Einführung in die Geschichte der Telekommunikation

Wintersemester 97/98

Seminarleiter: Prof. Dr. Hartmut Vinçon

Kryptographie

Grundlagen, Geschichte

und derzeitige politische Diskussion

Autor: Andreas Heß

Kirchenweg 2

55262 Heidesheim am Rhein

Matrikelnummer: 530266

5. Januar 1998

Inhaltsverzeichnis

Einleitung

In der heutigen Zeit spielt die Verschlüsselung von Daten mehr als je zuvor eine große und wichtige Rolle in der Telekommunikation.

Gerade die Kommunikation über elektronische Medien, insbesondere E-Mail, machen eine Verschlüsselung oftmals unabdingbar, gerade wenn persönliche oder sicherheitsrelevante Daten, wie beispielsweise Konto- oder Kreditkartennummern beim elektronischen Zahlungsverkehr, übertragen werden sollen, da bei der Übertragung über das Internet prinzipbedingt eine Mail von jedem Rechner aus, der an der Übertragung beteiligt ist, auch gelesen werden kann. Da es sich dabei in einem weltumspannenden Datennetz natürlich um unabsehbar viele Angriffsmöglichkeiten für potentielle „Datenspione“ handelt, ist es nicht machbar, diese Daten unverschlüsselt zu übertragen.

Im ersten Teil des Referats werden zunächst einige Grundlagen, zum Beispiel einige einfache und zum Teil schon sehr alte Verschlüsselungsalgorithmen, gezeigt.

Im zweiten Teil wird die Anwendung von Kryptographie in der Geschichte beleuchtet, zum Beispiel die „Enigma“-Maschinen der Deutschen im zweiten Weltkrieg und wie der Code von den Alliierten geknackt wurde.

Der dritte Teil behandelt schließlich die aktuelle Diskussion in Deutschland um frei zugängliche Kryptographie und ein eventuelles Kryptographieverbot.

Was hier nicht behandelt wird

Einige interessante Themen können leider in der Kürze der vorliegenden Arbeit nicht behandelt werden. Darunter fallen zum Beispiel weitergehende Details zu modernen Algorithmen. Diese können wegen ihrer Komplexität hier nur sehr kurz angesprochen und in ihrer prinzipiellen Funktionsweise erklärt werden, anders als bei den grundlegenden Verfahren, die als Hinführung zum Thema Kryptographie und zum weiteren Verständnis sehr ausführlich erklärt sind.

Auch moderne kryptographische Hardware, wie zum Beispiel Chipkarten und DES-Chiffrierhardware sowie die Verschlüsselungstechnik der PIN auf EC-Karten, ein Thema, mit dem sicher jeder schon einmal zu tun hatte, werden hier nicht behandelt.

Ebenso ist die Steganographie ein eigenes Thema. Die Steganographie versucht, anders als die Kryptologie, die sich nur mit der Chiffrierung von Nachrichten befaßt, schon die Existenz der Nachricht zu verschleiern.

Grundlagen der Kryptographie[1]

Transpositionschiffren

Die Transpositionschiffren sind keine Codierungen, wie man sie sich üblicherweise vorstellt, jedoch spielen sie immer noch eine wichtige Rolle in der Kryptographie.

Bei den Transpositionschiffren bleiben die zu verschlüsselnden „Buchstaben, was sie sind, sie bleiben aber nicht wo sie sind“ [2] Es wird also lediglich die Reihenfolge der Buchstaben verändert. Eine Transpositionschiffre erhält man beispielsweise, indem man einen Text spaltenweise statt zeilenweise aufschreibt, dann aber zeilenweise übermittelt. Dem Empfänger müssen dann, quasi als Schlüssel, die Anzahl der Zeilen bekannt sein.

Beispiel: Aus „`Dieser Text ist geheim`“ wird durch Umwandlung mittels des beschriebenen Verfahrens und einer Zeilenanzahl von 5

```
D R I H
I T S E
E E T I
S X G M
E T E X
```

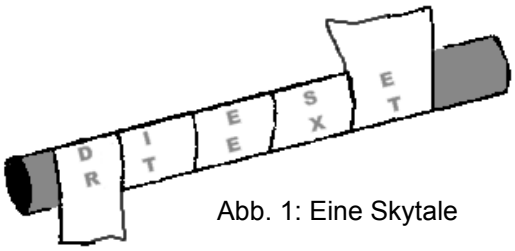


Abb. 1: Eine Skytale

die auf den ersten Blick unlesbare Botschaft „`DRIHITSEEETISYGMETEX`“

Diese Art der Codierung wurde bereits in der Antike von den Griechen benutzt. Zum Übermitteln von Geheimbotschaften verwendete man eine sogenannte „Skytale“, ein Holzstab mit einem festgelegten Durchmesser, um denn dann spiralförmig Pergamentstreifen gewickelt wurde, den der Sender dann von links nach rechts beschrieb.

Die im Bild gezeigte Skytale würde dem oben beschriebenen Zeilen-/Spaltenverfahren entsprechen. Würde man den Pergamentstreifen von oben nach unten lesen, erhielte man nur „`ETEXSXGMITSEDRIH`“, erst, wenn er um eine Skytale mit gleichem Durchmesser gewickelt würde, könnte man den Text wieder lesen.

Dieses Verschlüsselungsverfahren ist allerdings nicht sehr sicher, da es durch simples Ausprobieren in relativ kurzer Zeit geknackt werden kann. Trotzdem spielen Transpositionschiffren auch in modernen Algorithmen eine Rolle, wo sie beispielsweise zum nochmaligen Verschlüsseln bereits mit anderen Methoden verschlüsselter Texte eingesetzt wird.

Das Gegenstück zu den Transpositionschiffren bilden die Substitutionschiffren, die im folgenden vorgestellt werden.

---

[1] Die hier gezeigten einfachen, und zum Teil schon sehr alten Algorithmen werden in sehr vielen Büchern zum Thema Kryptologie behandelt. „Kryptologie“, „Abenteuer Kryptologie“ und die Internet-Seite „Cryptography for Beginners“ sind die Quellen, die hier Eingang gefunden haben, stellen aber für den an weitergehender Lektüre Interessierten nur einen kleinen Ausschnitt einer großen Fülle von Literatur dar.

[2] Kryptologie, S.12

Die monoalphabetische Substitution

Die monoalphabetische Substitution ist ebenfalls eines der einfachsten Verfahren, einen Text zu verschlüsseln. Wie der Name bereits ausdrückt, wird einfach jedem Buchstaben des Alphabets ein entsprechender Geheimbuchstabe zugeordnet. Dieser Geheimbuchstabe kann sich zum Beispiel aus einer Verschiebung des lateinischen Alphabets ergeben, er kann aber auch auf einer Geheimschrift mit völlig anderen Symbolen beruhen. Anders als bei den Transpositionschiffren bleibt also die Reihenfolge der Buchstaben erhalten, jedoch werden die Zeichen selbst verändert.

Auch monoalphabetische Substitutionen wurden bereits in der Antike eingesetzt. Ein Beispiel für eine monoalphabetische Substitution ist beispielsweise der sogenannte „Caesar-Code“, der auf Julius Caesar zurückgeht.[1] Das Geheimalphabet erhält man, indem man das Klartextalphabet um eine bestimmte Buchstabenanzahl verschiebt, also beispielsweise:

Klartext:	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
Geheimtext:	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

Der Schlüssel ist in diesem Falle der Anfangsbuchstabe des Geheimalphabets, also hier D.

