Inhaltsverzeichnis

Seit jeher versuchten Menschen Informationen vor anderen Personen geheim zu halten. In vielen Fällen gelang dies, wenn auch meist nur für eine bestimmte Zeitdauer. Daraus ziehe ich den Schluss, dass beim Verschlüsseln (Chiffrieren) von Informationen die Zeit, in welcher der Schutz gewährleistet ist, eine wichtige Rolle spielt. Informationen werden beim Übermitteln hauptsächlich durch Chiffrieren geschützt.

Chiffrieren trifft dort auf Grenzen, wo Informationen berechtigterweise mehreren Personen zu unterschiedlichen Zeitpunkten zur Verfügung stehen müssen und somit der Zugriffsmechanismus mehreren Personen zur Verfügung stehen muss.

Das grösste Risiko beim Chiffrieren liegt darin, dass man sich im allgemeinen auf deren Schutzwirkung verlässt, ohne zu wissen, ob dieses Vertrauen gerechtfertigt ist. Unter Umständen kann es relativ lange dauern, bis man merkt, dass die Verschlüsselung geknackt wurde. Die Wahrscheinlichkeit, dass dies eintrifft, steigt mit der Zeitdauer, während der verschlüsselte Informationen ohne weitere Schutzmassnahmen gespeichert werden. Weiter steigt die Wahrscheinlichkeit mit der Zeit, dass der benützte Schlüssel nicht mehr zur Verfügung steht. Da auch Speichermedien einer Alterung unterliegen und Verschlüsselung sehr empfindlich reagiert, kann eine verschlüsselte Information eventuell gar nicht mehr entschlüsselt werden.

1. Alphabetische – Verfahren

1.1. Anfänge

Die brutalste Art des Informationsschutzes bestand darin, dass der Meldeläufer nach der Erfüllung seiner Mission aus Gründen der Sicherheit das Zeitliche segnete. Dass diese Art der Übermittlung schnell an die Grenzen des Machbaren stösst, leuchtet wohl jedem ein.

1.2. Das Caesar – Verfahren

Der Feldherr Caesar schützte seine Informationen, indem Buchstaben durch andere Buchstaben ersetzt wurden. Dabei ging Caesar davon aus, dass nur der Empfänger (alleine) wusste, um wie viele Buchstaben der Text verschoben wurde.
Auf diese Weise erhielt zum Beispiel in Film „Odyssee 2000" der Computer seinen Namen. Er hiess HAL, sprich IBM.

Die Schwächen dieses Verfahrens liegen auf der Hand. Wenn man weiss, dass je nach Sprache gewisse Zeichen mehr oder weniger häufig auftauchen, ist die Verschiebung relativ leicht herauszufinden.

1.3. Das modifizierte Caesar Verfahren

Auf Grund dieser Erkenntnis wurden nicht mehr alle Buchstaben um eine bestimmte Anzahl Zeichen verschoben, sondern jedes Zeichen durch ein anderes ersetzt, ohne die ursprüngliche Reihenfolge beizubehalten. Zudem wurden die verwendeten Tabellen regelmässig gewechselt.

Der Nachteil dieses Verfahren liegt auf der Hand. Der Empfänger muss über die verwendete Tabelle verfügen können. Gegenüber dem einfachen Caesar Verfahren hat sich in Sachen Sicherheit nicht viel geändert, da auch hier auf Grund der Häufigkeit der vorkommenden Zeichen relativ schnell der Inhalt der Information herausgefunden werden kann.

1.4. Geheimcode des Sir Francis Bacon (1623)

Sir Francis Bacon hat jedem Buchstaben des Alphabetes eine Kombination von insgesamt fünf „a" und „b" zugeordnet.

A	B	C	D	E	F
aaaaa	aaaab	aaaba	aaabb	aabaa	aabab
G	**H**	**I**	**K**	**L**	**M**
aabba	aabbb	abaaa	abaab	ababa	ababb
N	**O**	**P**	**Q**	**R**	**S**
abbaa	abbab	abbba	abbbb	baaaa	baaab
T	**U**	**V**	**W**	**X**	**Y**
baaba	baabb	babaa	babab	babba	babbb
Z					
bbaaa					

Können Sie folgende Geheimmeldung entziffern?

„schwARze tulpe erWaRtet AntW!"

Sir Francis Bacon realisierte bei der Festlegung seines Codes vermutlich nicht, dass er damit das erste Beispiel eines fünfstelligen Binärcodes beschrieb, ohne den die moderne Informatik undenkbar wäre. Binär heisst der Code deshalb, weil er nur zwei Symbole verwendet, a und b.

Lassen Sie sich durch die obige Geheimmeldung nicht täuschen; Sie enthält zwar 31 verschiedene Buchstaben, beim genaueren Hinsehen aber nur zwei Buchstabensorten!

```
„schwA Rzetu lpeer WaRte tANtW !

 aaaab baaaa aaaaa babaa abbab
 B     R     A     V     O     !
```

1.5. Krummenacher

Eine weitere Möglichkeit wäre Information nach einem gewissen Plan in einem Gitter abzulegen:

U	A	S	E	I	R	S	I	E	S
R	N	S	R	N	H	T	S	L	S
3	T	A	E	T	E	S	E	N	E
H	C	S	A	E	U	N	E	E	U
L	S	V	D	B	T	T	R	R	F
U	R	E	R	E	X	E	H	I	K
D	N	B	I	R	R	T	R	R	H
A	E	E	L	K	E	E	H	G	E
N	T	S	R	A	H	R	E	E	S

Der Einfachheit halber ist oben links der Schlüssel aufgeführt „UR3". Dieser steht normaler weise nicht im von Herrn Krummenacher vorgeschlagen Verfahren.„UR3" bedeutet, dass unten rechts begonnen wird und anschliessend schlangenartig durch das Gitter gelesen wird. Satzzeichen und Lehrstellen fehlen:

```
SEHR GEEHRTER HERR KARLI BESTEN DANK FUER IHREN TEXT UEBER DAS
VERSCHLUESSELN ES IST SEHR INTERESSANT
```

Diesen Verfahren ähnelt dem Verschleierungsverfahren, bei welchem ein Band um einen Stab mit einem bestimmten Durchmesser gewickelt wurde und der Text in der Richtung des Stabes auf dieses Band aufgeschrieben wurde. Der ursprüngliche Text, war natürlich nur zu Lesen, wenn das Band erneut auf einen Stab mit dem gleichen Durchmesser aufgerollt wurde.

Das Risiko bei diesen Verfahren liegt im Verfahren selber. D.h. in der Anweisung, wie die Information zu verschleiern ist.

