. Die Liste der Zertifizierungsstellen und ihrer Zertifikate wird mit der jeweils neuen Version des Mailprogramms mitgeliefert, man kann sie aber auch selbst ändern: Zertifizierungsstellen hinzufügen, entfernen oder in ihrem

Wirkungsbereich (Mail, Browser...) einschränken.

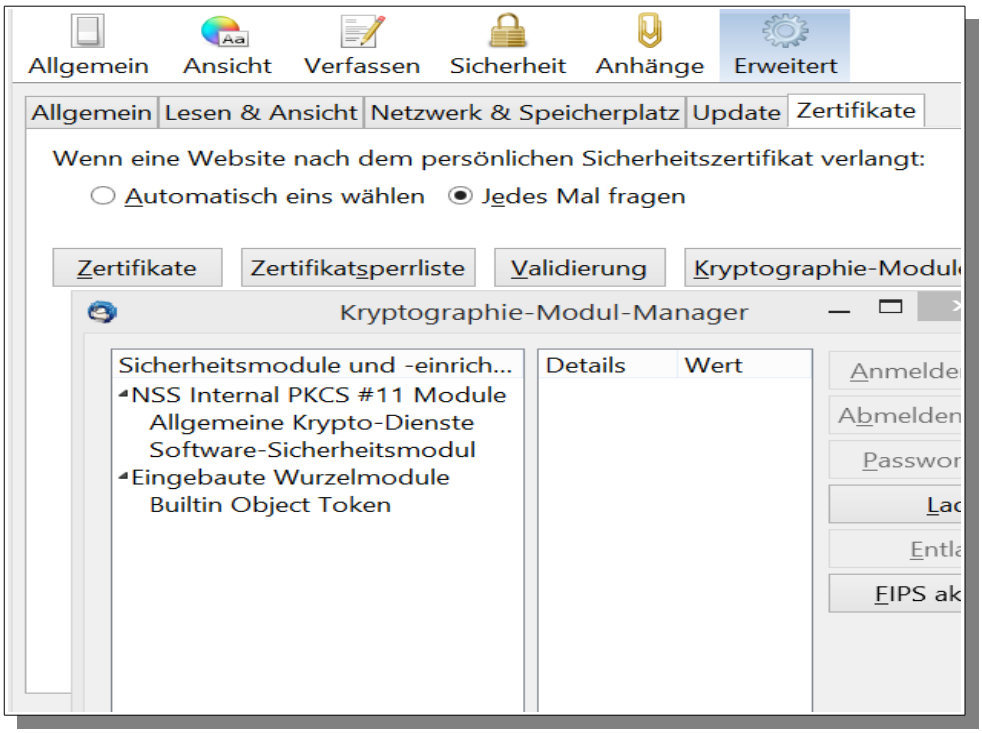
Praktisch können wir uns nur auf die Entwickler der Mailprogramme *und die Updates* verlassen und müssen nichts ändern.

Kryptographie-Module

Browser und Mail-Programme und die entsprechenden Programme der Kommunikationsfirmen sind schon lange für mehrere verschlüsselte Übertragungen mit Zertifikatverwaltung und Kryptographie.Modulen eingerichtet, das wurde aber bisher nicht vorgeschrieben und daher im Privatbereich selten verwendet.

Thunderbird enthält einen Kryptographie-Modul Manager (Bild).

Dieses Thema ist komplex und müsste – wenn überhaupt - in einem eigenen Vortrag behandelt werden.



10 Geheim!

James Ellis im GCHQ (Government Communication Headquarter), dem Britischen Geheimdienst, hatte schon in den 1960er Jahren die Idee der asymmetrischen Verschlüsselung und Clifford Cocks, Mathematiker und ebenfalls Mitarbeiter im GSHQ, hatte 1973 die mathematische Lösung beigesteuert. Das wurde Verfahren aber als Top Secret eingestuft und nicht weiter verfolgt. Erst 1997, als RSA schon lange patentiert war und damit schon gutes Geld verdient wurde, erlaubte die Regierung eine Bekanntgabe der Arbeiten von Ellis und Cocks und ermöglichte damit eine späte Anerkennung für die britischen Entwickler.
Die Reaktion des GCHQ war aber verständlich! Ihre Aufgabe war das Ausspionieren und Entschlüsseln und ist es heute noch, s. Datenschutz und NSA. Eine Veröffentlichung des Verfahrens hätte die Arbeit des GCHQ erschwert, denn es wäre auch dem Feind zur Verfügung gestanden....