Eine andere, ebenfalls schon sehr alte Form der monoalphabetischen Substitution ist das „Atbash“.[2] Bei diesem Verfahren wird das normale Alphabet einfach umgekehrt, d.h. aus A wird Z, aus B wird Y usw. Das Atbash-Verfahren ähnelt dem römischen Caesar-Code, ist aber jüdischen Ursprungs.

Es sind jedoch auch gänzlich andere monoalphabetische Zuordnungen denkbar. Man könnte ja einem Klartextbuchstaben jeden beliebigen anderen Buchstaben oder auch eine Ziffer oder ein geheimes Symbol zuordnen, solange dies eindeutig geschieht. Alle monoalphabetischen Substitutionen haben gemeinsam, daß sie auf äußerst einfach Art realisiert werden können.

Monoalphabetische Substitutionen sind jedoch mit statistischen Verfahren ebenso einfach zu knacken, da jede Sprache eine charakteristische Buchstabenverteilung besitzt. Im Deutschen und im Englischen ist beispielsweise E der am häufigsten vorkommende Buchstabe, also wird im Geheimtext das am häufigsten vorkommende Symbol möglicherweise das E repräsentieren.

[1] Kryptologie, S.13; Cryptography for Beginners
[2] Cryptography for Beginners

Die polyalphabetische Substitution

Die leichte Angreifbarkeit der monoalphabetischen Substitution führte dazu, daß man sich Gedanken machte, wie man die relativen Häufigkeiten der einzelnen Buchstaben im verschlüsselten Text verschleiern könnte, so daß der Angriff mittels Statistik erschwert wird.

Die homophone Chiffre[1]

Ein erster Versuch war die sogenannte homophone Chiffrierung. Hierbei wird häufig vorkommenden Buchstaben nicht ein geheimes Äquivalent, sondern mehrere Geheimzeichen zugeordnet. Da beispielsweise das `E` ein sehr häufig vorkommender Buchstabe ist, wird man ihm z.B. 10 verschiedene Geheimzeichen zuordnen, während dem `L` z.B. nur 3 oder dem `X` nur ein Zeichen zugeordnet ist. Da die umgekehrte Zuordnung jedoch nach wie vor eindeutig sein muß, d.h. ein Zeichen des Geheimtextes darf nur genau eine Bedeutung haben, während ein Klartextzeichen natürlich mehrere zugeordnete Zeichen hat, können die Zeichen des Geheimtextes natürlich keine Buchstaben sein, es würden sich beispielsweise Zahlen oder Buchstabenpaare anbieten. Zwar verschleiert dieses Verfahren die Buchstabenhäufigkeiten ziemlich gut, allerdings ist eine Kryptanalyse („Knacken“ des Codes) auch hier noch recht einfach möglich.[2]

Das Vigenère-Verfahren[3]

Ein besserer Ansatz ist das Vigenère-Verfahren. Es basiert darauf, daß für die einzelnen Buchstaben des Klartextes zum Verschlüsseln nicht dieselbe, sondern mehrere verschiedene monoalphabetische Verschlüsselungen verwendet werden und geht auf den „französischen Diplomaten Blaise de Vigenère (1523 bis 1596)“[4] zurück. Der Schlüssel ist dann nicht mehr, wie bei der Cäsar-Verschlüsselung, der Buchstabe, mit dem das verschobene Alphabet beginnt (s.o.), sondern ein Wort, wobei jeder Buchstabe des Schlüsselwortes für eine Cäsar-Verschlüsselung steht. Lautet das Schlüsselwort beispielsweise `GESICHRT`, so ergeben sich 8 verschiedene Cäsar-Verschlüsselungen, die rotierend auf den Test angewandt werden. Lautet der zu verschlüsselnde Text „`Dieser Text wurde gegen unbefugtes Lesen gesichert`“, ergibt sich:

```
Klartext:         DIESERTEXTWURDEGEGENUNBEFUGTESLESENGESICHERT
Schlüsselbuchst.: GESICHRTGESICHRTGESICHRTGESICHRTGESICHRTGESI
```

Es ergibt sich also, abhängig von der Position des Klartextbuchstaben, eine jeweils andere Cäsar-Verschlüsselung. Auch entspricht die statistische Buchstabenverteilung des verschlüsselten Textes keiner Charakteristik mehr, so daß die Zuordnung der Geheimsymbole

[1] Kryptologie, S. 36

[2] Auf die genauen Verfahren der Kryptanalyse kann hier nicht im Detail eingegangen werden, da dies den Rahmen des Referats sprengen würde. Zu allen einfachen Verfahren, die hier besprochen werden, existieren natürlich auch ebenso einfache Methoden, sie zu umgehen. In „Kryptologie“ finden sich bei den Beschreibungen der Algorithmen auch gleich die Methoden, wie man diese knacken kann. In „Abenteuer Kryptologie“ ist dem Thema Kryptanalyse ein ganzes Kapitel gewidmet.

[3] Kryptologie, S. 37

[4] Kryptologie, S. 37

zu den Klartextsymbolen nicht so einfach wie bei der monoalphabetischen Substitution möglich ist.

Ist jedoch die Schlüssellänge bekannt, läßt sich die Vigenère-Verschlüsselung bei der Analyse eines Geheimtextes auf Cäsar-Verschlüsselungen zurückführen, da der Schlüssel ja periodisch wiederholt wird. Betrachtet man also jedes Zeichen, das mit dem gleichen Schlüsselbuchstaben verschlüsselt wurde (in unserem Beispiel also jedes 8. Zeichen), so gehorchen diese Geheimzeichen wieder der gleichen Häufigkeitsverteilung wie bei der monoalphabetischen Substitution. Die Schlüssellänge läßt sich mit geeigneten statistischen Verfahren leicht bestimmen.[1]

Obwohl diese Unsicherheit des Vigenère-Algorithmus natürlich bekannt ist, wird er sogar in moderner Software noch eingesetzt, zum Beispiel bei der Textverarbeitung WordPerfect.[2]

Dies zeigt, wie wenig man sich auf diese Art von Verschlüsselung verlassen kann. Zum Glück gibt es für wichtige Daten natürlich auch Alternativen, wie die modernen Algorithmen zeigen, aber dazu später.

Das One-Time-Pad[3]

Ist allerdings der Schlüssel annähernd so lang wie der Text, der verschlüsselt werden soll, lassen sich auf diese Art und Weise natürlich keine Gesetzmäßigkeiten mehr feststellen, da man dann ja keine Buchstabengruppe mehr erhält, die mit dem gleichen Schlüsselbuchstaben verschlüsselt worden ist! Diesem Verfahren kommt in der Kryptologie eine Sonderrolle zu: Es ist das einzige Verfahren, das sogar mathematisch beweisbar sicher ist, allerdings nur so lange, wie als Schlüsselbuchstaben eine rein zufällige Buchstabenfolge verwendet wird, die absolut keiner Gesetzmäßigkeit mehr gehorcht. Diese besondere Art der polyalphabetischen Substitution wird auch als „One-Time-Pad“ bezeichnet.