2. Mechanische Verfahren

Relativ frühzeitig wurden Verschlüsselungsverfahren eingesetzt, welche mit mechanischen Apparaten unterstützt wurden. Wesentlich dabei war, dass es dabei immer noch ein Austauschen von Buchstaben - jedoch nach einem ausgeklügelten Verfahren - handelt. Das berühmteste Gerät ist wohl die „Enigma", welches von der deutschen Wehrmacht im zweiten Weltkrieg verwendet wurde. Mit diesem Gerät wurden noch Meldungen verschlüsselt, obschon die Alliierten den Kode schon kannten und so die Meldungen ebenfalls entschlüsseln konnten.

3. Elektronische Verfahren

3.1. Allgemeines

Die Verbreitung und Entwicklung der elektronischen, programmierbaren Rechenmaschinen (Computer) bieten optimale Voraussetzungen für das Chiffrieren von Informationen. Damit steigt auf der anderen Seite jedoch auch das Risiko, dass solche Verfahren geknackt werden können.

3.2. Mathematische Grundlagen

Um die elektronischen Verfahren verstehen zu können, kommt man nicht darum herum, sich minimale Kenntnisse auf dem Gebiete der Logik anzueignen. Wie der Name sagt, sollten die erklärten Methoden logisch sein und damit hoffentlich auch verstanden werden können. Ein weiterer Name, welcher in diesem Zusammenhang auftaucht, ist die Binäre oder Boolesche Mathematik. Binär sagt aus, dass zwei Zustände möglich sind (Wahr / Falsch bzw. Ja / Nein oder 1 / 0.).

3.2.1. Binäre Ziffern

Mit einer binären Stelle (Bit = Binary digIT) können zwei Zustände dargestellt werden. Mit jeder weiteren Stelle verdoppeln sich die Möglichkeiten, wie dies in der folgenden Tabelle aufgezeigt ist:

Tabelle 1 Binäre Ziffern

Stellen		Möglichkeiten
1	0 - 1	2
2	00 01 10 11	4
3	usw.	8
4		16
5		32
6		64
7		128
8		256
9		512
10		1024
11		2048
12		4096
13		8192
14		16384
15		32768
16		65536
17		131072
18		262144
19		524288
20		1048576

Mit Logarithmieren kann die Grössenordnung der gegebenen Möglichkeiten relativ einfach abgeschätzt werden:

$2^{x} = 10^{x * \log(2)}$.

Als Beispiel

$2^{10} = 10^{10 * \log(2)}$
$= 10^{10 * 0.30102}$
$= 10^{3.0103}$
$= 10^{3} * 10^{0.0103}$
$= 1'000 * 1.024$

$2^{20} = 10^{20 * \log(2)}$
$= 10^{20 * 0.30102}$
$= 10^{6.0206}$
$= 10^{6} * 10^{0.0206}$
$= 1'000'000 * 1.048$

Zur Erinnerung

2^{10} werden als 1 K bezeichnet und haben mit 1 kg (einem Kilogramm) wenig zu tun, obschon es auch 1 Kilo ausgesprochen wird.
2^{20} werden als 1 M, ein Mega
2^{30} (1'073'741'824) werden als 1 G, Giga bezeichnet.

Dazu zwei Beispiele:

Schach: Der chinesische Fürst, welcher das Schach - Spiel in Auftrag gegeben hatte, war derart entzückt, dass er dem Erfinder die Erfüllung eines Wunsches in Aussicht stellte. Der Erfinder forderte für das erste Feld 1 Reiskorn, für das zweite 2 Reiskörner, für das dritte 4 Reiskörner, usw. Der chinesische Fürst war von der Bescheidenheit des Erfinders überrascht und ordnete Erfüllung des Wunsches an. Leider konnte bis heute dieser Auftrag nicht realisiert werden. Es hätten nämlich $2^{64} - 1$ Reiskörner geliefert werden müssen. Angenommen 1 Reiskorn wiege 1 gr – so hätte ca. 10^{20} gr bzw. 10^{17} Kg bzw. 10^{14} Tonnen Reis geliefert werden müssen.

Papierfalten: Angenommen Sie hätten ein Papier der Stärke von 1/8 mm, welches sich beliebig falten liesse. Nach dreimaligem Falten hätte der Stapel 1 mm Höhe erreicht, ein weiteres Mal ergäbe 2 mm usw. Nach weiteren 60 mal wäre die Höhe auf ca. 10^{18} mm bzw. 10^{15} m bzw. 10^{12} km angewachsen.

3.2.2. Binäre Entsprechungen

Mit 4 Bit können 16 verschiedene Werte dargestellt werden: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F. Diese Zeichen umfassen den Hexadezimal - Kode. Um auch Buchstaben verwenden zu können, müssen neben den Ziffern auch Buchstaben berücksichtigt werden. Daraus entstand im Zusammenhang mit dem Telex - Verkehr ein 5 - Bit Telex - Code. Grosse und kleine Zeichen wurden erst durch Umschaltzeichen angezeigt. Später wurde der Code so erweitert, dass zwischen grossen und kleinen Buchstaben unterschieden werden konnte. Dieser ASCII – Code (ASCII = American Standard Code for

Information Interchange) umfasst 7 Bit und bietet 128 Möglichkeiten. In diesem Standard ist genau festgehalten, welche binären Werte welchem Zeichen entsprechen. Dies ist einer der wenigen Standards, welcher weltweit gilt. Mit anderen Worten: Soll Information so gespeichert werden, dass sie auch nach langer Zeit noch gelesen werden kann, muss dies in ASCII erfolgen

Der ASCII - Code um 1 Bit ergänzt, um nationalen Zeichen berücksichtigen zu können. Daraus entstand als neue Einheit das Byte. Das Byte umfasst 8 Bit. Mittlerweile genügen 8 Bit zur Darstellung des Zeichensatzes nicht mehr und werden durch andere Verfahren dargestellt.

3.2.3. Binäre Operatoren

Ein Computer arbeitet binär. Dies spielt insbesondere beim Chiffrieren eine massgebende Rolle. Von ganz besonderem Interesse ist dabei das exklusive Oder (XOR), wobei das Resultat nur dann 1 ist, wenn die beiden beteiligten Teile unterschiedliche Werte aufweisen.

Tabelle 2 - Exklusives ODER - XOR

A	B	Resultat
0	0	0
1	0	1
0	1	1
1	1	0

Das exklusive Oder weist die Besonderheit auf, dass durch zweimaliges Anwenden der exklusives Oder – Funktion wieder der originale Wert erscheint.

