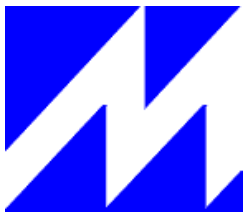


Märkische Fachhochschule
Fachbereich TBW

Kryptographie

Innovationsmanagement und Kommunikationssysteme

Seminar 9b

Prof. Dr. Jörg Liese
Prof. Dr. Andreas de Vries

Sommersemester 2001

Gisela Honert
Matrikel-Nr. : 10001458

Kai Rother
Matrikel-Nr. : 10001439

Inhaltsverzeichnis

Quellenverzeichnis

Beutelspacher, Albrecht / **Schwenk**, Jörg / **Wolfenstetter**, Klaus-Dieter (1998), Moderne Verfahren der Kryptographie, vieweg-Verlag Braunschweig / Wiesbaden

Garfinkel, Simon (1996), PGP – Pretty Good Privacy, O'Reilly International Thomson Verlag Bonn

Schmeh, Klaus (1998), Safer Net-Kryptographie im Internet und Intranet, dpunkt-Verlag Heidelberg

Selke, Gisbert W. (2000), Kryptographie – Verfahren, Ziele, Einsatzmöglichkeiten, O'Reilly International Thomson Verlag Köln

Singh, Simon (2000), Geheime Botschaften, Carl Hanser Verlag München - Wien

Froese, Jan / **Gebhard**, Simone / **Marunde**, Gerald (2000), Datensicherheit als Grundlage des internationalen elektronischen Handels - Verschlüsselung, Authentifizierung, Datenschutz,
www.hausarbeiten.de/cgi-bin/superDBdruck.pl/archiv/bwl/bwl-datensich/bwl-datensich.shtml

Soquat, Hubertus (2000), Was ist der Hintergrund für die Kryptographiepolitik,
www.sicherheit-im-internet.de/themes/themes.phtml?ttid=39&tsid=208&tdid=60&page=0

Pressemitteilung des **Bundesministerium für Wirtschaft und Technologie** und des Bundesministerium des Innern , Bonn, den 2. Juni 1999
www.sicherheit-im-internet.de/themes/themes.phtml?ttid=4&tsid=100&tdid=116&page=0

Wissenschaftliches Institut für Kommunikationsdienste GmbH – WIK
in Zusammenarbeit mit dem Institut für Sichere Telekooperation (SIT) und der GMD – Forschungszentrum Informationstechnik GmbH
im Auftrag des Bundesministeriums für Wirtschaft und Technologie (BMWi),
Position und Chancen der deutschen IT-Sicherheitsindustrie im globalen Wettbewerb
www.sicherheit-im-internet.de/themes/themes.phtml?ttid=4&tdid=375

Pressemitteilung des **Bundesministerium für Wirtschaft und Technologie** und des Bundesministerium des Innern,
Bundeskabinett stellt Weichen für E-Commerce
www.sicherheit-im-internet.de/themes/themes.phtml?ttid=38&tsid=100&tdid=442&page=0

Abbildungen

Seite 6 aus **Singh**, Simon, Geheime Botschaften, Seite 23
Seite 7 aus **Singh**, Simon, Geheime Botschaften, Seite 170
Seite 8 aus **Beutelspacher**, Albrecht / **Schwenk**, Jörg / **Wolfenstetter**, Klaus-Dieter, Moderne Verfahren der Kryptographie, Seite 6
Seite 9 aus **Singh**, Simon, Geheime Botschaften, Seite 71
Seite 10 aus **Beutelspacher**, Albrecht / **Schwenk**, Jörg / **Wolfenstetter**, Klaus-Dieter, Moderne Verfahren der Kryptographie, Seite 10
Seite 11 aus **Beutelspacher**, Albrecht / **Schwenk**, Jörg / **Wolfenstetter**, Klaus-Dieter, Moderne Verfahren der Kryptographie, Seite 11

1. Vorwort

Es ist seit alters her ein Anliegen der Menschheit, erstaunlicherweise aber auch von Tieren, Dinge und Informationen zu verheimlichen oder zu verstecken um sich einen Vorteil zu verschaffen.
Menschen betreiben dies mit einem bemerkenswertem Einfallsreichtum. Kryptographie zieht sich wie ein roter Faden durch die Geschichte der Menschheit und beeinflusste diese zum Teil erheblich im Positiven wie im Negativen.

Aufgrund der Fülle von kryptographischen Innovationen und Anwendungen werden wir versuchen einen systematischen Überblick mit einzelnen praktischen Beispielen zu dem Thema zu geben.

Zur aktuellen Situation der Verschlüsselungstechnik beschränken wir uns auf das Gebiet der kommerziellen und privaten Bedeutung, die nachrichtendienstliche und militärische Bedeutung kann aufgrund der Informationslage nur an geschichtlichen Beispielen verdeutlicht werden.

2. Grundlegendes zur Kryptographie

2.1 Terminologie

Zum besseren Verständnis und um Unklarheiten zu vermeiden ist eine kurze Erläuterung der grundlegenden Begriffe hilfreich.

Kryptologie ist die Wissenschaft von der Verschlüsselung in allen Formen, Oberbegriff für Kryptographie und Kryptoanalyse. **Kryptographie** ist die Wissenschaft von der Verschlüsselung oder der Verschleierung des Inhaltes einer Nachricht. Der **Schlüssel** ist eine Übereinkunft zwischen dem Sender und Empfänger einer Nachricht, um diese zu codieren oder zu chiffrieren und wieder lesbar zu machen. **Klartext** ist die ursprüngliche Mitteilung vor der Verschlüsselung, **Geheimtext** die Mitteilung (der Klartext) nach der Verschlüsselung. Unter **Kryptoanalyse** versteht man das Erschließen des Klartextes aus dem Geheimtext ohne Kenntnis des Schlüssels. **Codierung** ist jegliche Form der Verschlüsselung, die nicht flexibel ist, bei der nur ein Schlüssel verwendet wird, nämlich das Codebuch. Zum Beispiel hat der Befehl „Besteigt den Fujiyama!“ den Angriff der Japaner auf Pearl Harbor in die Wege geleitet. **Chiffrieren** ist die Technik einen Klartext mit Hilfe eines Verschlüsselungsverfahrens in einen Geheimtext zu überführen. Beispielsweise ist der Name des Computers HAL in Stanley Kubricks Film „2001-Odyssee im Weltall“ eine Chiffre für IBM.

2.2 Problem Datensicherheit

„The right to be let alone – the most comprehensive of rights, and the right most valued by civilized men.” Dieses Zitat aus der persönlichen Beurteilung von Louis D. Brandeis, Richter im Prozess Olmstead gegen die Vereinigten Staaten,1928, beschreibt hervorragend die Wichtigkeit von Datenschutz und Datensicherheit.
Der Schutz der Privatsphäre ist vielen Menschen sehr wichtig, ebenso ist es das Anliegen von Unternehmen / Staaten / Nachrichtendiensten usw. ihre Daten vor fremdem Zugriff zu bewahren.

Dies ist zu Hause, z.B. im Tresor, auch kein Problem, viel problematischer ist es diese Daten während der Übermittlung zu schützen. Konventionell hatte man dafür Brief-

umschläge, eine eMail ist eher mit einer Postkarte vergleichbar. Jeder, dem so eine elektronische Postkarte in die Hand fällt, kann sie lesen. An dieser Stelle sorgt eine gute Verschlüsselung für Abhilfe. Kryptographie ist eine so wirkungsvolle Methode, dass sie in den USA sogar unter das Waffengesetz fällt.