Da ein solcher Schlüssel natürlich nicht leicht übermittelt werden kann, ist dies auch das größte Problem dieses Verfahrens. Man könnte natürlich auf die Idee kommen, ein literarisches Werk als Schlüssel zu verwenden, die nötige Information zum Rekonstruieren der Nachricht könnte dem Empfänger leicht übermittelt werden, er braucht sich dann nur das entsprechende Werk zu besorgen. Allerdings ist die Folge von Schlüsselbuchstaben dann natürlich nicht mehr zufällig, sondern gehorcht den selben statistischen Verteilungen, die wir uns schon beim Knacken der monoalphabetischen Substitution zunutze gemacht haben. Also ist in diesem Fall keine Sicherheit mehr gewährleistet.

Abwandlungen des One-Time-Pad-Verfahrens werden manchmal auch in modernen Verschlüsselungsprogrammen verwendet. Zur Schlüsselgenerierung wird dann eine Pseudo-Zufallszahlenfolge verwendet. Die Qualität des Verfahrens hängt dann im wesentlichen von der Qualität der generierten Zahlenfolge ab.

[1] Kryptologie, S. 39
[2] Wie die WordPerfect-Verschlüsselung gebrochen wird, ist in „Abenteuer Kryptologie“ ab S. 72 beschrieben. Im Buch und auf der Begleit-CD findet sich ein dokumentiertes Programm, das diese Aufgabe erledigt.
[3] Kryptologie, S. 49, S. 55

Moderne Verschlüsselungsalgorithmen

Von den bisher besprochenen Verschlüsselungsalgorithmen sind wegen der beschriebenen Unsicherheiten nur noch Varianten des One-Time-Pad, und leider trotz der bekannten Unsicherheit auch des Vigenère-Verfahrens, im Gebrauch.

Daher sollen im folgenden einige moderne Verfahren kurz genannt werden. Die Beschreibung kann jedoch nicht so ausführlich wie bei den einfachen Verfahren sein, da die modernen Algorithmen meist sehr viel komplexer sind und einige Mathematik voraussetzen.

Feistel-Netzwerke[1] (DES)

Anfang der 70er Jahre wurde von dem IBM-Mitarbeiter Horst Feistel das Konzept der Feistel-Netzwerke veröffentlicht, die die Basis für viele moderne Verfahren bildet, darunter auch das vor allem im Bankwesen sehr gebräuchliche DES (Data Encryption Standard). Im Gegensatz zu den bisher besprochenen Algorithmen, bei denen es sich um sogenannte Stromchiffren handelte, sind die Feistel-Netzwerke sogenannte Blockchiffren. Das bedeutet, daß der Klartext zunächst in gleichlange Blöcke geteilt werden muß, die dann durch den Algorithmus in ebenfalls gleichlange Geheimtextblöcke überführt werden.

Bei den Feistel-Netzwerken wird zunächst der Klartextblock in zwei gleichgroße Halbblöcke geteilt und in zwei neue Halbblöcke überführt. Als neuer linker Block wird der alte rechte Halbblock genommen, zur Berechnung des neuen rechten Halbblocks wird der alte rechte Halbblock mit einer Funktion f, die sich aus dem Schlüssel und einem veränderlichen Rundenschlüssel ergibt, verschlüsselt und anschließend mit den alten linken Halbblock bitweise Exklusiv-Oder verknüpft. Dies wird nun mehrmals, jeweils von den neuen, sich ergebenden Halbblöcken ausgehend, mit verschiedenen Rundenschlüsseln wiederholt. Ein solcher Durchlauf heißt auch eine Runde.

Die Besonderheit dieses Verfahrens besteht darin, daß man mittels Umformungen der sich daraus ergebenden Gleichungen die Geheimtexte dechiffrieren kann, ohne daß die Funktion f umkehrbar sein muß.

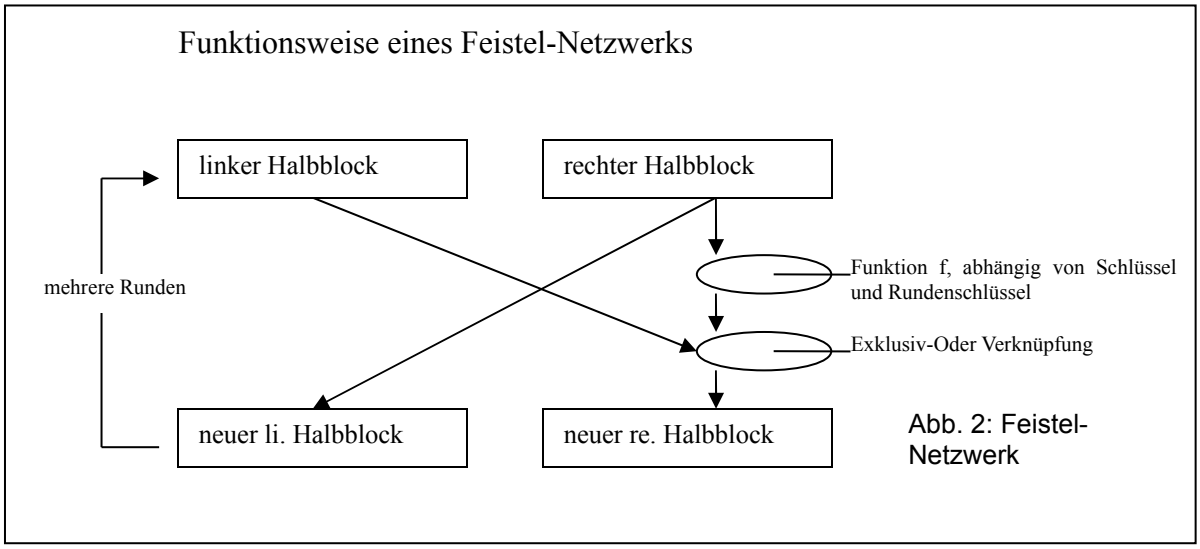


Abb. 2: Feistel-Netzwerk

[1] Abenteuer Kryptologie, S. 112 ff
Hier sind die Feistel-Netzwerke und speziell auch der DES-Algorithmus recht detailliert beschrieben.

Wie schon erwähnt, ist der DES-Algorithmus ein solches Feistel-Netzwerk und „verwendet einen 56 Bit langen Schlüssel, um blockweise 64 Bit Klartext in 64 Bit Geheimtext zu überführen bzw. umgekehrt. Das geschieht in 16 schlüsselabhängigen Runden.“[1]

Anwendungsgebiete von DES sind neben dem Bankwesen z.B. auch die Paßwortverschlüsselung bei Unix-Systemen. Zwar gilt der DES-Algorithmus immer noch als sehr sicher, jedoch sind bestimmte Angriffe, die meistens auf ein systematisches Durchprobieren aller möglicher 2^{56} Schlüssel hinauslaufen, nicht ausgeschlossen. Diese Angriffe haben alle gemeinsam, daß sie nur mit sehr großem Aufwand an Hardware und Zeit realisiert werden können. Eine mit DES verschlüsselte Chiffre könnte daher möglicherweise, wenn man berücksichtigt, daß das Brechen des Codes auch als Dienstleistung angeboten werden könnte, schon unter Aufwand einer „fünf- oder sechsstellige[n] Summe“[2] geknackt werden.

Asymmetrische Verfahren (RSA)

Die bisher betrachteten Verfahren sind zwar teilweise sehr sicher, sie haben aber alle das Problem der Schlüsselübermittlung gemeinsam: Sowohl der Sender als auch der Empfänger benötigen einen geheimen Schlüssel, der vorher auf einem sicheren Weg übertragen werden muß. Weil derselbe Schlüssel sowohl zum Chiffrieren als auch zum Dechiffrieren verwendet wird, spricht man auch von symmetrischen Verfahren.