D. H. wird das Resultat von A xor B erneut mit dem Wert B mit xor verknüpft, resultiert der Wert von A.

$$A = B \text{ xor } (B \text{ xor } A)$$

Tabelle 3 - Zweimaliges exklusives ODER

A	B	Res 1	B	Resultat
0	0	0	0	0
1	0	1	0	1
0	1	1	1	0
1	1	0	1	1

3.3. Vernam - Verfahren

In der Kryptologie wird die grundlegende Information als Klartext (plain text) bezeichnet. Diese Information kann auch als eine Folge einzelner Byte (Byte – Stream) und damit, da ein Byte aus 8 Bits besteht, auch als eine Folge von Bits (Bit - Stream) betrachtet werden. Beim Verfahren von Vernam werden nun die Bits eines Klartextes mit den Bits eines Schlüssels (Key – Stream) mit

xor verknüpft und ergeben so das Chiffrat (cipher text). Dieses Verfahren ist äusserst schnell und absolut sicher, wenn folgenden Bedingungen erfüllt sind:

- der verwendetet Schlüssel muss absolut zufällig sein
  (dies wird erreicht, indem elektronisch („weisses") Rauschen gespeichert wird),
- Sender und Empfänger müssen über den gleichen Schlüssel verfügen müssen
  und
- Der Schlüssel muss gleich lang wie die zu verschlüsselnde Information sein muss und darf nur einmal verwendet werden.

Die Problematik bei diesem Verfahren liegt darin, dass die beteiligten Partner (Sender und Empfänger) über einen identischen Schlüssel verfügen müssen.

Lange Zeit wurden Lochstreifen erzeugt und eine Kopie davon dem Partner übergeben. Da dieses Verfahren recht kompliziert ist, wurde nach Möglichkeiten gesucht, einen mathematischen Algorithmus als Key – Stream einzusetzen, welcher der Sicherheit des Vernam – Verfahrens möglichst nahe kommt.

3.4. Symmetrische Verfahren

Gesucht werden mathematische Algorithmen, welche auf Grund eines Schlüssels Information so verschlüsseln können, dass eine unberechtigte Entschlüsselung – wenn überhaupt – nur mit einem nicht vertretbaren Aufwand erfolgen kann. Aufgrund der steigenden Rechenleistung steigen natürlich auch die Anforderungen an solche Verschlüsselungsverfahren.

3.4.1. Schlüssellänge

Lange Zeit galt der amerikanische DES (Data Encryption Standard) mit einer Schlüssellänge von 56 Bit als defacto - Standard. Obschon für DES ursprünglich eine grössere Schlüssellänge vorgesehen wurde, wurde diese von den amerikanischen Sicherheitsbehörden auf 56 limitiert. Momentan sind - unter dem Aspekt der nationalen Sicherheit - in den Vereinigten Staaten Bestrebungen im Gang die bewilligte Schlüssellänge auf 40 Bit zu reduzieren (NSA – National Security Agency).

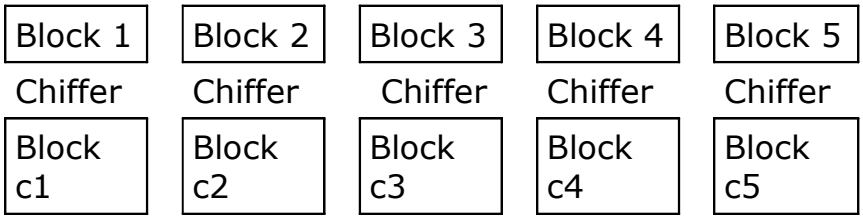
Heute gilt in der Lehre der Verschlüsselung (Kryptologie) eine Schlüssellänge von 128 Bit als absolutes Minimum, um Informationen ausreichend schützen zu können.

3.4.2. Verschlüsselungsverfahren

Neben der Schlüssellänge spielt auch das Verschlüsselungsverfahren eine wichtige Rolle.

3.4.2.1. ECB Electronic Code Book

Beim ECB (Electronic Cook Book) Verfahren wird jeder Block auf die gleiche Weise verschlüsselt. Mit anderen Worten liefern identische Blöcke identische Resultate.

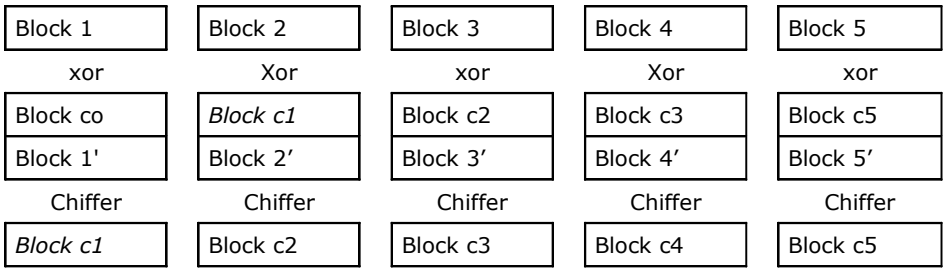


Unter anderen wird bei Datenbanken wahlfrei auf einzelne Datensätze zugegriffen. Dieser Zugriff erfolgt auf Massenspeichern (Platten) immer direkt über den betroffenen Sektor bzw. Cluster. Aus diesem Grund können Festplatten nur mit diesem Verfahren geschützt werden.

Dies kann unter gewissen Umständen gefährlich sein. Angenommen ein äusserst wichtiger Plan X mit einer Auflösung von 600 dpi (dot per inch) wird so verschlüsselt. Da dieser Plan zum Grossteil aus weissen Flächen und nur ein kleiner Teil aus schwarzen Strichen besteht, kann relativ einfach herausgefunden werden, welche Blöcke die weissen und welche die schwarzen Stellen darstellen. Aufgrund der hohen Auflösung enthalten z. B. die Blöcke 2, 3 und 4 nur weisse Stellen. Diese Blöcke sind völlig identisch. Dies trifft leider auch für die verschlüsselten Blöcke c2, c3 und c4 zu. Daher ergibt die Analyse des Chiffrates die ursprüngliche Information mit genügender Genauigkeit, ohne den Verschlüsselungsalgorithmus und den entsprechenden Schlüssel überhaupt kennen zu müssen.

3.4.2.2. CBC Cipher Block Chaining

Beim Chiffrieren eines Klartextes kann die Information noch zusätzlich geschützt werden, indem die Blöcke so verändert werden, indem sie mit dem Resultat des letzten Verschlüsselungsblockes verknüpft werden (CBC - Cipher Block Chaining).



Wird der oben erwähnte Plan X so verschlüsselt, liefert obiges „Entschlüsselungsverfahren" kein brauchbares Resultat mehr.

3.4.2.3. Komprimieren

Informationen werden hauptsächlich zum Übermitteln verschlüsselt. Um die Übermittlungszeit klein zu halten, werden Informationen vor dem Verschlüsseln meist komprimiert.

3.4.3. Verschlüsselte Übermittlung mit symmetrischem Verfahren

Tabelle 4 - Symmetrische Verschlüsselung

		Sender A		Empfänger B	
A1	Word	PlainText			
A2	ZIP	Comprimat			
A3	IDEA(KEY)	Chiffrat			
U1			Übermittlung		
B3				Chiffrat	IDEA(KEY)
B2				Comprimat	UnZIP
B1				PlainText	Word

Der Absender A

A1: erstellt die Information (z. B. mit Word),

A2: komprimiert diese Information A1 (z. B. mit PkZIP)

und

A3: chiffriert diese komprimierte Information

(z. B. mit IDEA und einem entsprechenden Schlüssel KEY).