2.3 Ziele der Kryptographie

Kryptographie soll die Daten vor unberechtigten Zugriffen schützen, so dass sie ungelesen und unverändert beim richtigen Empfänger ankommen. Ziele sind also Authentikation, Geheimhaltung und Anonymität. Folgende Fragestellungen sollen also beantwortet werden:

- Ist derjenige, von dem die Nachricht stammt, auch wirklich der, für den ich ihn halte?
- Ist derjenige, der die Nachricht erhält, auch wirklich der, für den ich ihn halte?
- Ist die Nachricht unverändert und vollständig bei mir angekommen?
- Hatten Fremde Einblick in die Nachricht?
- Können Rückschlüsse auf Sender und Empfänger gezogen werden?

Kryptographie versucht, all diese Dinge sicherzustellen.

2.4 Ziele der Kryptoanalyse

Kryptoanalyse ist das systematische Entschlüsseln von Geheimtexten. Ziel ist somit das unberechtigte Zugreifen auf Nachrichten. Dies teilt sich in zwei Sekundärziele auf, entweder möchte der Kryptologe eine codierte Information wieder lesbar machen, oder er will anhand des chiffrierten Textes den zugrundeliegenden Schlüssel herausfinden.[1]

Die Kryptoanalyse verwendet dafür verschiedene Methoden, wie z.B. die Brute-Force-Methode oder die Häufigkeitsanalyse der Buchstaben. Man kann die Brute-Force-Methode auch als Schlüsselsuche bezeichnen, da alle möglichen Schlüssel ausprobiert werden. Die Häufigkeitsanalyse ist ein systematisches Abzählen der Zeichen des Geheimtextes, die mit der Häufigkeit der einzelnen Buchstaben in der jeweiligen Sprache verglichen und ersetzt werden.
Die Evolution der Kryptographie wird durch die Kryptoanalyse getrieben. Denn jedes Mal, wenn es den Kryptoanalytikern gelingt, einen Code zu brechen, sind die Kryptographen gefordert, einen stärkeren Code zu entwickeln. Maria Steward wurde nur verurteilt und hingerichtet, da es den Kryptoanalytikern möglich war Ihre Geheimschrift zu entschlüsseln und damit den geplanten Anschlag auf die englische Königin zu beweisen.
Ihre Hinrichtung belegt, dass sie wohl keinen sehr starken Algorithmus benutzt hat.

Kryptoanalyse ist eine sehr personal- und kostenintensive Angelegenheit. Es ist zum Beispiel bekannt, dass für die National Security Agency der USA mehr Mathematiker arbeiten als für irgendeine andere Institution oder Firma auf der Welt. Weiterhin ist die NSA der weltweit größte Abnehmer von Computern. Gerüchten zufolge hört die NSA weltweit die meisten Telefongespräche ab.[2]

3. Geschichte

Die frühesten Chiffrierverfahren wurden ca. 2000 v.Chr. in Ägypten verwendet, wo Nachrichten als Hieroglyphen in Steinplatten gehauen wurden.[3] Die ersten Beschreibungen von Geheimschriften finden sich schon bei Herodot, Autor der *Historien.* Herodot zufolge rettete die Kunst der Geheimschrift Griechenland vor der Eroberung

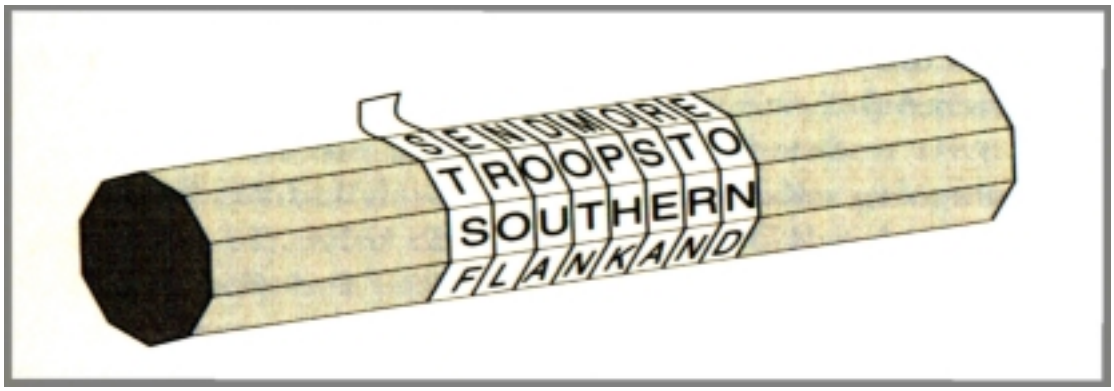
[1] vgl. PGP Seite 45
[2] vgl. PGP Seite 71
[3] vgl. PGP Seite 69

durch Xerxes, den Führer der Perser. Zu kriegerischen und diplomatischen Zwecken bediente sich auch Julius Caesar der Kryptographie. Er benutzte eine Substitutions-Chiffre. Der Kaiser ersetzte einfach jeden Buchstaben der Nachricht durch den Buchstaben, der 3 Stellen weiter im Alphabet folgte. Diese Art der Substitution wird auch als Caesar-Verschiebung bezeichnet. [4]

Im ersten Jahrhundert nach Christi erläutert Plinius der Ältere wie die ‚Milch' der Thithymallus-Pflanze als unsichtbare Tinte verwendet werden kann.[5] Das verstecken von Botschaften ist eine weitere Möglichkeit der sicheren Übermittlung von Nachrichten und wird als Steganographie bezeichnet.

Im Kamasutra wird irgendwo (je nach Ausgabe an den Punkten 35 – 45) den Frauen empfohlen die Kunst der Geheimschrift zu studieren, um ihre Affären geheimzuhalten.

Eine Form der Transposition ist das erste militärische Kryptographie-Verfahren, die Skytale, wie sie schon im 5. Jahrhundert die Spartaner gebrauchten. Die Skytale ist ein Holzstab, um den ein Streifen Leder oder Pergament gewickelt wird. Der Sender schreibt die Nachricht der Länge des Stabes nach auf den Streifen und wickelt ihn ab. Danach scheint der Streifen nur eine sinnlose Aufreihung von Buchstaben zu enthalten.[6]



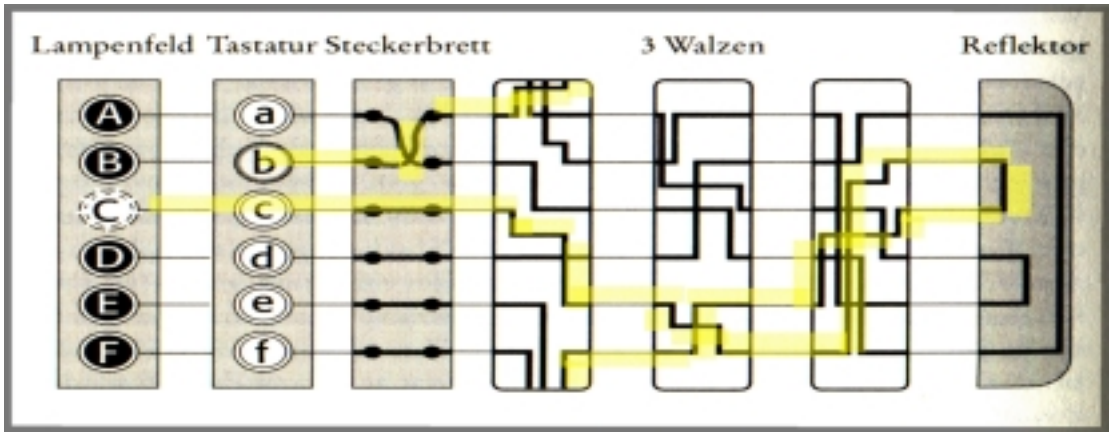
Um die Nachricht wiederherzustellen wickelt der Empfänger den Streifen einfach um eine Skytale gleichen Durchmessers wie sie der Sender benutzt hat.