11 PGP

Phil Zimmermann war der Meinung, dass die wirkungsvolle Methode RSA nicht nur dem Militär, den Geheimdiensten und den Banken vorbehalten bleiben sollte, sondern von jedermann zum Schutz seiner privaten Korrespondenz benutzt werden sollte. Er entwickelte 1991 ein

Programmpaket, dass auf jedem PC laufen sollte und mit dem jedermann Daten verschlüsselt übertragen konnte. Es heißt "**pretty good privacy" (PGP).**

Das brachte ihn in Teufels Küche.

- Die Geheimdienste wie NSA, die schon damals alles abhörten und alle E-Mails mitlasen (das war bekannt, es ist in der Literatur nachzulesen. Warum kam das jetzt erst plötzlich hoch?) reagierten prompt. Ein Antrag wurde gestellt *"Der Kongress hält es für erforderlich, dass Anbieter elektronischer Kommunikationsdienste und die Hersteller elektronischer Kommunikationsgeräte garantieren, ihre Kommunikationssysteme so auszustatten, dass die Klartextinhalte von Telefongesprächen, Datenübertragungen und anderen Mitteilungen den staatlichen Behörden zur Verfügung gestellt werden können, sofern hierzu eine gesetzliche Erlaubnis vorliegt."*
- Zimmermann wurde wegen Exports von Rüstungsgütern an Feindstaaten angeklagt
- Er bekam Probleme mit dem Patentschutz von RSA

Wie es weiter ging? Dazu gibt es spannende Literatur s. 13, PGP ist auch heute verfügbar, das Programm ist für den Privatgebrauch kostenlos.

> *Wir haben vor einigen Jahren im Club einen Versuch gemacht, PGP zum Verschlüsseln von Mails zu benutzen. Wir verwendeten PGP als End-to-End Verschlüsselung, d. h. beide Partner mussten ihren Schlüssel (privat oder öffentlich) kennen und verwalten. Das war sogar sicherer als der heute übliche Verfahren, auf den Teilstrecken verschlüsseln. Es war aber umständlicher, da auf jedem PC die Schlüssel aller Mail-Empfänger im Adressbuch zu verwalten waren. Übrigens protestierten damals schon die Virenschutzprogramme auf den PCs, sie konnten ja verschlüsselte Mails nicht kontrollieren. Wieso ist das heute kein Problem? Was hat sich geändert?*

12 Ein Literaturhinweis:

Eine Fundgrube ist das Buch von Simon Singh "Geheime Botschaften".

13 Links

http://de.wikipedia.org/wiki/Transport_Layer_Security
http://de.wikipedia.org/wiki/Digitales_Zertifikat
http://de.wikipedia.org/wiki/RSA-Kryptosystem
http://de.wikipedia.org/wiki/Symmetrisches_Kryptosystem
http://de.wikipedia.org/wiki/Extended-Validation-Zertifikat
http://wiki.hackerboard.de/index.php/Pretty_Good_Privacy
http://de.wikipedia.org/wiki/Pretty_Good_Privacy

14 Weitere Themen im Zusammenhang mit Cryptologie (für eventuelle weitere Vorträge)

- Daten in der **Dropbox verschlüsseln**
- Daten **auf dem eigenen PC verschlüsselt** ablegen, Partitionen verschlüsseln
- **Zertifikate**
- **Mail und Viren**: Was geschieht genau beim Mailempfang? Schützt die Einstellung "Nur Kopfzeilen herunterladen" sicher vor Viren? Kann schon das Anschauen einer Mail gefährlich sein, ohne dass Sie etwas anklicken oder die Anlage anfordern - oder ist das nur ein Gerücht? Wenn vor einer Mail gewarnt wird: Wer warnt und warum? Wegen Virus, Copyrightverletzung, Pornografie, Anleitung zu Straftaten, ...?