Das Chiffrat wird nun übermittelt (U1).

Der Empfänger B führt nun diese Tätigkeiten in umgekehrter Reihenfolge aus. Er

B3: entschlüsselt das erhaltene Chiffrat
(damit der Empfänger das Chiffrat entschlüsseln kann, muss er über den gleichen Schlüssel KEY verfügen, mit dem der Absender die komprimierte Information chiffriert hat)

B2: entkomprimiert die komprimierte Information

und

B1: kann nun die Information lesen.

Bei diesem Verfahren ist sichergestellt, dass nur jemand, welcher über den Schlüssel KEY verfügt, diese Information verschlüsselt oder entschlüsseln kann. Nichts mehr und nichts weniger. Es wird keine Aussage gemacht, ob er berechtigt oder nicht berechtigt im Besitz dieses Schlüssels ist.

Eine Schwachstelle dieses Verfahren ist, dass der Schlüssel ausgetauscht werden muss. Sobald mehr als eine Person über einen Schlüssel verfügt, kann nicht mit Sicherheit garantiert werden, dass die jeweiligen Besitzer alles vermeiden, dass der Schlüssel abhanden kommt.

Gelangt der Schlüssel in unberechtigte Hände, kann die Information entschlüsselt, eingesehen und im schlimmsten Fall verändert und neu verschlüsselt werden. Dies ist äusserst gefährlich, da der berechtigte Empfänger in –den seltensten Fällen feststellen kann, dass die Information manipuliert wurde. Im Gegenteil man verlässt sich darauf, dass chiffrierte Informationen geschützt sind.

Eine weitere Schwachstelle ist die Verwendung der Schlüssel, das Key – Management. Im Interesse der Sicherheit sollten Schlüssel nur einmal verwendet – „one time session key". Aus praktischen Gründen werden Schlüssel oft längere Zeit benutzt.

Da bei der ausschliesslichen Verwendung von asymmetrischen Schlüsseln bei der Übermittlung keine praktikablen Lösungen bestehen, müssen andere Verfahren verwendet werden.

3.5. Asymmetrische Verfahren

3.5.1. Asymmetrische Verschlüsselung des Schlüssels

Beim asymmetrischen Verfahren existieren zwei zusammenpassende Schlüssel: ein geheimer, persönlicher Schlüssel (Private Key) und ein öffentlicher Schlüssel (Public Key). Sind die öffentlichen Schlüssel einmal auf einem vertrauenswürdigen Weg unter den Beteiligten verteilt, steht mit dem "asymmetrischen Verfahren" ein elegantes Verfahren zur Verfügung, welches neben dem Schutz des Schlüsselaustausches noch weitere Möglichkeiten bietet.

Mit diesem Verfahren wird sichergestellt, dass eine Meldung, welche mit dem öffentlichen Schlüssel einer Person verschlüsselt wurde, nur mit dem persönlichen Schlüssel dieser Person entschlüsseln kann bzw. kann eine Meldung, welche mit einem persönlichen Schlüssel verschlüsselt werden, von allen, welche über den zugehörigen öffentlichen Schlüssel verfügen, entschlüsselt werden.

Das bekannteste Verfahren heisst RSA - Verfahren (nach seinen Erfindern Rivest, Shamir und Adleman). Das Verfahren gewährleistet, dass aus der Kenntnis des öffentlichen Schlüssels nicht auf den entsprechenden geheimen Schlüssel geschlossen werden kann.

Da die asymmetrischen Verfahren relativ rechenintensiv sind, werden Informationen (bzw. deren Komprimate) mit einem zufälligen Schlüssel („one time session key") symmetrisch chiffriert und lediglich dieser Schlüssel asymmetrisch verschlüsselt.

Tabelle 5 - Asymmetrische Verschlüsselung

		Sender A		Empfänger B	
A1	Word	PlainText			
A2	ZIP	Comprimat			
A3	IDEA(KEY)	Chiffrat			
A4	RSA(PubB)	KEY			
U1			Übermittlung		
B4				KEY	RSA(PriB)
B3				Chiffrat	IDEA(KEY)
B2				Comprimat	UnZIP
B1				PlainText	Word

Mit diesem Verfahren verschlüsselt der Absender den verwendeten symmetrischen Schlüssel „KEY" mit dem öffentlichen Schlüssel des Empfängers „PubB". Nur der Empfänger B kann den symmetrischen Schlüssel KEY entschlüsseln, da nur er über den entsprechenden geheimen, privaten Schlüssel „PriB" verfügt (oder zumindest nur er über diesen Schlüssel verfügen sollte). Der Empfänger hat bei diesem Verfahren keine Gewissheit, wer ihm diese Information übermittelt hat. Jeder, der über den öffentlichen Schlüssel von „B" (PubB) verfügt, kommt als Absender in Frage.

3.5.2. Digitale Signatur

Das asymmetrische Verfahren bietet noch eine weitere Möglichkeit. Genauso wie Informationen, welche mit einem öffentlichen Schlüssel verschlüsselt wurden, nur mit dem entsprechenden privaten Schlüssel entschlüsselt werden können, können Informationen, welche mit einem geheimen Schlüssel verschlüsselt wurden, nur mit dem entsprechenden öffentlichen Schlüssel wieder entschlüsselt werden.

Wenn der Absender eine weitere Meldung mit seinem geheimen Schlüssel (PriA) verschlüsselt, kann der Empfänger diese zusätzliche Meldung nur mit dem öffentlichen Schlüssel des Absenders (PubA) entschlüsseln.
Diese Meldung kann nur jene Person verschlüsselt haben, welche über den geheimen Schlüssel (PriA) verfügt.

Tabelle 6- Digitale Signatur

	Sender A		Empfänger B	
A1 Word	PlainText			
A2 ZIP	Comprimat			
A3 IDEA(KEY)	Chiffrat			
A4 RSA(PriA)	Meldung			
A5 RSA(PuB)	KEY			
U1		Übermittlung		
B5			KEY	RSA(PriB)
B4			Meldung	RSA(PubA)
B3			Chiffrat	IDEA(KEY)
B2			Comprimat	UnZIP
B1			PlainText	Word

Sinnvollerweise hängt diese zusätzliche Meldung in irgend einer Form mit der zu übermittelnden Information zusammen. Im allgemeinen wird dazu der Hashwert der Information verwendet. Eine Hashfunktion liefert für jede Information einen eindeutigen Wert. Wird dieser Hashwert als Meldung verwendet, kann der Empfänger zudem noch herausfinden, ob die übermittelte Information in irgend einer Weise verändert wurde, weil er ja selber diesen Wert (Hash B) berechnen und mit dem übermittelten Wert (Hash A) vergleichen kann.