Eine Lösung dieses Problems bieten jedoch die neuen, asymmetrischen Verfahren. Hierbei findet sowohl ein geheimer als auch ein öffentlicher Schlüssel Verwendung. Der geheime Schlüssel kann aus dem öffentlichen Schlüssel nicht hergeleitet werden. Da hierbei die Problematik des Schlüsselaustauschs wegfällt, wird diese Art der Chiffrierung heute sehr oft für E-Mails angewandt.

Will eine Person A einer Person B eine verschlüsselte Nachricht zukommen lassen, so benötigt A zunächst den öffentlichen Schlüssel von B. Dieser kann von B gefahrlos bekanntgegeben werden, da er nur zum Verschlüsseln dient, nicht aber zum Entschlüsseln. Hierfür benutzt B den geheimen Schlüssel, der von B unter Verschluß gehalten wird.

Einige asymmetrische Verfahren, darunter das bekannte RSA, ermöglichen darüber hinaus die Erstellung von sogenannten digitalen Unterschriften. Hierbei wird das Verfahren einfach „umgekehrt“ angewandt: Der geheime Schlüssel wird zum Chiffrieren verwendet, und die erhaltene Nachricht kann dann mit dem öffentlichen Schlüssel dechiffriert werden. Damit gilt also jede Nachricht, die mit einem öffentlichen Schlüssel dechiffriert werden kann, als authentisch, da sie mit dem geheimen Schlüssel, der unter Verschluß ist, verschlüsselt worden sein muß.

Obwohl das Verfahren zu komplex ist, als daß man es hier in Kürze beschreiben könnte, soll wenigstens der Ansatz des wohl populärsten asymmetrischen Algorithmus, des RSA-Algorithmus, der unter anderem in dem bekannten Programm PGP verwendet wird, kurz gezeigt werden: Möglich wird ein solches Verfahren durch die mathematischen Probleme des diskreten Logarithmus, also die nach x aufgelöste Form einer Gleichung der Form
$a^x = g \bmod n$. Da wir hier Modulo, also ganzzahlig mit Rest, rechnen, ist die Lösung nicht etwas $\log_a(g)$, sondern insbesondere für große n sehr schwierig herzuleiten. Desweiteren spielt das Problem der Faktorisierung großer Zahlen der Form p*q, p und q seien Primzahlen, eine

[1] Abenteuer Kryptologie, S. 115
[2] Abenteuer Kryptologie, S.120
Hier sind auch nähere Informationen zu den bekannten Angriffen auf DES nachzulesen.

Rolle. Für große Zahlen ist dies nämlich mit einem sehr hohen Aufwand verbunden; im RSA-Algorithmus wird hiermit das Herleiten des geheimen aus dem öffentlichen Schlüssel erschwert. Der RSA-Algorithmus wäre also gebrochen, wenn man ein einfaches Verfahren zur Faktorisierung großer Zahlen finden würde.

Nachteile des RSA-Verfahrens sind der hohe Zeitaufwand für das Chiffrieren und Dechiffrieren sowie die leichte Angreifbarkeit, wenn Teile des Klartextes bekannt sind. Daher wird es in gängiger Software wie z.B. PGP nur verwendet, um einen zufällig generierten und nur für eine Übermittlung benutzten „Sitzungsschlüssel“ für ein symmetrisches Verfahren zu chiffrieren, mit dem der eigentliche Klartext chiffriert wird. Da der Sitzungsschlüssel selbst mit einem sicheren Verfahren verschlüsselt ist, kann er dann gefahrlos zusammen mit der mit dem symmetrischen Verfahren chiffrierten Botschaft übermittelt werden.

Die Verwendung von asymmetrischen Verschlüsselungsalgorithmen erleichtert zwar den Schlüsselaustausch, da ein Teil des Schlüssel ja öffentlich ist und nicht geheimgehalten zu werden braucht, da diese Algorithmen jedoch gerade bei E-Mail-Kontakten angewandt werden, bei der sich die Kommunikationspartner unter Umständen noch nie persönlich begegnet sind, ergibt sich die Fragestellung, ob derjenige, von dem wir den öffentlichen Schlüssel erhalten haben, auch derjenige ist, der er zu sein vorgibt. Ein potentieller Angreifer könnte beispielsweise den E-Mail-Verkehr zwischen zwei Benutzern abfangen, und beiden gefälschte öffentliche Schlüssel zuspielen, indem er vorgibt, der jeweils andere Kommunikationspartner zu sein. Jedoch läßt sich auch diese Gefahr durch geeignete Verfahren minimieren, worauf allerdings nicht näher eingegangen werden soll.

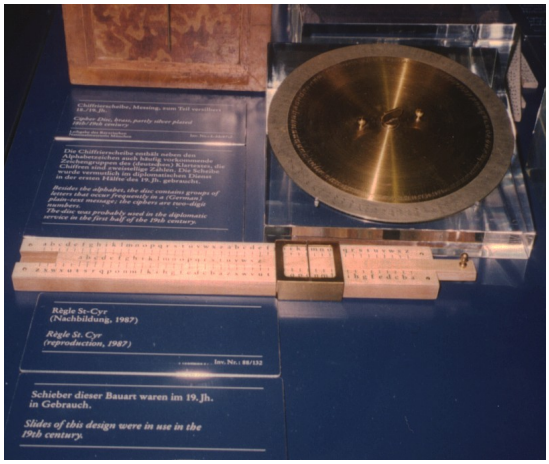
Kryptographie in der Geschichte

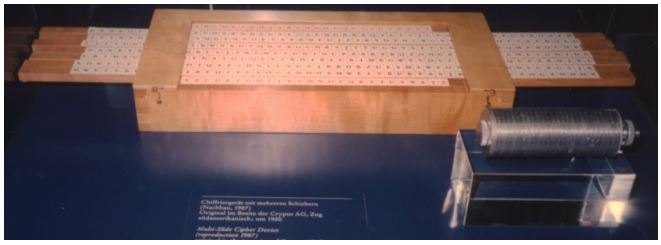
Alte Geräte[1]

Oft denkt man bei Verschlüsselung und Verschlüsselungsgeräten automatisch an den Computer, doch wie bei der Besprechung der Algorithmen erwähnt, sind viele Verfahren bereits sehr alt.

Die monoalphabetischen Verfahren waren noch sehr einfach in der Umsetzung, man ersetzte einfach das normale Alphabet durch ein frei gewähltes. Allerdings wurden schon in der Antike Hilfsmittel für die Verschlüsselung eingesetzt, wie beispielsweise für die Transpositionschiffren die Skytale, ein einfacher Holzstab.