Um 1700 entstanden die ersten Chiffrierbüros der europäischen Mächte, sogenannte ‚Schwarze Kammern', Nervenzentren, in denen Botschaften entschlüsselt und Informationen zusammengetragen wurden. Die berühmteste, disziplinierteste und schlagkräftigste war die Geheime Kabinettskanzelei in Wien. Dort wurde die Post der diplomatischen Vertretungen in Wien systematisch abgefangen, innerhalb von 3 Stunden abgeschrieben und wieder versiegelt und zurück zum Hauptpostamt geliefert.
Die Abschriften, bis zu einhundert am Tag, ließ man von den Kryptoanalytikern entschlüsseln.[7]

Ab 1800 waren erste mechanische Chiffriergeräte im Einsatz, deren Weiterentwickelung um 1920 in den Rotorchiffriermaschinen gipfelte. Die bekannteste dieser Art war die von den Deutschen im 2. Weltkrieg benutzte Enigma.

[4] vgl. Geheime Botschaften Seite 25
[5] vgl. Geheime Botschaften Seite 20
[6] vgl. Geheime Botschaften Seite 23
[7] vgl. Geheime Botschaften Seite 81

Äußerlich handelte sich dabei um eine Art Schreibmaschine, bei der nach dem Drücken eines Buchstabens auf der Tastatur ein codierter Buchstabe auf einem Lampenfeld aufleuchtet. Der wichtigste Teil der Maschine ist die Walze (auch Rotor genannt), eine dicke Gummischeibe, die von Drähten durchzogen ist. Von der Tastatur ausgehend führen die Drähte in die Walze hinein, in deren Innern sie kreuz und quer verlaufen bis sie schließlich im Lampenfeld austreten.



Nach dem Drücken eines Buchstabens drehte sich die erste Walze um eine Position weiter, so dass eine andere Verdrahtung aktiviert wird, nach einer vollständigen Umdrehung wird die zweite Walze eine Position weitergedreht usw., so dass derselbe Klartextbuchstabe in verschiedene Geheimtextbuchstaben überführt wird.

Möglichkeiten der Verschlüsselung mit einer 3-Walzen-Enigma

Jede der 3 Walzen kann in eine von 26 Stellungen gebracht werden, es gibt daher 26x26x26 Walzenstellungen, also 17576.
Die 3 Walzen können in 6 verschiedene Reihenfolgen gebracht werden.
Die Zahl der Möglichkeiten 6 Buchstabenpaare von 26 zu verbinden und damit zu vertauschen beträgt 100391791500.

Die Gesamtzahl der Verschlüsselungen ergibt sich aus der Multiplikation dieser 3 Zahlen. 17576x6x100391791500 ergibt in etwa 10^{15} Möglichkeiten.[8]

Trotz dieser gewaltigen Anzahl an Möglichkeiten gelang es polnischen Kryptoanalytikern einfache Enigmas zu entschlüsseln. Durch die Tatsache, das nicht 3-Walzen, sondern Enigmas mit 4 bis 8 Walzen eingesetzt wurden, gelangten die Polen an die Grenze ihrer Möglichkeiten und ein Team von 7.000 Mathematikern und Wissenschaftlern fing im englischen Bletchley Park mit dem Entschlüsseln des deutschen Funkverkehrs an. Da alle 24 Stunden der Code der Enigma verändert wurde musste täglich der Tagesschlüssel aufs neue gefunden werden.[9] Bei Einführung von neuen Walzen stand man für eine längere Zeit quasi im Dunkeln, es wird aber geschätzt, dass die Arbeit der Kryptoanalytiker den Krieg um bis zu drei Jahre verkürzt haben könnte.

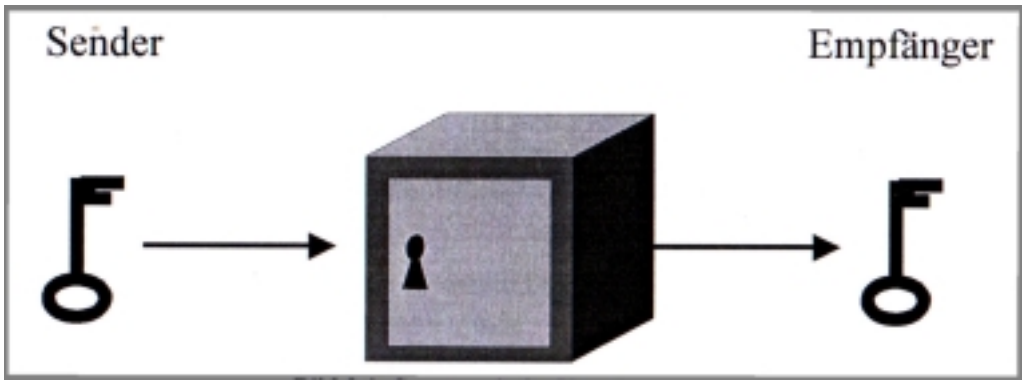
Ein Meilenstein war 1976 die Veröffentlichung des Prinzips der Public-Key-Kryptographie durch Whitfield Diffie und Martin Hellman. Mit ihrer Arbeit wurde ein jahrtausende altes,,unlösbares' Problem denkbar elegant gelöst.

[8] vgl. Geheime Botschaften Seite 171
[9] vgl. Geheime Botschaften Seite 179

Während in der Welt der alten Kryptologie je 2 Teilnehmer, die geheim miteinander kommunizieren wollten, schon vorher ein Geheimnis haben mussten (ihren geheimen Schlüssel), ist dies in der Public-Key-Kryptographie nicht mehr der Fall: jeder, auch jemand, der mit mir noch nie Kontakt hatte, kann mir eine verschlüsselte Nachricht schicken, die nur ich entschlüsseln kann.[10]

4. Arten der Verschlüsselung

4.1 Symmetrische Verschlüsselung



Ein symmetrischer Verschlüsselungsalgorithmus besteht aus einer **Funktion f** mit zwei Eingabewerten, dem **Schlüssel k** und dem **Klartext m**, und einer Ausgabe, dem **Geheimtext c**, der sich aus k und m ergibt.
Der Sender verschlüsselt eine Nachricht m, indem er

$$c = f(k,m)$$

berechnet, wobei k der gemeinsame Schlüssel ist.
Der Empfänger kann mit Hilfe des selben Schlüssels k den Geheimtext entschlüsseln indem er

$$f^*(k,c)=m$$

berechnet.[11]

Wenn man so mit jemandem verschlüsselte Nachrichten austauschen will, dann muss man dieser Person auch den kryptographischen Schlüssel mitteilen, den man verwendet. Hier liegt eines der Hauptprobleme der symmetrischen Verschlüsselung, da man einen sicheren Übertragungsweg für den Schlüssel haben müsste, z.B. wurden die diplomatischen Vertretungen der USA mit Schlüsseln versorgt, indem man Kurieren, die natürlich keinen Kofferschlüssel hatten, Koffer ans Handgelenk kettete. Kamen die Kuriere nicht an, so wurde dies sehr schnell bemerkt und die Codierschlüssel nicht verwendet (die Kofferschlüssel übrigens auch nicht).[12] Zudem brauchen mehrere Leute, die sich austauschen wollen, eine ganze Menge von Schlüsseln. Die Anzahl der Schlüssel berechnet sich über ((n)(n-1))/2. Schon bei 10 Leuten bräuchte man also 45 Schlüssel, damit jeder mit jedem sicher kommunizieren kann.[13]