Tabelle 7 - Digitale Signatur und Authentizität

	Sender A		Empfänger B	
A1 Word	PlainText			
A2 MD5	HashA			
A3 ZIP	Comprimat			
A4 IDEA(KEY)	Chiffrat			
A5 RSA(PriA)	Signatur			
A6 RSA (PubB)	Key			
U1		Übermittlung		
B6			Key	RSA(GeB)
B5			HashA	RSA(PuA)
B4			Chiffrat	IDEA(KEY)
B3			Comprimat	UnZIP
B2			HashB	MD5
B1			Plain Text	Word

3.5.3. Digitale Quittung

Zur Vollständigkeit fehlt nur noch, dass der Absender im Moment noch über keine Quittung verfügt, dass er diese Information an den Empfänger versandt hat und dieser die Information auch entschlüsselt hat. Auch dies lässt sich mit dem asymmetrischen Verfahren relativ einfach erledigen. Der Empfänger muss lediglich den Hash – Wert der Information (HashB, der ja mit dem entschlüsselten Hash – Wert HashA übereinstimmen muss) mit seinem geheimen Schlüssel verschlüsselt an den Absender zurückschicken, womit der Sender aufzeigen kann, dass dieser Hash - Wert vom Empfänger nur in Kenntnis seiner ursprünglichen Information erstellt werden konnte.

Tabelle 7 - Digitale Quittung

	Sender A		Empfänger B	
A1 Word	PlainText			
A2 MD5	Hash A			
A3 ZIP	Comprimat			
A4 IDEA(KEY)	Chiffrat			
A5 RSA(PriA)	Signatur			
A6 RSA(PubB)	Key			
U1		Übermittlung		
B6			Key	RSA(PriB)
B5			Hash A	RSA(PubA)
B4			Chiffrat	IDEA(KEY)
B3			Comprimat	UnZIP
B2			Hash B	MD5
B1			PlainText	Word
B7			Hash	RSA(PriB)
U2		Übermittlung		
A7 RSA(PubB)	Hash			

3.5.4. Elektronische Beglaubigung

Einigen sich die Partner auf eine dritte vertrauenswürdige Stelle (Third Thrusted Party), kann die Archivierung der so erstellten und geschützten Hash - Werte bei dieser Stelle jederzeit den elektronischen Beweis antreten, dass der Absender diese Information gesandt und der Empfänger diese gelesen hat. Dabei braucht diese vertrauenswürdige Stelle gar keine Kenntnis der betreffenden Information zu haben - die entsprechend verschlüsselten Hashwerte genügen.

Zu der Hashfunktion ist zu sagen, dass jede Information einen eindeutigen Hashwert liefert, aber auf Grund des Hashwertes nie auf die ursprüngliche Information geschlossen werden kann.

4. Ausblick

4.1. Trends, Zukunft

4.1.1. Steganographie

Wie die Geheimdienste vergangener Zeiten Informationen mittel Mikroverfilmung in unverfänglichen Texten eingefügt wurden, geht man heute vermehrt dahin Informationen in einem digitalen Bild unterzubringen, indem zum Beispiel jedes 100 Bit zur versteckten Information und nicht zum Bild gehört. Man kann sich selber vorstellen, dass dieser „Missbrauch" bei einer angenommenen Auflösung von 600 dpi (dots per inch) nicht auffällt. Um in dieser Art 6000 Zeichen (Bytes) zu verstecken, braucht es nur einen Ausschnitt von ca. 2.5 mal 25.0 cm. Zum Vergleich sei darauf hingewiesen, dass auf normales Papier mit einer 10 - er Schaltung maximal 80 Zeichen pro Zeile und pro Seite maximal 70 Zeilen, d. h. 5600 Zeichen geschrieben werden können.

4.1.2. Rauschen

Das auf der akustischen Seite die Zeit nicht stillgestanden ist, kann man sich denken. Beispielsweise wäre ein analoges Verfahren zur Steganographie auch hier möglich.

5. Wo steht die Kryptologie heute

Abschrift des Artikels von Dr. Peter Nyffeler, Chef Sektion Kryptologie der Untergruppe Führungsunterstützung in Mosaik 87/88.

Die klassische Aufgabe der Kryptologie besteht darin, einen geheimen Text so zu übermitteln, dass er nur vom befugten Empfänger gelesen werden kann. Dabei steht Text zusammenfassend auch für Sprache, Bild, Daten usw. Mit zunehmender Vernetzung kamen Aufgaben wie Authentifikation, digitale Unterschrift dazu. Kryptologische Verfahren leisten einen wesentlichen Beitrag zur Lösung dieser Aufgaben. In einem ersten Teil befassen wir uns mit der ursprünglichen Hauptaufgabe, der Gewährleistung der Vertraulichkeit. Der nächste Teil wird sich mit Lösungsansätzen bei digitalen Unterschriften, elektronischem Handel usw. auseinandersetzen. Dabei sind unsere Ausführungen nicht nur auf spezifisch militärische Anwendungen beschränkt.

5.1. Kryptologie

Die Kryptologie befindet sich im Spannungsfeld zwischen Kryptographie und Kryptonanalysis, zwischen dem Entwickler – dem „Designer" – und dem „Knacker".

5.1.1. Kryptographie

Aufgabe der Kryptographie oder des Designers ist es, den Klartext zusammen mit dem Chiffrierschlüssel in das Chiffrat zu transformieren, so dass die Rücktransformation in den Klartext nur in Kenntnis des Dechiffrierschlüssels möglich ist.

Der Prozess der Transformation – die Chiffrierung oder des Chiffrieralgorithmus – muss schnell sein; die Rücktransformation – die Dechiffrierung oder der Dechiffrieralgorithmus – soll ebenfalls schnell sein und darf nur bei Kenntnis des Dechiffrierschlüssels gelingen. Die beiden Schlüssel, Chiffrier- und Dechiffrierschlüssel, können gleich sein; mindestens der Dechiffrierschlüssel dar aber nur dem befugten Empfänger bekannt sein und ist daher geheim zu halten.

5.1.2. Kryptonanalysis

Die Aufgabe der Kryptonanalysis oder des Dektryptierers besteht darin, ohne Kenntnis des Dechiffrierschlüssels aus dem Chiffrat und Teilen des Klartextes den vollständigen Klartext und womöglich den Schlüssel zu bestimmen.

5.2. Kryptosystem

Unter einem Kryptosystem versteht man die angewandten kryptographischen Algorithmen und zusätzlich die Art ihrer Implementierung. Damit wird schon auf eine grundsätzliche Problematik hingewiesen, insbesondere wenn man an das weite Gebiet der Computer-Sicherheit denkt: Der Kryptograph kann zwar die Verantwortung für die gewählten Algorithmen übernehmen. Die Implementierung hängt aber stark vom Betriebssystem ab; deren Sicherheit lässt sich daher nur sehr schwer, falls überhaupt, überprüfen.