Echte kryptographische Geräte wurden allerdings erst sehr viel später eingeführt, als polyalphabetische Verfahren die Chiffrierung und Dechiffrierung verkomplizierten und sich dadurch bedingt natürlich leicht Fehler in die Texte einschlichen. Bereits im 17. Jahrhundert kamen sogenannte Chiffrierstäbchen auf, die es ermöglichten, polyalphabetische





links: Abb. 3: Chiffrierscheibe aus dem 18./19. Jh. und Nachbau eines Chiffrierschiebers aus dem 19. Jh.

oben: Abb. 4: Nachbau eines Chiffrierschiebers von 1920, Chiffriergerät der US-Army von 1920

Substitutionen auszulegen, um sie direkt abzulesen. Im 18. und 19. Jahrhundert baute man dann Chiffrierscheiben und Chiffrierschieber, wodurch die Anwendung polyalphabetischer Algorithmen gegenüber den Stäbchen noch weiter vereinfacht wurde. Chiffrierschieber und andere Chiffriergeräte für polyalphabetische Chiffren wurden noch bis in die 20er Jahre unseres Jahrhunderts gebaut und eingesetzt. Während die Kryptographie trotz all dieser Geräteentwicklungen früher doch eher eine weniger wichtige Rolle spielte und meist den Diplomaten vorbehalten war, wurde im zweiten Weltkrieg die Kryptographie geradezu kriegsentscheidend.

Kryptographie im Zweiten Weltkrieg: Die Enigma[2]

Technischer Aufbau der Enigma

Vor dem zweiten Weltkrieg wurden die kryptologischen Verfahren durch die Entwicklung sogenannter Rotormaschinen drastisch verbessert. Dieses von mehreren Entwicklern, darunter

[1] Informatik-Ausstellung, S. 105 ff.
[2] Abenteuer Kryptologie, S. 38 ff. sowie Spektrum der Wissenschaft
„Enigma“ von griechisch „Rätsel“

dem Deutschen Arthur Scherbius im Jahre 1918, unabhängig voneinander entwickelte Konzept ermöglichte erstmals die Generierung hinreichend langer Schlüsselfolgen, um die polyalphabetische Substitution sicherer zu machen. Beim Rotorverfahren werden mehrere Scheiben, deren elektrische Verdrahtung das Alphabet abhängig von der Stellung in ein anderes überführt (es wird also eine Substitution durchgeführt), hintereinander geschaltet, und zwar derart, daß die Chiffrierung eines Zeichens die erste Scheibe (d.h. den ersten Rotor) um eine Position weiterdreht. Hat der erste Rotor alle Positionen durchlaufen, dreht er über eine Mechanik (ähnlich wie z.B. in einem Kilometerzähler oder ein sonstiges Zählwerk) den zweiten Rotor um eine Position weiter. Je nach Ausführung der Maschine enthält diese 3 oder mehr Rotoren aus einer größeren Auswahl. Der Schlüssel besteht bei einem solchen Verfahren aus der Auswahl der Rotoren, ihrer Reihenfolge sowie ihrer Anfangsstellung.

Die Enigma wurde zusätzlich zu den Rotoren noch mit einem sogenannten Reflektor, der, nachdem das elektrische Signal alle Rotoren durchlaufen hatte, eine weitere Substitution durchführte und das Signal in umgekehrter Reihenfolge wieder durch die Rotoren leitete, ausgestattet. Jeder Rotor wurde also zweimal durchlaufen. Weiterhin wurde noch ein Steckerbrett verwendet, das die Buchstaben vor und nach dem Durchlaufen der Rotoren noch ein weiteres Mal vertauschte. Die Enigma wurde in mehreren Ausführungen mit 3 oder 4 („Marineausführung“, auf U-Booten verwendet) Rotoren gebaut.

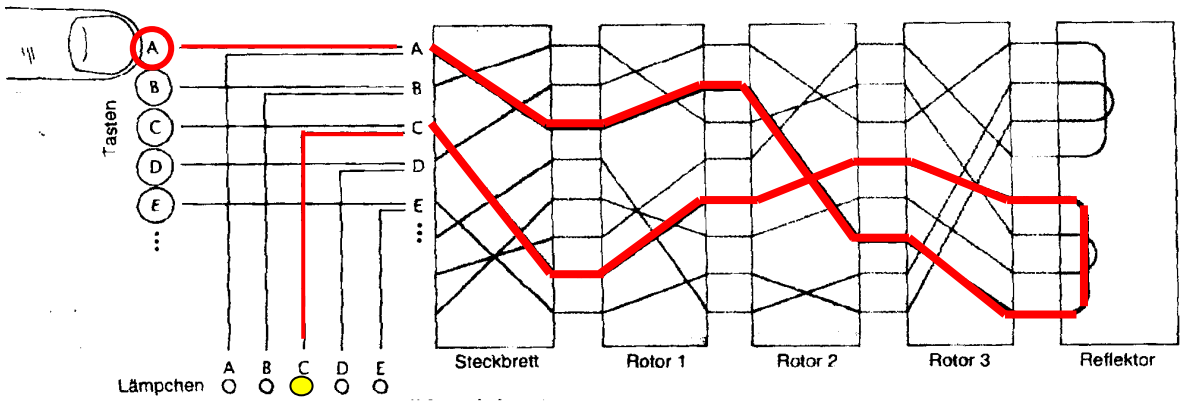


Abb. 5: Die Funktionsweise der Enigma

Wie konnte die Enigma geknackt werden?

Auf den ersten Blick erscheint das Verschlüsselungsverfahren, das in der Enigma Verwendung fand, äußerst sicher. Es handelt sich schließlich um ein Vigenère-Verfahren mit außerordentlich großer Schlüssellänge. Bei einer Enigma mit 3 Rotoren ergibt sich schon eine Schlüssellänge „von $26^3 = 17576$“[1], zum Verschlüsseln von oft nur kurzen Befehlen, Wetterberichten oder dergleichen sicher ausreichend. Wie bereits besprochen, ist ein polyalphabetisches Verfahren dann beweisbar sicher, wenn der Schlüssel genau so lang wie der Text ist und keinerlei Gesetzmäßigkeit unterliegt. Bei einer Schlüssellänge von 17576 ist der Schlüssel sicherlich in den meisten Fällen hinreichend lang, jedoch unterliegt er einigen fatalen Gesetzmäßigkeiten.

Insbesondere die Einführung des „Reflektors“, durch den eigentlich eine Verbesserung der Sicherheit erreicht werden sollte, indem die Schlüssellänge dadurch vergrößert wird, daß das Signal nochmals rückwärts durch alle Rotoren geleitet wird, erwies sich als Fehler. Der Reflektor war nämlich so ausgelegt, daß niemals ein Buchstabe mit sich selbst verschlüsselt wird. Dies erscheint auf den ersten Blick nicht weiter schlimm, bei näherer Betrachtung zeigt

[1] Abenteuer Kryptologie, S. 40

sich jedoch, daß diese Information schon ein wesentliches dazu beitragen kann, den Klartext zu rekonstruieren.

Wenn der potentielle Angreifer nämlich weiß, daß ein bestimmtes Wort im Text enthalten ist, kann er nämlich sofort sehen, an welcher Position es nicht stehen kann.[1] Ein Beispiel soll dies verdeutlichen: Wir schlüpfen in die Rolle der Briten und wissen, daß das Wort „U-Boot“ im Text enthalten sein muß und haben den über Funk übertragenen Befehl abgehört. Da kein Buchstabe des Wortes „U-Boot“ mit sich selbst verschlüsselt worden sein kann, können wir mögliche Positionen des Wortes ausmachen und durch die dann mögliche Zuordnung von Klartext zu Geheimtext Stück für Stück auf den Schlüssel stoßen:

```
Geheimtext:   NVGOXUBNKSLTPT
Vergleich:    UBOOT
               UBOOT
                UBOOT
                 UBOOT
                  UBOOT
                   UBOOT
                    UBOOT
                     UBOOT
                      UBOOT
```

Wir haben also schon herausgefunden, daß das Wort „U-Boot“ nur an 5 von 10 möglichen Stellen, nämlich an den schräg gedruckten, stehen kann.