[10] vgl. Moderne Verfahren der Kryptographie Seite V
[11] vgl. Moderne Verfahren der Kryptographie Seite 7
[12] vgl. PGP Seite 47
[13] vgl. PGP Seite 51

4.1.1 Substitution

Bei der Substitution werden die Buchstaben des Klartextes einzeln durch andere Buchstaben des Geheimtextalphabets ersetzt. Unzählige Verfahren machen sich diese Art der Verschlüsselung zu nutze. Es gibt unterschiedliche Methoden der Substitution, z.B. die monoalphabetische Verschlüsselung, bei der jeder Klartextbuchstabe mit immer dem selben Geheimtextbuchstaben chiffriert wird (Caesar-Verschiebung).
Bei der polyalphabetischen Verschlüsselung gibt es mehrere Geheimtextalphabete und ein Buchstabe des Klartextes wird mit unterschiedlichen Geheimtextbuchstaben chiffriert (Vigenere-Verschlüsselung, siehe nachfolgendes Beispiel).

Schlüsselwort	L I C H T L I C H T L I C H T L I C H T L
Klartext	t r u p p e n a b z u g n a c h o s t e n
Geheimtext	E Z W W I P V C I S F Q E H V S W U A X Y

4.1.2 Transposition

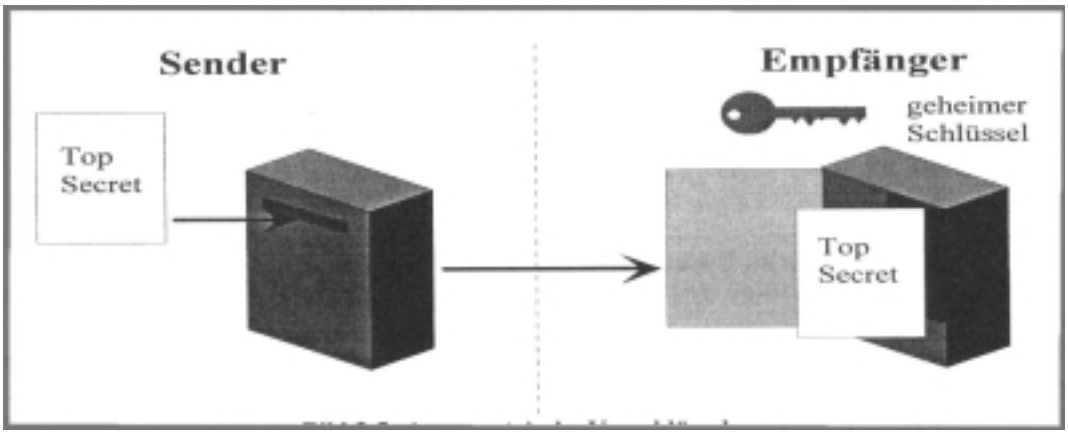
Bei der Transposition werden die Buchstaben einer Botschaft einfach anders angeordnet, was nichts anderes ergibt als ein Anagramm. Bei sehr kurzen Mitteilungen, etwa einem einzigen Wort, ist dieses Verfahren relativ unsicher, weil es nur eine eng begrenzte Zahl von Möglichkeiten, gibt die Buchstaben umzustellen[14]. Damit eine Transposition brauchbar ist, müssen die Buchstaben nach einem handhabbaren System umgestellt werden, z.B. die ‚Gartenzaun'-Transposition, welche wie folgt funktioniert.
Die Buchstaben des Textes werden abwechselnd auf zwei Zeilen geschrieben. Um die Geheimbotschaft herzustellen wird die Reihe der Buchstaben auf der unteren Zeile an die Buchstabenreihe der oberen Zeile angehängt.

Der Kaffee ist alle.
d r a f e s a l .
 e k f e i t l e
drafesal ekfeitle.

Drafesal ekfeitle ist kein schwäbischer Dialekt, sondern der transpositionierte Text. Die Entschlüsselung erfolgt nun mit demselben Schlüssel wie die Verschlüsselung.

[14] vgl. Geheime Botschaften Seite 22

4.2 Asymmetrische Verschlüsselung



In der Mitte der 70'er Jahre veröffentlichten die Amerikaner Diffie und Hellman sowie unabhängig von ihnen Ralph Merkle eine geradezu revolutionäre Idee. Sie schlugen vor, Verfahren zu benutzen, bei denen zum Verschlüsseln ein anderer Schlüssel als zum Entschlüsseln nötig ist. Darüber hinaus sollte es unmöglich sein, aus der Kenntnis einer der beiden Schlüssel den anderen ableiten zu können.
Vergleicht man die vorher bekannten Systeme mit einem Safe, für den 2 Personen einen Schlüssel haben, so entspricht die neue Idee einem Nachttresor. Viele Menschen können etwas einwerfen, aber nur der legitime Empfänger kann den Tresor öffnen.[15]

Die asymmetrische Verschlüsselung wird auch als Public-Key-Verschlüsselung bezeichnet. Bei der asymmetrischen Verschlüsselung werden zwei Schlüssel verwendet. Man erzeugt ein Schlüsselpaar, bestehend aus einem öffentlichen Schlüssel und einem privaten Schlüssel. Der öffentliche Schlüssel wird bekannt gemacht, aber der private Schlüssel wird geheimgehalten.

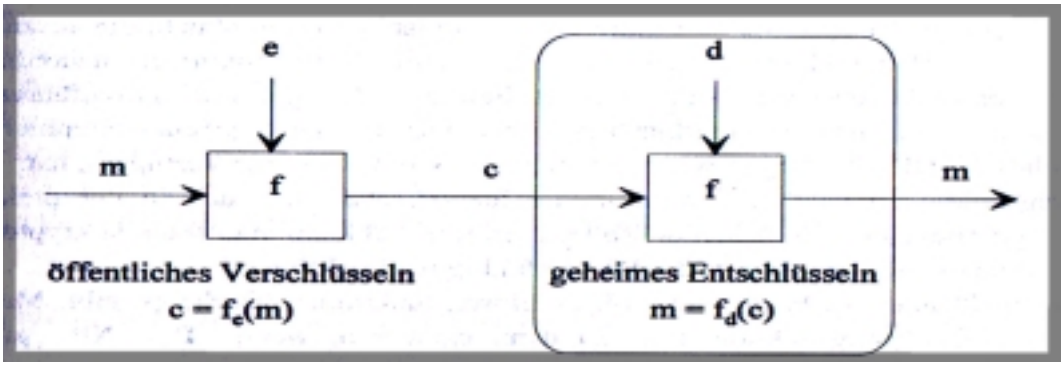
Die Kommunikation funktioniert folgendermaßen: Der Sender verschlüsselt den Klartext mit dem öffentlichen Schlüssel des Empfängers. Da es nicht möglich ist, mit dem öffentlichen Schlüssel die Daten zu entschlüsseln sind diese nun sicher. Dadurch kann nur der Empfänger des Chiffretextes den Text mit seinem zugehörigen privaten Schlüssel entschlüsseln. Somit ist eine spontane verschlüsselte Kommunikation möglich. Durch Anwendung der asymmetrischen Verschlüsselung lässt sich auch das Schlüsselaustausch-Problem sowie das Schlüsselvermehrungsproblem der symmetrischen Verschlüsselung lösen.