5.3. Chiffrierverfahren

5.4. „one-time pad"

Beim „one-time pad" wird als Chiffrierschlüssel und Dechiffrierschlüssel die gleiche geheime Zufallsfolge verwendet. Diese Zufallsfolge muss „echt" zufällig erzeugt werden, darf also insbesondere nicht reproduzierbar sein. Zudem darf die Zufallsfolge nur eine Übermittlung brauchen, da man sonst die Redundanz der Klartexte zur Dekryptierung ausnützen könnte.

Der „one-time pad" ist ein beweisbar sicheres Chiffrierverfahren nach dem Prinzip:

Klartext + Zufallsfolge = Zufallsfolge

(Anmerkung FJK: + bedeutet hier EXOR - Verknüpfung)

Damit wäre das kryptographische Hauptproblem ein für alle Mal gelöst. Diese absolute Sicherheit hat aber ihren Preis: Die Zufallsfolgen, die vorgängig ausgetauscht und geheimgehalten werden, müssen mindestens so lang sein wie der Klartext selbst. Dies ist in den meisten Fällen betrieblich nicht handhabbar. Daher hat der „one-time pad" vor allem theoretische Bedeutung, nämlich als ein Modell, dem man sich möglichst gut anzunähern versucht.

5.5. Symmetrische Chiffrierung

Symmetrische Chiffrierverfahren zeichnen sich dadurch aus, dass Chiffrier- und Dechiffrierschlüssel gleich und damit beide geheim sind. Aus praktischen Gründen werden Chiffrieralgorithmen in der Regel so entworfen, dass der zugehörige Dechiffrieralgorithmus wesentlich derselbe ist.

5.5.1. Stromchiffrierung („stream cipher")

Dies ist eine Annäherung an den „one-time pad", indem die Chiffrierung und Dechiffrierung mit der gleichen schlüsselabhängigen Pseudozufallsfolge erfolgt. Pseudozufallsfolgen sind deterministisch, wiederholen sich (Periode) und haben ein Konstruktionsgesetz (Rekursion). Stromchiffrierverfahren sind sehr gut untersucht, werden aber vor allem als proprietäre (nicht öffentliche) Chiffrierverfahren eingesetzt.

5.5.2. Blockchiffrierung

Wie der Name ausdrückt, transformieren Block - Algorithmen Klartext und Chiffratblöcke, Typischerweise der Länge von 64 oder 128 Bits. Dies entspricht prinzipiell der klassischen Substitution, wo ein Klartextbuchstabe durch jeweils immer denselben Chiffrierbuchstaben ersetzt wird.

Bei einem Alphabet von 26 Buchstaben kann diese Substitution unter Ausnützung der Buchstabenhäufigkeit dekryptiert werden. Alphabete mit 2^{64} bzw. 2^{128} „Buchstaben" können natürlich nicht mehr statistisch ausgewertet werden.

Bekannte Vertreter der Blockchiffrierung sind DES (Data Encryption Standard) und IDEA (International Data Encryption Algorithm). Beide sind öffentlich.

5.6. Asymmetrische oder Public-Key-Chiffrierung

Jeder Teilnehmer **i** besitzt zwei Schlüssel (keys).

Den geheimen **Private Key S_i** und den öffentlichen **Public Key P_i** mit der Eigenschaft $P_i(S_i(x)) = S_i(P_i(X)) = (X)$.

Damit kann zwischen zwei Teilnehmern A und B, welche gegenseitig ihre öffentlichen Schlüssel ausgetauscht haben, sowohl chiffriert/dechiffriert wie auch authentifiziert werden.

(Chiffriert A einen Klartext mit P_b und signiert diesen Klartext mit seinem geheimen S_a, so kann nur B dieses Chiffrat dechiffrieren, da nur B über den benötigten geheimen S_b verfügt. Zudem kann er mit P_a feststellen, dass die Signatur von A vorgenommen wurde, da nur A über den entsprechenden geheimen P_a verfügt).

Dass solche Systeme überhaupt existieren, beruht auf dem Vorhandensein von sogenannten Einwegfunktionen, d. h. mathematischen Funktionen, welche in der einen Richtung schnell, in der anderen Richtung aber nur mit sehr hohem Aufwand an Rechenkapazität oder Zeit berechenbar sind.

Zwei solcher Funktionen sind

$$Y = a^x \pmod p$$

und

$$y = x^a \pmod n$$

Die erste Funktion, wobei **p** eine Primzahl ist, ist eine echte Einwegfunktion und kann daher nicht direkt für ein „Public Key" – Kryptosystem genutzt werden; sie bildet jedoch die Grundlage für die DH (Diffie-Hellmann) – Schlüsselverteilung.

Die zweite Funktion, wobei **n** das Produkt zweier Primzahlen ist, besteht auf dem schwierigen Problem der Faktorenzerlegung grosser Zahlen und bildet die Grundlage des RSA (Rivest-Shamir-Adleman) Kryptosystems. Es handelt sich um eine Trapdoor-Einwegfunktion: Für jemanden, der die Zerlegung von **n** in die beiden Primzahlen kennt, existiert ein effizienter Dechiffrieralgorithmus.

5.7. Sicherheit von Verfahren

Bei der Beurteilung der Sicherheit von Chiffrierverfahren geht man davon aus, dass der Algorithmus, Chiffrate und Teile von Klartexten bekannt sind, und nur der Chiffrierschlüssel unbekannt ist. Das Verfahren ist sicher, wenn die beste Methode unter diesen Voraussetzungen das Ausprobieren („brute force attack") der möglichen Schlüssel ist und die Schlüsselmannigfaltigkeit derart gross ist, dass dies nicht mit vertretbarem Aufwand durchgeführt werden kann.

5.7.1. Sicherheit der Algorithmen

Es gibt sowohl bei symmetrischen wie asymmetrischen Chiffrierverfahren entsprechende Chiffrieralgorithmen, welche bis jetzt allen Angriffen mit mathematischen Verfahren widerstanden haben; eine absolute Sicherheit gibt es aber nicht. In den letzten Jahren hat sich gezeigt, dass aufgrund verbesserter mathematischer Verfahren oder Erhöhung der Rechenkapazität laufend Schlüssellängen angepasst werden mussten.

Bei „Public Key" – Kryptosystemen besteht immer die minime Gefahr, dass bei schwierigen mathematischen Problemen – wie dem Faktoriserungsproblem – unvorhersehbare Durchbrüche möglich sind.