Wir können zwar jetzt allein aus dieser Information noch nicht den Schlüssel oder den Geheimtext herleiten, jedoch haben wir wichtige Schritte in Richtung auf dieses Ziel gemacht. Außerdem kann man bei dieser sogenannten negativen Mustersuche noch wesentlich bessere Ergebnisse erzielen, wenn ein größerer Teil des Textes, also beispielsweise ein sehr langes Wort oder ein ganzer Abschnitt, bekannt ist.

Diese Schwachstelle alleine wäre nicht ausreichend gewesen, um den Code der Enigma zu knacken, jedoch gibt es noch ein ganze Reihe weiterer Schwachstellen, ganz abgesehen von groben Fehlern, die bei der Bedienung begangen wurden und so wichtige Details über die Schlüssel lieferten.

Die Polen begannen bereits 1927 Informationen über die Enigma zu sammeln, als „ihr Zoll eine Enigma abfing, die versehentlich an eine deutsche Firma in Polen geschickt wurde“[2]. Diese Entwicklung führte 1938 zur Entwicklung von Dechiffriergeräten, die die Schlüsselstellung der Enigma ermittelten. Diese Maschinen bekamen den Namen „Bombe“. Ob sie diesen Namen wegen ihres Tickens[3] erhielten oder weil ihre ursprüngliche Form an eine Eistorte, polnisch „bomba“[4], erinnerte, darüber sind sich die Quellen uneins.

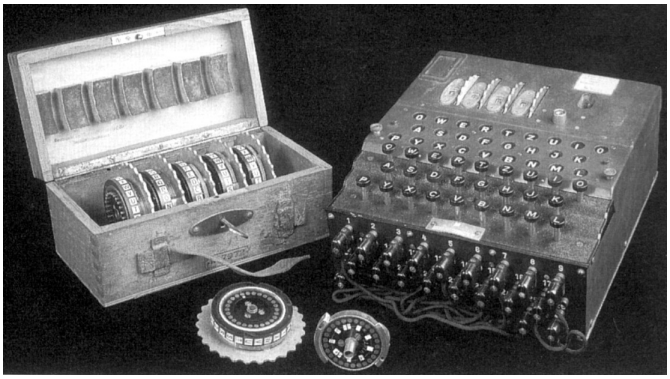
Weil weitere Einzelheiten der Enigmas, zum Beispiel die Beschaffenheit der Rotoren, bereits vorher analysiert worden waren, konnten die mit der Enigma verschlüsselten Funksprüche relativ leicht entschlüsselt werden. Erst 1939, nach mehreren Änderungen an der Enigma,

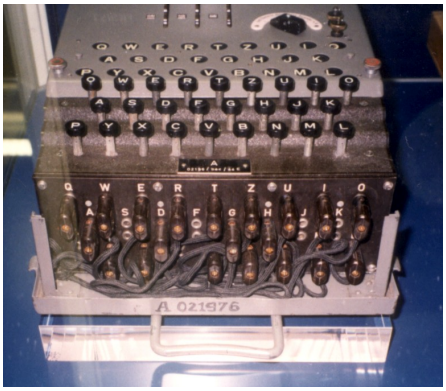
[1] Abenteuer Kryptologie, S. 68
[2] Abenteuer Kryptologie, S. 43
[3] Spektrum der Wissenschaft, S. 182
[4] Abenteuer Kryptologie, S. 46

mußten die Polen aufgeben und gaben ihre Ergebnisse an die Briten weiter, die ihre kryptanalytischen Bemühungen von 1938 an in Bletchley, einer Kleinstadt nördlich von London, in den als „Bletchley Park“ bekannt gewordenen „General Communications Headquarters (GCHQ)“ durchführten. Hier wurden nicht nur die Funksprüche der Enigmas, sondern auch mit der wesentlich komplexeren „Lorenzmaschine“ SZ 42 verschlüsselten Nachrichten erfolgreich analysiert.

Zum Entschlüsseln der Nachrichten wurden von den Briten des weiteren eigens Röhrenrechenmaschinen gebaut. Der Colossus und der Nachfolgetyp Colossus Mark II[1], von dem insgesamt 10 Stück gebaut und in Bletchley genutzt wurden, gelten heute neben Konrad Zuses Relaisrechner Z3 und dem amerikanischen Röhrenrechner ENIAC als die ersten Computer.

Warum es kriegsentscheidend war, daß die Enigma geknackt wurde





links: Abb. 6: Die Enigma in der Marine-Ausführung mit 4 Walzen und Holzkiste zum Aufbewahren der empfindlichen Austauschwalzen

rechts: Abb. 7: Die Enigma in der Ausführung mit 3 Walzen

Insbesondere den Bemühungen der Briten, ihre kryptanalytischen Erkenntnisse geheimzuhalten, ist es zu verdanken, daß die Entschlüsselung der Enigma kriegsentscheidend wurde. Durch verschiedene Taktiken gelang es, die Informationen, die aus der Kryptanalyse der Enigma gewonnen worden waren, einzusetzen, ohne daß die Deutschen Verdacht schöpften. So wurden beispielsweise vor einem Luftangriff auf einen Schiffskonvoi, dessen Position durch abgefangene Funksprüche ermittelt worden war, stets Aufklärungsflugzeuge losgeschickt, um den Eindruck zu erwecken, diese hätten den Konvoi entdeckt.[2] Auch ist von mindestens einem Fall bekannt, in dem die Briten „in einem Code, von dem sie wußten, daß die Deutschen ihn entschlüsseln konnten [...] einem nicht existierenden Agenten [...] für seinen Tip“[3] dankten.

Es gibt sogar Spekulationen, daß vor dem deutschen Luftangriff auf Coventry „ein entsprechender Funkspruch“[4] abgehört und entschlüsselt worden sei, die Briten aber nicht reagierten, um den Deutschen nicht zu verraten, daß die Enigma geknackt worden war.

Aber auch die Tatsache, daß Hitler die deutschen Verschlüsselungsmaschinen Enigma und SZ 42 für absolut sicher hielt und die Deutschen auch kaum eigene Kryptanalyse betrieben, trug wesentlich dazu bei, daß das Geheimnis der Briten gewahrt blieb.

[1] PM, S. 90
[2] PM, S. 89
[3] PM, S. 89
[4] Abenteuer Kryptologie, S. 48

Die Entschlüsselung von Funksprüchen war es auch, die es im Juni 1944 den Alliierten ermöglichten, erfolgreich in der Normandie zu landen. Man wußte dadurch, daß die Deutschen glaubten, die Alliierten wollten den Kanal bei Calais überqueren; ein Gerücht, das diese vorher selbst gestreut hatten.[1]

In Spekulationen über den Verlauf des Kriegs, wenn die Briten die deutschen Codes nicht hätten knacken können, wird davon ausgegangen, daß die Invasion der Alliierten erst später stattgefunden hätte und daß möglicherweise auch Atombomben auf Europa gefallen wären.[2]

Die Enigma nach dem Krieg

Da aufgrund der Geheimhaltungspolitik der Briten bis 1974 (!) nicht öffentlich bekannt war, daß der Algorithmus der Enigma gebrochen worden war, wurden auch nach dem Krieg noch Enigmas verwendet. Wahrscheinlich wurden die Enigmas jedoch teilweise auch mit der Absicht weitergegeben, diejenigen abhören zu können, die immer noch die Enigma verwendeten.[3]

Abb. 8: Auch nach dem Krieg wurden, bevor allgemein Computer Verwendung fanden, noch Verschlüsselungsmaschinen neu entwickelt. Das Bild zeigt ein Rotor-Chiffriergerät mit Zusatz-Lochstreifengerät der Bauart Hagelin-Cryptos Type H (hergestellt von 1963 bis 1965) und ein kleines Taschenchiffriergerät vom Typ Hagelin-Cryptos CD-57. Diese Nachkriegsentwicklungen werden hier jedoch nicht besprochen.