Die Schwierigkeit besteht nun darin diese allgemeine Idee zu konkretisieren. Die beiden Hälften eines Schlüsselpaares müssen genau zueinander passen – sonst könnte man nicht erwarten, dass ein privater Schlüssel eine mit dem öffentlichen Gegenstück verschlüsselte Nachricht wieder dechiffriert. Dies heißt, dass eine sehr enge formelmäßig erfassbare Beziehung zwischen den beiden Hälften besteht. Wenn es die aber gibt, was sollte einen Angreifer davon abhalten, das entsprechende Gleichungssystem zu lösen? Denn der öffentliche Schlüssel würde aus praktischen Überlegungen heraus nicht oft gewechselt werden.[16]
Im Frühling 1976 befassten sich drei junge Professoren (Ron Rivest, Adi Shamir und Len Adleman) des Fachgebietes Theoretische Informatik am MIT mit der Diffie-Hellman Abhandlung *New Directions in Cryptographie.*

[15] vgl. Moderne Verfahren der Kryptographie Seite 63
[16] vgl. Kryptographie - Verfahren, Ziele, Einsatzmöglichkeiten Seite 64

Nach mehreren Fehlschlägen versuchte die Gruppe zu beweisen, dass ein solches mathematisches Verfahren nicht möglich ist. Im April ’77 hatte Ron Rivest die zündende Idee. Das System basiert auf der Feststellung von Donald Knuth von der Stanford-Universität, dass es leicht ist, zwei Primzahlen zu multiplizieren, aber ungleich schwieriger, das Produkt wieder in die beiden Faktoren zu zerlegen.[17]

Mathematisch und praktisch sieht die Grundlage des RSA-Verfahrens (**R**ivest, **S**hamir, **A**dleman) folgendermaßen aus:



1. Gisela wählt zwei riesige Primzahlen , *p* und *q*. Gisela hält $p = 17$ und $q = 11$ für riesig. Diese Zahlen muss sie geheim halten.
2. Gisela multipliziert die beiden Zahlen und erhält $N = 187$. Sie wählt eine weitere Zahl $e = 7$.
3. Die Zahlen *e* und *N* werden für die Verschlüsselung benötigt und veröffentlicht.
4. Der zu verschlüsselnde Text wird in eine binäre Zahl verwandelt, nennen wir sie *M*. Dieses *M* wird verschlüsselt und ergibt den Geheimtext *C* nach folgender Formel: $C = M^e \pmod N$.
5. Nehmen wir an, Kai wolle Gisela eine Nachricht schicken, wählen wir ein x als Code unendlicher Liebe, so wird das x in ASCII durch 1011000 dargestellt und entspricht der Dezimalzahl $M = 88$.
6. Diese Zahl kann von Kai in die Verschlüsselungsformel für die Mitteilung an Gisela eingesetzt werden.
   $C = 88^7 \pmod{187}$
7. Kai benutzt an dieser Stelle, wie immer, nicht seinen Taschenrechner, da die Zahl astronomisch groß ist. Allerdings kommen wir durch die Zerlegung der Potenzen zu folgendem:
   $88^7 \pmod{187} = [88^4 \pmod{187} \times 88^2 \pmod{187} \times 88^1 \pmod{187}] \pmod{187}$
   $88^1 = 88 = 88 \pmod{187}$
   $88^2 = 7744 = 77 \pmod{187}$
   $88^4 = 59969536 = 132 \pmod{187}$
   $88^7 = 88^4 \times 88^2 \times 88^1 = 88 \times 77 \times 132 = 894432 = 11 \pmod{187}$
   Jetzt schickt Kai den Geheimtext, $C = 11$, an die reizende Gisela.
8. Da die Exponenten in der Modul-Artithmetik Einwegfunktionen sind ist es sehr schwer von $C = 11$ aus den Weg zurück zu gehen und die ursprüngliche Botschaft *M* zu erschließen.
9. Gisela kann die Botschaft jedoch leicht entschlüsseln da sie eine Information besitzt: die Werte von *p* und *q*. Gisela errechnet die Zahl *d*, den Dechiffrierschlüssel, der als privater Schlüssel bezeichnet wird. *d* wird mit folgender Formel berechnet:
   $e \times d = 1 \pmod{(p-1) \times (q-1)}$
   $7 \times d = 1 \pmod{16 \times 10}$

[17] vgl. PGP Seite 84

$7 \times d = 1 \pmod{160}$
$d = 23$

10. Um die Nachricht ihres Geliebten zu entschlüsseln benutzt die holde Gisela einfach die folgende Formel:
$M = C^d \pmod{187}$
$M = 11^{23} \pmod{187}$
$M = [11^1 \pmod{187} \times 11^2 \pmod{187} \times 11^4 \pmod{187} \times 11^{16} \pmod{187}] \pmod{187}$
$M = [11 \times 121 \times 55 \times 154] \pmod{187}$
$M = 88$ = x in ASCII = unendliche Liebe in Giselas Codebuch.[18]

Rivest, Shamir und Adleman haben damit eine Funktion geschaffen, welche nur mit Kenntnis von *p* und *q* umgekehrt werden kann.

In der Praxis werden zur Verschlüsselung von Nachrichten sogenannte Hybridverfahren eingesetzt. Es handelt sich dabei um die gemeinsame Verwendung einer symmetrischen Verschlüsselung zur Chiffrierung der Daten und eines asymmetrischen Verfahrens zum Austausch des dafür benötigten gemeinsamen Schlüssel.

Open-Source-Produkte, wie asymmetrische Algorithmen, gelten als besonders vertrauenswürdig, da sie die Option beinhalten, die Sicherheitsfunktionen wirksamen Prüfprozessen zu unterwerfen. Die Offenlegung der Sourcecodes bildet ein wichtiges Verkaufsargument und wird zunehmend als eine Möglichkeit der Vertrauensgenerierung angesehen.

5. Hashfunktion und elektronische Signatur

5.1 Hashfunktion

Hashfunktionen dienen allgemein dazu, die Unverfälschtheit, also die Integrität von Texten oder Daten nachzuweisen. Kryptographische Hashfunktionen sind demnach mathematische Methoden, die aus einem beliebigen Klartext nach einem vorbestimmten Verfahren ein Kommprimat im Sinne einer Prüfziffer generieren. Eine solche Funktion verwandelt einen Klartext derart in ein entsprechendes Kommprimat, den sogenannten Hashwert, dass auch die kleinste Veränderung des ursprünglichen Texts zu einem gänzlich anderen Kommprimat führt.
Es gehört zu den Anforderungen an diese mathematische Funktion, dass aus dem einmal erzeugten Hashwert der ursprüngliche Text nicht wieder rekonstruiert werden kann.[19] Außerdem sollte die Hash-Funktion möglichst kollisionsfrei sein, das heißt es sollte nicht leicht möglich sein, zwei Nachrichten zu konstruieren, die den gleichen Hashwert haben. Um die Integrität von Daten nachzuweisen, wird von den Daten der Hashwert berechnet. Wenn zu einem späteren Zeitpunkt eine erneute Berechnung des Hashwerts aus dem vermeintlich gleichen Text zu einem anderen Ergebnis führt kann die Verfälschung des Texts angenommen werden.