5.7.2. Schlüssellängen

Eine genügend grosse Vielfalt der Schlüssel ist eine notwendige, aber bei weitem nicht hinreichende Bedingung für die Sicherheit von Chiffrierverfahren. Es muss insbesondere gewährleistet sein, dass die Mannigfaltigkeit z. B. durch Schwächen im Algorithmus nicht herabgesetzt werden kann. Eine absolute Empfehlung für Schlüssellängen ist unmöglich und hängt insbesondere auch von den gewählten Algorithmen ab.

Beim DES als Vertreter der Blockchiffrierung weiss man, dass die ursprüngliche Version mit 56 wirksamen Schlüsselbits dekryptiert werden kann, jedoch mit erheblichem Aufwand an Computerkapazität. Beim IDEA mit 128 Schlüsselbits nützt alle Computerkapazität nichts zum Ausprobieren der Schlüssel.

Beim RSA als Vertreter einer „Public Key" – Chiffrierung ist die Schlüssellänge von der Entwicklung der Primfaktorzerlegungsmethode abhängig. Der grösste in Primfaktoren zerlegte RSA - Modul ist derzeit etwa 150 – stellig und damit nahe bei 512 Bits. Um gegen zukünftige Entwicklungen gewappnet zu sein, sollte eine Schlüssellänge (RSA – Modul) von minimal 1024 Bits gewählt werden.

5.7.3. Symmetrische Chiffrierung – Public Key Chiffrierung

Der RSA ist etwa 1000 mal langsamer als der DES, die benötigte Schlüssellänge etwa 10 mal grösser. Dafür liegen die Vorteile bei der Schlüsselverteilung (key encryption) und Authentifikation. Daraus ergibt sich sofort, dass hybride Systeme (Chiffrierung symmetrisch, Authentifikation und Schlüsselverteilung asymmetrisch) optimal sind.

5.8. Rapides ziviles Wachstum

Kryptologie wurde früher vorwiegend in Militär und Diplomatie angewendet, heute hat der zivile Bereich eine mindest so grosse Bedeutung.

Man kennt heute sichere Algorithmen bei entsprechenden Schlüssellängen. Scheinbare Gegensätze wie symmetrische – asymmetrische Verfahren lassen sich in hybriden Systemen optimal nutzen. Quintessenz: Die Kryptographie ist gegenüber der Kryptonanalysis gegenwärtig im Vorteil, die Schere zwischen den beiden geht immer weiter auseinander.

Es besteht daher ein Konflikt zwischen dem Bedürfnis, die Privatsphäre zu schützen und der Notwendigkeit, zur Kriminalitätsbekämpfung diesen Schutz umgehen zu können. Dies erklärt die Forderung der US Regierung nach Kontrollmechanismen (z. B. Key Escrow). Ob und wie diese durchgesetzt werden, können ist noch offen.

Bei der Beurteilung der Sicherheit von Kryptosystemen hat sich der Schwerpunkt von den Algorithmen zu deren Implementation und zur Schlüsselverwaltung hin verschoben.

5.9. Wie sicher ist sicher?

Im ersten Teil haben wie angedeutet, wie die Vertraulichkeit mit kryptologischen Methoden gewährleistet werden kann. Dies ist, sowohl betrieblich wie auch zeitlich, mit einem gewissen Aufwand verbunden.

Daher werden Kryptologen oft mit der Anforderung „ich möchte eine möglichst einfache Chiffrierung, welche meine Informationen 2 Stunden bzw. vor aufsässigen Journalisten schützt" konfrontiert.

Diese Fragestellung ist bezüglich der Vertraulichkeit falsch, denn wenn eine Chiffrierung heute Stunden schützt, so schützt sie morgen Minuten und übermorgen Sekunden.

Anderseits ist in den meisten praktischen Fällen Vertraulichkeit nicht notwendig.

Man möchte aber sicher sein, dass Meldungen unverfälscht vom richtigen Sender (hier **Alice** genannt) zum richtigen Empfänger (namens **Bob**) gelangen; man wünscht die Authentifikation von Meldungen bzw. Personen.

Mit anderen Worten: man nimmt passive Attacken (abhören) in Kauf, verhindert aber aktive Attacken (verändern).

Wollen Alice beziehungsweise Bob später in Streitfällen das Zustandekommen der Meldung einem Dritten nachweisen (man spricht hier von „non repudiation oder Nichtwiderrufbarkeit von Meldungen), so braucht es ein Analogon zur bekannten (Hand-)Unterschrift, die digitale Signatur.

5.10. Prinzip der Authentifikation

Authentifikationen treten im täglichen Leben in vielfältiger Form auf, beim Bankschalter, bei der Passkontrolle, bei Eingangskontrollen usw.

Charakteristisch für eine Authentifikation ist, dass **Merkmale** einer Identität (Identifikation) mit gespeicherten Merkmalen **verglichen** und bei Übereinstimmung die Identität akzeptiert werden. Diese Merkmale müssen ein typisches Abbild der Identität sein, d. h. möglichst eindeutig und unfälschbar. In den obigen Beispielen ist dies die Unterschrift, der Pass, der Fingerabdruck.

5.10.1. Meldungsauthentifikation

Bei Meldungen in elektronischer Form ist das Merkmal eine Zahl, der „Hashwert", welcher aus der Meldung mit Hilfe der Hashfunktion abgeleitet wird.

Der Hashwert hat typischerweise eine Länge von 128 oder 160 Bits, ist also normalerweise wesentlich kürzer als die Meldung. Zudem muss der Hashwert möglichst eindeutig und unfälschbar sein. Die Hash - Funktion muss daher mindestens folgende drei Bedingungen erfüllen:

- Der Hashwert H = h(M) ist schnell berechenbar.
- Für jeden gegebenen Hashwert H ist es extrem schwierig, ein M zu finden, so dass H = h(M). Aus dem Hashwert kann also nicht auf die Meldung zurückgeschlossen werden.
- Für eine gegebene Meldung M ist es extrem schwierig, ein M' zu finden, so dass h(M) = h(M'). Die Meldung ist also nicht modifizierbar, was bei Banktransaktionen sofort einleuchtet.

5.10.2. Personenauthentifikation

Mit dem Hashwert ist zwar die Meldung authentifiziert. Es kann aber jedermann mit der bekannten Hashfunktion Meldungen mit dem entsprechenden Hashwert versehen und einzuschleusen versuchen.

Um dies zu verhindern, müssen auch Merkmale von Alice und Bob einbezogen werden und hier bieten sich kryptologische Schlüssel und symmetrische oder asymmetrische (public key) Chiffrierverfahren an.

5.10.2.1. MAC, Authentifikation mit symmetrischer Chiffrierung

Alice chiffriert den Hashwert H = h(M) mit dem gemeinsamen Schlüssel S: $E_s(H)$ und hängt dies an die ursprüngliche Meldung an.

Bob bildet $D_s(E_s(h))$, dechiffriert also die angehängte Zahl, und vergleicht sie mit seinem aus M errechneten Hashwert. Bei Übereinstimmung weiss er, dass die Meldung unverfälscht ist und nur von jemandem stammen kann, welcher den Schlüssel S kennt.