Die aktuelle politische Diskussion um Kryptographie

Auch heute ist die Kryptologie wieder ein heiß diskutiertes Thema, allerdings geht es nicht mehr darum, dem Feind militärische Informationen vorzuenthalten, sondern vor allem um den Einsatz von kryptographischen Verfahren auf breiter Basis.

Während der Einsatz von Kryptographie, wie er beispielsweise im Bankwesen notwendig ist, außer Frage steht, fürchten die Behörden durch die Verschlüsselung von E-Mails, Telefongesprächen oder sonstigen Nachrichten um ihre Abhörmöglichkeiten.

[1] PM, S. 90
[2] Abenteuer Kryptologie, S. 50
[3] Abenteuer Kryptologie, S. 50
Hier finden sich noch detailliertere Angaben zum Einsatz der Enigma nach dem Krieg

Die Kryptographiefrage international

Nationale Regelungen in den USA und Frankreich

Die Kryptographie wird international sehr unterschiedlich aufgefaßt. In den USA beispielsweise gilt Kryptographie gemäß dem Gesetz als Kriegsmunition und unterliegt strengen Exportverboten. Dies gilt teilweise selbst für unsichere und längst gebrochene Verfahren, betrifft jedoch auch moderne Software für die Verschlüsselung von E-Mails, zum Beispiel das weit verbreitete Programm PGP. Daß dieses Exportverbot allerdings reichlich absurd ist, zeigt die Tatsache, daß auch die US-Version der Software PGP über das Internet frei erhältlich ist und von überall auf der Welt geladen werden kann.

Außerdem ist zwar der Export der Software an sich verboten, nicht jedoch der Export gedruckter Quelltexte. Daher gibt es inzwischen auch europäische PGP-Version, deren Quelltexte legal in Buchform importiert und in Europa eingescannt und compiliert wurden.

Als einziges demokratisches Land, das Kryptographie für Privatpersonen quasi total verbietet, steht Frankreich da. „Ein Gesetz vom 29. Dezember 1990 erlaubt dort elektronische Verschlüsselung nur auf Genehmigung, Privatpersonen wird sie jedoch nicht erteilt.“[1]

Die OECD-Krypto-Richtlinien[2]

Auf internationaler Ebene wurden am 27. März 1997 von der Weltwirtschaftsorganisation OECD erstmals Richtlinien veröffentlicht. Bei den Verhandlungen konnten sich allzu restriktive Positionen, wie die Frankreichs, Großbritanniens und auch der USA, nicht durchsetzen, allerdings kann nach den OECD-Richtlinien „nationale Kryptographie-Politik [...] den gesetzlichen Zugang zum Klartext verschlüsselter Daten oder zu kryptographischen Schlüsseln erlauben.“[3] Trotz dieser Einschränkung werden die Richtlinien vielfach als ein „lang erwartetes internationales Signal für eine liberale Kryptopolitik“[4] gewertet.

Die Diskussion in Deutschland

Auch in Deutschland wird derzeit über die Regulierung von Kryptographie diskutiert. Die Vorschläge reichen hier von leichten Regelungen mit Schlüsselhinterlegung bis zu einem „Quasi-Total-Verbot“[5] von Kryptographie.

Argumente für eine Krypto-Regulierung

Das einzige Argument für eine Einschränkung der freien Anwendung von Kryptographie, das immer wieder vorgebracht wird, ist die Möglichkeit des Abhörens des Nachrichtenaustauschs krimineller Vereinigungen. Kryptographie ermögliche es Straftätern, so die Argumentation des Bundesinnenministeriums, sich einer Überwachung zu entziehen.[6]

[1] Schnüffler am Ende
[2] OECD-Krypto-Richtlinien
[3] OECD-Krypto-Richtlinien
[4] OECD-Krypto-Richtlinien
[5] Kanthers Kurs auf das Kryptoverbot
[6] Schnüffler am Ende

Argumente gegen Krypto-Regulierung

Wirtschaftliche Argumente
Wichtige Argumente gegen Einschränkungen der Anwendungen von Kryptographie kommen von Seiten der Wirtschaft. Der Bundesverband der Deutschen Industrie e.V. (BDI) bemerkt hierzu beispielsweise, ein „derartiges Vorgehen stände in keinem Einklang mit den Wirtschaftsinteressen, da man Datenübertragungen vor Dritten sicher schützen müsse.“[1] Insbesondere steht diese Meinung auch gegen die Forderung des Bundesinnenministers Kanther, bei Verwendung von starken kryptographischen Verfahren sollten die Schlüssel „sicher hinterlegt“[2] werden, da dies eine große Gefahr darstellt, sobald die hinterlegten Schlüssel in falsche Hände geraten.

Durchführbarkeit nicht gewährleistet
Neben der Befürchtung, daß ein Kryptographieverbot oder entwendete Schlüssel der Wirtschaftsspionage dienen könnten, gilt es zu bedenken, daß eine Regulierung der Kryptographie auch vielfach nicht durchführbar scheint.

Würde man sich beispielsweise für eine Regelung entscheiden, die nur die Benutzung bestimmter schwacher kryptographischer Algorithmen erlaubt, könnte man die Anwendung verbotener, starker Kryptoverfahren dadurch verschleiern, daß man die Chiffrate starker Verfahren nachträglich mit einem erlaubten Algorithmus überschlüsselt.[3] Eine derartige Vorgehensweise wäre nur dann zu enttarnen, wenn wirklich alle Nachrichten von der überwachenden Stelle entschlüsselt würden; ein Unterfangen, daß sehr viel Zeit und Steuergelder verschlingen würde.

Aber auch falls es zu einem totalen Kryptographieverbot kommen würden, könnte man den Einsatz starker Kryptologie dennoch tarnen. Das Verfahren der Steganographie ermöglicht es, beliebige Mitteilungen in Bildern (z.B. durch subtile Farbveränderungen in einzelnen Bildpunkten), Klängen (z.B. durch nicht oder nur kaum hörbare Tonveränderungen) oder auch ganz simpel in gedruckten i-Punkten („Microdots“) zu verstecken, ohne daß überhaupt die Existenz einer solchen Nachricht auffallen würde. Bereits heute gibt es PC-Programme, die auf einfachste Weise Steganographie für Jedermann ermöglichen, bei einem Kryptoverbot würde steganographische Software sicher noch verbessert werden.

Verfassungswidrigkeit
Das vielleicht wichtigste Argument kommt aus den Reihen der Juristen und Datenschützer. Sie „kritisieren das geplante Regulierungsvorhaben als ‚verfassungsrechtlich nicht haltbar‘“[4], weil es gegen diverse Paragraphen des Grundgesetzes verstoße.