Der Vorteil dieses Verfahrens liegt in der Tatsache, dass zur Integritätssicherung nicht der gesamte Text, sondern lediglich ein vergleichbar kurzer Hashwert besonders geschützt, gespeichert oder übermittelt werden muss. Diese Eigenschaft macht sich im Folgenden die digitale Signatur zu nutzen. Da die Hash-Verfahren öffentlich bekannt sind, kann jeder ausgehend vom ursprünglichen Klartext selbst den Hashwert errechnen und durch

[18] vgl. Geheime Botschaften Seite 452
[19] vgl. Safer Net Seite 114

Vergleich feststellen, ob der mitgelieferte Hashwert des Senders mit dem eigenen Ergebnissen identisch ist. In dieser Weise kann durch jeden überprüft werden, ob ein bestimmtes Hashergebnis auch wirklich einer bestimmten Nachricht zuzuordnen ist.[20]

Prüfsummen sind nicht brauchbar zur Bildung kryptographischer Hashfunktionen, da es leicht möglich ist Nachrichten mit der gleichen Prüfsumme zu konstruieren, zum Beispiel ergibt eine Überweisung von 2580 DM auf das Konto 82677365 dieselbe Quersumme wie eine Überweisung von 2980 DM auf das Konto 71234599 eines Angreifers[21].

5.2 Digitale Signatur

Die digitale Signatur kann zur Integritätssicherung von Daten, zur Authentifizierung des Kommunikationspartners und zur Unwiderrufbarkeit von Nachrichten verwendet werden. Mit Hilfe der digitalen Signatur unterzeichnet ein Absender seine Nachricht. Sie basiert auf der Public-Key Verschlüsselung. Dabei werden Daten mit dem geheimen privaten Schlüssel des Absenders unterschrieben**,** und mit dem zugehörigem öffentlichen Schlüssel wird durch den Empfänger die Unterschrift auf Echtheit geprüft. Aus Effizienzgründen wird dabei wie folgt vorgegangen:
Der Absender A erzeugt einen Hashwert seiner Nachricht, verschlüsselt ihn mit seinem privaten Schlüssel und verschickt die unverschlüsselte Nachricht und den verschlüsselten Hashwert zum Empfänger B. Der Absender verschlüsselt zur Authentifizierung diesen Hashwert mit seinem privaten Schlüssel. Bei der Übertragung kann ein Angreifer die Nachricht ausspähen und versuchen, den privaten Schlüssel herauszufinden, um später unter falscher Identität Nachrichten verschicken zu können. Da er ebenfalls Zugriff auf den öffentlichen Schlüssel hat kann auch er die Nachricht lesen. Somit ist bei der Übertragung nur Authentizität jedoch keine Vertraulichkeit gegeben.
Der Empfänger B entschlüsselt den Hashwert mit dem öffentlichen Schlüssel des Absenders A und errechnet selber den Hashwert der empfangenen Nachricht und vergleicht diesen Hashwert mit dem entschlüsselten Hashwert. Sind beide gleich, so stammt die Nachricht vom Absender A und die Datenintegrität ist gewährleistet. Der Empfänger B kann wiederum den aus den empfangenen Daten resultierenden Hashwert mit seinem eigenen privaten Schlüssel signieren und als Empfangsquittung zurücksenden[22].

6. Rechtliche Grundlagen

Der deutsche Gesetzgeber behandelt Authentikations- und Konzelationssysteme getrennt, obwohl beides kryptographische Verfahren sind. Während erste mittlerweile eine recht ausführliche gesetzliche Regelung erfahren haben, verbleiben letztere weitgehend ungeregelt. Die Differenzierung zwischen Signatur- und Verschlüsselungsverfahren erscheint gerechtfertigt, da sie aus juristischer Sicht völlig unterschiedlichen Zwecken dienen, die Erwartungen der Benutzer an die Systeme verschieden sind und sich auch jeweils andere Probleme ergeben.

6.1 Kryptographie

Der Einsatz von Verschlüsselungsprodukten ist in vielen Ländern der Welt seit jeher staatlichen Verboten oder starken Kontrollen unterworfen worden. Auch zulässige Überwachungsmaßnahmen, etwa der Strafverfolgungsbehörden, könnten eventuell

[20] vgl. www.hausarbeiten.de/cgi-bin/superDBdruck.pl/archiv/bwl/bwl-datensich/bwl-datensich.shtml
[21] vgl. Moderne Verfahren der Kryptographie Seite 13
[22] vgl. www.hausarbeiten.de/cgi-bin/superDBdruck.pl/archiv/bwl/bwl-datensich/bwl-datensich.shtml

beeinträchtigt werden, wenn starke Verschlüsselungsprodukte die Telekommunikationswege unzugänglich machen.[23]

Bislang stellt der Missbrauch von Verschlüsselung in Deutschland für die Strafverfolgung kein Problem dar, eine Prognose lässt sich hieraus allerdings nicht ableiten. Es ist in Deutschland daher wohl erforderlich aktive Technikfolgenabschätzung im Hinblick auf die Belange der Strafverfolgungs- und Sicherheitsbehörden zu betreiben, um Fehlentwickelungen frühzeitig zu erkennen.[24]

Andererseits besteht seitens der privaten Anwender ein starkes Interesse am Schutz ihrer Privatsphäre. Auch Wirtschaft und Industrie sind schon aus Wettbewerbsgründen auf den Schutz von Geschäfts- oder Produktionsverfahren angewiesen.

In der Bundesrepublik Deutschland gibt es keine gesetzliche Regelung zur Beschränkung der Entwicklung, der Produktion, der Vermarktung, der Einfuhr oder der Benutzung von Verschlüsselungsprodukten. Lediglich der Export ist durch die zwischenstaatlichen Vereinbarungen des Wassenaar-Abkommens, des darauf basierenden EG-Rechts, das wiederum in das deutsche Ausfuhrrecht eingebunden ist, geregelt.[25]

In den vergangenen Jahren gab es national und auch international in allen interessierten Kreisen Erörterungen über die Notwendigkeit und Zulässigkeit von Beschränkungen. Dabei zeigte sich verstärkt, dass für das Wachstum der elektronischen Kommunikation und vor allem des E-Commerce eine sichere Kommunikation unerlässlich ist. Besonders die USA hatten international für eine verstärkte Kontrolle von starken Kryptoprodukten mit ihrem Sonderbotschafter Aaron geworben. Erst jüngst (Anfang 2000) haben die USA ihre Haltung gelockert, und geänderte Exportkontrollregelungen eingeführt.[26]

Die Aufhebung der Exportbeschränkung für PGP nach zehn Jahren zeigt, dass der Trend in Richtung Liberalisierung weist. Experten erwarten, dass die Kryptodebatte in den USA so lange fortgesetzt wird, bis die letzten Restriktionen aufgehoben sind. Als Folge davon wird in den nächsten Jahren mit einer erheblichen Verschärfung der Wettbewerbssituation auf den Weltkryptomärkten zu rechnen sein. Bisher profitierten nationale Kryptoindustrien von den Exportbeschränkungen der USA, durch die das Produktangebot auf dem Weltmarkt eingeschränkt wurde. Für die im internationalen Vergleich quantitativ und qualitativ dominierende US-Kryptowirtschaft stellte diese Regelung bisher ein erhebliches Hemmnis dar. Der aus dem Vertrauensvorsprung resultierende Marktvorteil deutscher Produkte („Buy German“) könnte also künftig erheblich relativiert werden. Des weiteren ist damit zu rechnen, dass US-amerikanische Anbieter sich durch Übernahmen nationaler Unternehmen Zutritt zu den Auslandsmärkten verschaffen.[27]

Vor diesem Hintergrund hat sich der Bundesminister für Wirtschaft und Technologie für die Bekräftigung und Klarstellung des ungehinderten Einsatzes von starken Verschlüsselungsprodukten eingesetzt (sogenannter Kryptoeckwertebeschluss des Bundeskabinetts vom Juni 1999). So sind von der Entwicklung, der Produktion über das

[23] vgl. www.sicherheit-im-internet.de/themes/themes.phtml?ttid=39&tsid=208&tdid=60&page=0
[24] vgl. www.sicherheit-im-internet.de/themes/themes.phtml?ttid=4&tsid=100&tdid=116&page=0
[25] vgl. www.sicherheit-im-internet.de/themes/themes.phtml?ttid=39&tsid=208&tdid=60&page=0
[26] vgl. www.sicherheit-im-internet.de/themes/themes.phtml?ttid=4&tdid=375
[27] vgl. www.sicherheit-im-internet.de/themes/themes.phtml?ttid=39&tsid=208&tdid=60&page=0

Vermarkten oder Einführen bis hin zum Gebrauch beim Anwender, Verschlüsselungsprodukte in jeder Stärke unkontrolliert zugelassen.