Der chiffrierte Hashwert $E_s(h(M))$, welcher von der Meldung und dem Schlüssel S abgeleitet ist, wird MAC (Message Authentication Code) genannt. Der MAC (M,S) ist nichts anderes als eine schlüsselabhängige Checksumme.

5.10.2.2. Digitale Signatur: Authentifikation mit asymmetrischer Chiffrierung

Der Ablauf ist wie bei der Authentifikation mit symmetrischer Chiffrierung, wobei Alice den Hashwert mit ihrem geheimen privaten Schlüssel (private key) chiffriert (genauer authentifiziert) und Bob diese an die Meldung angehängte Zahl $S_A(h(M))$, die digitale Signatur, mit dem öffentlichen Schlüssel von Alice dechiffriert $P_A\ (S_A\ (h(M)))$.

Hier wird die Unverfälschtheit der Meldung garantiert, welche nur von Alice stammen kann, sofern Alice's öffentlicher Schlüssel wirklich echt (authentisch) ist. Der Nachweis dieser Echtheit bedingt der Einbezug von Dritten. Damit erfüllt die digitale Signatur (Unterschrift) alle Funktionalität der Handunterschrift.

5.10.3. Die Zertifizierungsstelle („Certificate Authority" oder „Notariat")

Die Zertifizierungsstelle garantiert die Echtheit des öffentlichen Schlüssels eines Teilnehmers J durch ihre digitale Signatur, $S_N(h(Id_J,P_J))$, welche im wesentlichen von der Identität und dem öffentlichen Schlüssel des Teilnehmers abhängt.

Alice hängt die digitale Signatur der Zertifizierungsstelle, das Zertifikat, zusätzlich zu ihrer eigenen digitalen Signatur an die Meldung, und Bob kann sowohl die digitale Signatur von Alice wie auch das Zertifikat überprüfen.

Bob kann mit diesem Vorgehen Dritten gegenüber nachweisen, dass er die Meldung von Alice erhalten hat. Ist der Umgekehrte Nachweis auch notwendig, wie etwa beim E-Mail, so ist eine Rückmeldung als Analogon zur Quittung notwendig.

Zur Überprüfung der Zertifikate benötigen alle Teilnehmer den öffentlichen Schlüssel der Zertifizierungsstelle, also gewissermassen das Zertifikat des Zertifikates, das Zertifikat des Zertifikates des Zertifikates, usw. man wird die Geister, die man gerufen, nicht mehr los!

Irgendwann muss der öffentliche Schlüssel einer Zertifizierungsstelle sicher übermittelt und fälschungssicher aufbewahrt werden. Als effiziente Lösung für diese Aufgabe bietet sich die Chip-Karte an, insbesondere die Smart-Card. Darin werden sowohl die sensitiven Schlüssel (private Schlüssel, öffentlicher Schlüssel der Zertifizierungsstelle) gespeichert und als auch die kryptologischen Algorithmen ausgeführt. Damit wird eine klare Trennung zwischen krytologischen Daten und Prozessen einerseits und Betriebssystem andrerseits erreicht.

5.11. Authentizität und Vertraulichkeit

Authentizität kann an sich durch Vertraulichkeit (Chiffrierung der ganzen Meldung, nicht nur des Hashwertes) garantiert werden.

Um dies zu erreichen, kann man symmetrische Chiffriersysteme einsetzen. Dies hat den Nachteil, dass Bob nur dann nachweisen kann, die Meldung von Alice erhalten zu haben, wenn Alice ihren geheimen Schlüssel zur Verfügung stellt.

Setzt man asymmetrische Chiffrierverfahren ein, so umgeht man diese Nachteile, allerdings auf Kosten eines wesentlich höheren Rechenaufwandes. Aus diesem Grund ist es daher von Vorteil, die zwei verschiedenen Problembereiche Authentizität und Vertraulichkeit auch durch verschiedene Methoden zu lösen.

5.12. Kryptologie heute und morgen

Heute kennt man gute Verfahren und Methoden für Chiffrierung, Schlüsselverwaltung, Authentifikation und digitale Signaturen.

Aufgabe der Kryptologie ist daher vor allem die effiziente, problemangepasste Kombination verschiedener Methoden und die Verifikation der entsprechenden Implementationen und der entsprechenden Protokolle.

Wie bei der normalen Unterschrift werden digitale Signaturen nur dann auf breiter Basis eingesetzt, wenn sie rechtsgültig sind. Im Gegensatz etwa zum Deutschen Signaturgesetz besteht in der Schweiz Handlungsbedarf. Immerhin wurde mit der Verordnung für die PKI (Public Key Infrastructure) in dieser Richtung der Anfang gemacht. Authentizität und Vertraulichkeit lassen sich also bei E-Mail, E-Commerce usw. lösen.

5.13. Anonymität gewährleisten

Ein wesentliches Anliegen im Informationszeitalter ist der Schutz der Privatsphäre, die Gewährleistung der Anonymität. Denken wir nur an die Spuren bei Kreditkarten aller Art und die mannigfaltigen Statistiken, welche Rückschlüsse auf Lebensstil, Konsumverhalten usw. erlauben.

Für die Gewährleistung der Anonymität bestehen schon heute kryptologische Lösungsansätze, wie sie z. B. über Internet – Abstimmungen publiziert wurden. Dabei geht es sowohl um die Anonymität der Stimmenden wie auch um die Anonymität der Stimm-Meldungen (Beeinflussung des Abstimmungsverhaltens!).

Da sich die Gewährleistung der Anonymität in den bremsenden Spannungsfeldern Privatperson – Staat bzw. Privatperson – Wirtschaft

befindet, wird bis zur Umsetzung der Lösungsansätze noch einige Zeit verstreichen.

6. Abschliessende Bemerkungen von FJK

Die Annahme, dass Informationen auf lokalen Speichermedien am besten durch Festplatten - Verschlüsselung geschützt sei, ist aus zwei Gründen äusserst gefährlich.

1. Bei der Verschlüsselung wird Blockverschlüsselung verwendet. D. h. ein gleicher Block wird immer gleich verschlüsselt. Mit geeigneten Methoden kann eventuell Information ohne die Verschlüsselung zu knacken mit genügender Genauigkeit sichtbar gemacht werden (siehe oben Plan).
2. Festplattenverschlüsselung ist der beste Schutz gegen unberechtigtes Aufstarten - nicht mehr - nicht weniger. Ist das System einmal berechtigterweise gestartet, erben alle Prozesse die Privilegien des Berechtigten. Wird so z. B. Internet gestartet, erbt der Internet-Browser die Privilegien und kann somit wie der Benutzer alle Informationen in seinem Zugriffsbereich „bearbeiten".