Die Standpunkte der Parteien

CDU/CSU
Die CDU und die CSU sind derzeit die einzigen Parteien, die eine Regulierung von Kryptographie in Deutschland befürworten. Die Pläne des Bundesinnenministers Kanther zielen auf eine Verpflichtung zur Hinterlegung der Schlüssel bei einer zentralen Stelle. Gleichzeitig sollen andere Verfahren, die diese staatlichen Abhörmöglichkeiten nicht bieten, verboten werden.

[1] Jeder Bürger ist verdächtig
[2] Kanther fordert Key Escrow
[3] Jeder Bürger ist verdächtig
[4] Jeder Bürger ist verdächtig

FDP
Der kleine Koalitionspartner in der Regierung ist dagegen anderer Ansicht. Sowohl Bundesjustizminister Schmidt-Jorzig als auch Bundeswirtschaftsminister Rexrodt treten für eine „vollständige Freigabe von Verschlüsselungsverfahren“ ein. „Der zuständige Berichterstatter der FDP, Karl-Hans Laermann, hatte ‚unmißverständlich‘ versichert, es werde mit der FDP keine Kryptographieverbote oder –beschränkungen geben.“[1]

SPD
Auch die SPD ist gegen eine einschränkende Regeln in der Kryptographiefrage. In einem Interview auf die Haltung seiner Partei hierzu angesprochen, sagte der Bundestagsabgeordnete Jörg Tauss: „Restriktive Regelungen zum Einsatz kryptografischer Verfahren wären verfassungsrechtlich fragwürdig und wirtschaftspolitisch schädlich. So ist die einstimmige Beschlußlage.“[2]

Bündnis 90/Die Grünen
Die Haltung von Bündnis 90/Die Grünen ist ähnlich. Laut Manuel Kiper, Bundestagsabgeordneter von Bündnis 90/Die Grünen, hat seine Partei bereits im Sommer 1995 „einstimmig jede Kryptoregelung abgelehnt“[3].

[1] Kanther fordert Key Escrow
[2] E-Mail-Interview mit Jörg Tauss
[3] E-Mail-Interview mit Manual Kiper

Fazit

Nach Betrachtung der Argumente für und gegen eine Regelung der Kryptographie kann man meiner Meinung nach nur zu dem Schluß kommen, daß eine Schlüsselhinterlegung oder ein totales Verbot von Kryptographie wesentlich mehr schadet, als es nutzt. Insbesondere könnten hinterlegte Schlüssel zur Industriespionage genutzt werden, was für den gerade in der heutigen Zeit so viel beschworenen Wirtschaftsstandort Deutschland sicher kein Bonus ist.

Aber auch wenn man sich für eine Regelung nach französischem Vorbild entschließt und Kryptographie genehmigungspflichtig wird, ist dies keine gute Wahl. Der Leidtragende ist in diesem Fall beispielsweise der E-Mail-Nutzer, der seine vertraulichen Daten vor neugierigen Augen schützen möchte.

Egal, welche regulierenden Maßnahmen ergriffen werden, Straftäter und kriminelle Vereinigungen könnten in jedem Fall durch das Ausspionieren von Unternehmen oder vertraulicher Daten von Privatleuten Nutzen daraus ziehen, während sie sich selbst durch die Nutzung steganographischer Verfahren unbemerkt einer Überwachung entziehen können.

Meiner Auffassung nach ist jegliche Einschränkung der Freiheit, kryptographische Verfahren zu nutzen, eine verfassungswidrige Einschränkung der persönlichen Freiheit und als solche aufs schärfste zu verurteilen. Ein Kryptoverbot bedeutet eine Kriminalisierung der Bürger und einen unverhältnismäßig hohen Aufwand, wenn es überwacht werden soll, während es einen Schutz vor Kriminellen nur vorgaukelt.

Literaturverzeichnis

In den Fußnoten werden die schräg gedruckten Kurzbezeichnungen verwendet.

Bücher

Kryptologie Prof. Dr. Beutelspacher, Albrecht, Kryptologie, Braunschweig/Wiesbaden 1994, Vieweg

Abenteuer Kryptologie Wobst, Reinhard, Abenteuer Kryptologie, Bonn 1997, Addison-Wesley-Longman

Informatik-Ausstellung Weinhardt, Karl (Hrsg.), Informatik - Führer durch die Ausstellung – Deutsches Museum, München 1990

Zeitschriften

Spektrum der Wissenschaft Dewdney, A. K., Auf den Spuren der Enigma Teil 1, Spektrum der Wissenschaft, Spektrum der Wissenschaft Verlagsgesellschaft mbH, S. 118 ff.

PM Marquardt, Ulf, Knackt den Code der Deutschen, P. M. – Peter Moosleitners interessantes Magazin, Ausgabe 10/1997, S. 86 ff.

Internet-Quellen

Cryptography for Beginners http://www.ftech.net/~monark/crypto/crypt/crypt.htm, 26.11.97

Schnüffler am Ende http://www.thur.de/ulf/krypto/zeitpgp.html, 1.12.97

OECD-Krypto-Richtlinien http://www.heise.de/bin/tp-issue/tp.html?artikelnr=1168&mode=html, 25.11.97

Kanthers Kurs auf das Kryptoverbot http://www.thur.de/ulf/politik/abhoer.html, 24.11.97

Jeder Bürger ist verdächtig http://www.heise.de/bin/tp-issue/tp.html?artikelnr=1147&mode=html, 25.11.97

Kanther fordert Key Escrow http://www.heise.de/bin/tp-issue/tp.html?artikelnr=1185&mode=html, 26.11.97

E-Mail-Interview Kiper http://www.heise.de/bin/tp-issue/tp.html?artikelnr=1171&mode=html, 25.11.97

E-Mail-Interview Tauss http://www.heise.de/bin/tp-issue/tp.html?artikelnr=1151&mode=html, 25.11.97

Weiterführende Internet-Seiten

„Die Kryptodebatte“ (Informationen zur aktuellen politischen Diskussion, viele Links)
http://members.aol.com/InfoWelt/k.htm, 26.11.97

„Encryption“ (Weitere Grundlageninformationen)

http://www.eco.utexas.edu/Homepages/Faculty/Norman/long/Student.Projects/SSim/index.html, 25.11.97

„Security-Server“ der Uni Siegen (Sehr umfangreich, viele Links)
http://www.uni-siegen.de/security/

Bildquellenverzeichnis

Seite 4	Abb. 1	Eine Skytale	Eigene Zeichnung
Seite 8	Abb. 2	Feistel-Netzwerk	Eigene Zeichnung
Seite 11	Abb. 3	Chiffrierscheibe	Eigene Aufnahme im Deutschen Museum München, Dezember 1997
	Abb. 4	Chiffrierschieber	Eigene Aufnahme im Deutschen Museum München, Dezember 1997
Seite 12	Abb. 5	Enigma (Schema)	aus *Spektrum der Wissenschaft*, S. 118, nachbearbeitet
Seite 14	Abb. 6	Enigma	aus *Informatik-Ausstellung,* Bild 23
	Abb. 7	Enigma	Eigene Aufnahme im Deutschen Museum München, Dezember 1997
Seite 15	Abb. 8	Hagelin-Cryptos	Eigene Aufnahme im Deutschen Museum München, Dezember 1997