Auch andere Länder, wie z.B. Großbritannien, Kanada und Irland, verfolgen einen vergleichbaren Ansatz. Erst zu Beginn des Jahres 1999 hat die französische Regierung die bis dahin stark beschränkte Nutzung von Kryptoprodukten gelockert.

Mit der Haltung der Bundesregierung für einen unbeschränkten Einsatz von starken Verschlüsselungsprodukten steht dem Anwender und Verbraucher ein Mittel zum effizienten Schutz seiner Daten zur Verfügung.

Gleichzeitig erhält mit dieser Politik die deutsche Industrie die Chance, sich vor einem verlässlichen Hintergrund weiterhin als Anbieter von qualifizierten Verschlüsselungsprodukten im Weltmarkt zu positionieren; denn auch andere Industrieländer haben erkannt, welche wirtschaftlichen Möglichkeiten vor allem im eCommerce vorhanden sind, wenn Produkte zur Sicherung der Kommunikation eingesetzt werden können.[28]

6.2 Digitale Signatur

Bundeswirtschaftsminister Dr. Werner Müller: "Mit dem neuen Signaturgesetz, mit dem Deutschland als eines der ersten Länder Europas die Richtlinie für den elektronischen Geschäftsverkehr umsetzt, stellen wir die entscheidenden Weichen für einen europäischen Binnenmarkt für E-Commerce".

Das Gesetz regelt die erforderliche Sicherheitsinfrastruktur für elektronische Signaturen mit Rechtswirkung, die "qualifizierten elektronischen Signaturen". Gleichzeitig greift der Entwurf die Ergebnisse der Evaluierung des seit 1997 geltenden Signaturgesetzes auf.

Die Rechtswirkung dieser Signaturen wird nicht im Signaturgesetz geregelt, sondern ist Gegenstand eines Gesetzentwurfs zur Anpassung der Formvorschriften des Privatrechts an den modernen Rechtsgeschäftsverkehr, der zeitnah zum Signaturgesetz in den Bundestag eingebracht werden soll. Eine Anpassung der Formvorschriften im öffentlichen Recht ist in Vorbereitung.
Das Signaturgesetz sieht folgende wesentliche Anpassungen an die EG-Signaturrichtlinie vor:

Festlegung von EU-weit einheitlichen rechtlichen Rahmenbedingungen für elektronische Signaturen mit Rechtswirkung. Angleichung der allgemeinen Sicherheitsanforderungen an Zertifizierungsstellen und technische Signaturkomponenten entsprechend dem gemeinsamen europäischen Standard der Signaturrichtlinie. Wegfall der Genehmigungspflicht für Zertifizierungsstellen nach geltendem Signaturgesetz; stattdessen Einführung eines allgemeinen Aufsichtssystems entsprechend der Signaturrichtlinie. Beibehaltung des Sicherheitsniveaus nach geltendem Signaturgesetz bei der Prüfung von Zertifizierungsstellen und technischen Signaturkomponenten über die Einführung einer freiwilligen Akkreditierung für Zertifizierungsdiensteanbieter; akkreditierte Zertifizierungsdiensteanbieter erhalten die Berechtigung, im Geschäftsverkehr mit der umfassend geprüften Sicherheit für ihre Zertifikate werben zu können. Bestandsschutzregelung für Zertifizierungsdiensteanbieter, die bereits nach geltendem Signaturgesetz geprüfte Leistungen oder Produkte anbieten. Aufnahme einer Regelung zur

[28] vgl. www.sicherheit-im-internet.de/themes/themes.phtml?ttid=39&tsid=208&tdid=60&page=0

Haftung von Zertifizierungsdiensteanbietern verbunden mit der Verpflichtung zur ausreichenden Deckungsvorsorge. Außerdem greift das Gesetz die Ergebnisse der Evaluierung des geltenden Signaturgesetzes durch Klarstellungen, z.B. hinsichtlich der Befugnisse der Berufskammern oder der Funktionen der Zertifizierungsdiensteanbieter, auf.

Minister Müller: "Wir wollen mit der Gesetzesnovelle den internationalen Erfahrungsvorsprung Deutschlands im Bereich der elektronischen Signaturen erhalten und ausbauen. Ich bin zuversichtlich, dass die elektronische Unterschrift auch im Alltag bald zur Normalität wird."

Das Gesetz umfasst eine breite Palette von Regelungen. Diese reichen von der Festschreibung der Zulassungsfreiheit für Diensteanbieter, der Anbieterkennzeichnung und Preisangabenregelung über die kommerzielle Kommunikation (Werbung, Sponsoring, Öffentlichkeitsarbeit u.a.) bis zum elektronischen Vertragsabschluss, zur Verantwortlichkeit von Diensteanbietern und zur Einführung von Streitschlichtungsverfahren und Verhaltenskodizes. Müller: "Die Diensteanbieter des E-Commerce brauchen rasch einen zuverlässigen Rechtsrahmen in diesem äußerst dynamischen Wirtschaftsbereich.“[29]

Das Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften ist am 16. Mai 2001 in Kraft getreten.

7. Position und Chancen

7.1 Gesamtwirtschaftliche Bedeutung

Die wirtschaftliche Bedeutung der deutschen Kryptoindustrie ist beträchtlich. Sie besteht zum einen im direkten Beitrag der Anbieter zur gesamtwirtschaftlichen Wertschöpfung. Prognosen gehen von jährlichen Wachstumsraten von 30% in Deutschland aus, noch optimistischere Schätzungen sprechen von einer Verdoppelung. Das Weltmarktpotenzial für Kryptoware wächst voraussichtlich in den nächsten Jahren auf ein Niveau zwischen 11 und 44 Mrd. US$. Zum anderen gibt es bedeutsame indirekte Effekte. Sie resultieren aus dem Schutz der Informationsressourcen von Unternehmen sowie aus der Generierung von Vertrauen in die Sicherheit elektronischer Transaktionen. In einem Hochtechnologieland wie der Bundesrepublik gehören Information und Wissen zu den wertvollsten Produktionsfaktoren. Sicherheit wird damit zum Standortfaktor.

7.2 Überblick Kryptomarkt

Der Markt für Kryptoware ist ein äußerst dynamischer Wachstumsmarkt, der in den nächsten Jahren große Chancen für deutsche Unternehmen bietet.

Die Entwicklung der Märkte für Kryptoware gehört weltweit zu den innovativsten und vielversprechendsten der IT-Industrie. Vor allem das zunehmende Sicherheitsbewußtsein bei der Nutzung offener Datennetze läßt eine erhebliche Nachfragesteigerung erwarten. Produktsparten wie Public Key Infrastructure (PKI), Verschlüsselung und Authentifikation sowie die damit verbundenen Dienstleistungen entwickeln sich besonders dynamisch.

[29] http://www.sicherheit-im-internet.de/themes/themes.phtml?ttid=38&tsid=100&tdid=442&page=0

Nicht zuletzt aufgrund der liberalen Rahmenbedingungen wird deutscher Kryptoware ein hohes Maß an Vertrauen entgegengebracht. Die Geschäftserwartungen sind bei den deutschen Anbietern durchgehend positiv. In der Regel gehen die Unternehmen von einer Umsatzentwicklung aus, die weit über den Wachstumsraten des Weltmarktes liegt. Die Exportquote beträgt über 50%. Als wichtigste Exportländer gelten GB, USA, Skandinavien, Frankreich sowie weitere EU-Länder.

Die Produktpalette der deutschen Hersteller deckt alle entscheidenden Bereiche der Kryptoware und der IT-Sicherheit ab. Freeware- oder Sharewarprodukte spielen - PGP ausgenommen - für deutsche Anwender eine noch untergeordnete Rolle. Während die Hersteller diese Vertriebsform als wenig lukrativ einschätzen, bevorzugen die Anwender einen über die Lieferung des kommerziellen Kryptoproduktes hinausgehenden umfassenden Service. Hierzu gehören z.B. Sicherheitsanalysen, Erarbeitung von Security Policies, Prüfung, Wartung oder eine Hotline-Beratung, die in dieser Form für Freeware nicht vorhanden sind.

Deutsche Unternehmen besitzen im Bereich der Hochsicherheitstechnologie entscheidende komparative Vorteile. Massenmarktgüter spielen eine untergeordnete Rolle. Offenbar schätzen die Unternehmen ihre Wettbewerbsfähigkeit in diesem Bereich zu pessimistisch ein. Experten sehen die Ursache dafür u.a. in Marketingdefiziten.

Fast die Hälfte der deutschen Kryptounternehmen wurde in den letzten fünf Jahren gegründet. Der Zusammenhang zwischen der Entstehung des Internet und der Gründung von Sicherheitsunternehmen zeigt, dass die deutsche Wirtschaft in der Lage ist, rasch auf die Anforderungen der Märkte zu reagieren. Die Gesamtzahl der Beschäftigten liegt inzwischen bei 2.000 bis 3.000 Mitarbeitern. Hinzu kommen etwa 400 bis 500 Sicherheitsexperten, die für Beratungsunternehmen tätig sind. Insgesamt ist die Kryptobranche stark mittelständisch geprägt.

Im allgemeinen besitzen die Unternehmen die für KMU übliche Rechtsform einer GmbH. Gleichzeitig zeichnet sich ein Trend zum Gang an die Börse ab, um Kapital für weiteres Wachstum zu mobilisieren. Besonders erfolgreich wurde dieser Weg von Unternehmen wie Articon Information Systems AG, Brokat Infosystems AG und Utimaco Safeware AG beschritten. Insgesamt besteht ein Trend zur Konzentration, der jedoch in Hinblick auf die internationale Wettbewerbsfähigkeit der deutschen Unternehmen von Experten als Konsolidierungsprozeß beurteilt wird. Weniger positiv ist zu bewerten, dass KMU von Übernahmen aus dem Ausland bedroht sind und dadurch die nationale Kryptowirtschaft geschwächt wird.

Deutschland gilt bei den Unternehmen als einer der vorteilhaftesten Standorte in Bezug auf die Erfordernisse der Kryptoindustrie. Dennoch werden manche Rahmenbedingungen als hemmend für das weitere Wachstum angesehen. Dazu gehört in erster Linie der Mangel an qualifizierten Arbeitskräften aus dem informationstechnisch-ingenieurswissenschaftlichen Bereich. Als mindestens ebenso bedeutend wird das wenig ausgeprägte Sicherheitsbewußtsein sowohl bei geschäftlichen als auch bei privaten Nutzern beurteilt. Hier sehen die Unternehmen trotz bestehender Initiativen von BMWi, BMI und BSI noch erheblichen Aufklärungsbedarf. Vor allem wird bemängelt, dass Entscheidungskompetenzen zu Sicherheitsfragen noch weitgehend auf der DV-Ebene und nicht in den „Chefetagen“ angesiedelt sind.

Notwendige staatliche Fördermaßnahmen umfassen aus Sicht der Unternehmen die Beibehaltung einer wettbewerbsfreundlichen Politik, die die Öffnung der Märkte

vorantreibt. Daneben ist die Vermittlung von Risikokapital immer noch ein wichtiger Aspekt für die Unternehmen, obwohl die Möglichkeiten in diesem Bereich sich in den letzten Jahren wesentlich verbessert haben. Die Intensivierung der Forschung und die Förderung von Kooperationen zwischen Industrie und Hochschulen wird als zentral erachtet. Ebenfalls beurteilen die Unternehmen die Nachfrage der öffentlichen Hand nach Kryptoware als besonders bedeutsam für die weitere Marktentwicklung. Des weiteren sind eine aktive Standardisierungspolitik und die Senkung von Patentgebühren im europäischen Rahmen aus Sicht der Unternehmen Ansätze für eine aktive Kryptopolitik.

7.3 Forschung und Entwicklung

Eine strategische Relevanz von Patenten wird von den deutschen Unternehmen nur zum Teil gesehen. In Bereich der Kryptoalgorithmen überwiegen US-amerikanische Entwicklungen. Zeit- und Kostenaspekte gelten vor allem auf europäischer Ebene als Hemmfaktoren für die Anmeldung von Patenten.

Deutsche Unternehmen zählen eher zu den Lizenznehmern als den Lizenzgebern. Die Verfügbarkeit von Kryptoalgorithmen wird jedoch nicht als Engpass wahrgenommen. Die Lizenzgebühren werden in der Regel nicht als zu hoch eingeschätzt.

Die Anzahl der im FuE-Bereich beschäftigten Mitarbeiter liegt derzeit schätzungsweise bei etwa 1.000 Personen. Die Ausgaben für Forschung und Entwicklung belaufen sich auf etwa 60 Mio. DM für das Jahr 1998.

„Wissen“ ist für die Kryptoindustrie die wichtigste Ressource. Die Hälfte der Unternehmen unterhält intensive Kooperationsbeziehungen zu Hochschulen und Forschungsinstitutionen. Der Austausch von Erfahrungen, die Bearbeitung von konkreten Projekten sowie die Mitarbeiterrekrutierung stehen dabei im Vordergrund. Die Mehrheit der Unternehmen wünscht sich eine Intensivierung der Kontakte sowie eine stärkere Förderung der Grundlagenforschung in öffentlichen Einrichtungen.[30]

8. Fazit

Durch das illegale Ausspähen, Manipulieren oder Zerstören von Daten werden jährlich Schäden in Milliardenhöhe verursacht. Datensicherheit ist somit zu einem Faktor im Wettbewerb geworden der über Erfolg und Misserfolg von Unternehmen entscheidet. Nur durch den Einsatz starker kryptographischer Produkte lassen sich Angriffe auf Daten effektiv verhindern. In jedem Fall ist die Leistungsfähigkeit kryptographischer Produkte heute größer als jemals zuvor.

Was wir allerdings für das wichtigste Argument für den Einsatz starker Kryptographie halten ist:
„The right to be let alone – the most comprehensive of rights, and the right most valued by civilized men.”.

[30] http://www.sicherheit-im-internet.de/themes/themes.phtml?ttid=4&tdid=375