Hauptseminar

Informatik und Gesellschaft

Prof. Dr. Klaus Lagally
Stefan Schimpf

Verschlüsselung — Grundrecht oder Delikt?

bearbeitet von Ralf Kohler

Universität Stuttgart 1997

DIE NIK-EBERT-KARIKATUR

Schöne neue Telekommunikation

Ausarbeitung zum Vortrag im Rahmen des Hauptseminars *Informatik und Gesellschaft* im Sommersemester 1997 an der Universität Stuttgart, Fakultät Informatik, Abteilung Betriebssoftware. Der Vortrag gibt einen Überblick über die aktuelle Diskussion um den freien Einsatz starker kryptographischer Verfahren.

Inhaltsverzeichnis

0.1 Motivation

Spione, Agenten, geheime Militärdokumente — ein Hauch von Abenteuer schwingt mit, wenn der Begriff *Kryptologie* fällt. Dabei handelt es sich doch um eine der Schlüsseltechnologien (im wörtlichen wie im übertragenen Sinne) der Informationsgesellschaft. Digitale Märkte, um nur ein Schlagwort aufzugreifen, sind ohne diese Verfahren nahezu undenkbar. Neben der naheliegenden Frage, wozu Verschlüsselung denn gebraucht wird, drängt sich in diesem Zusammenhang auch die Frage auf, warum der Kryptologie so lange so wenig Beachtung geschenkt wurde. Die Bedeutung der Kryptologie steht auch in einem krassen Gegensatz zu ihrer Akzeptanz. Oft wird sie im Zusammenhang mit der Verbreitung pornographischer oder extremistischer Inhalte über das Internet genannt — die eigentliche Problematik wird dadurch eher verschleiert als erhellt. Inzwischen tobt international eine heftige Auseinandersetzung um den Einsatz starker kryptographischer Verfahren, wobei sich oft Wirtschaft, Datenschützer und Bürgerrechtler auf der einen Seite und Geheimdienste und Strafverfolgungsbehörden auf der anderen Seite entgegenstehen.

Kapitel 1

Was ist Kryptologie?

1.1 Einige Worte zur Geschichte

Daß das Versenden verschlüsselter Botschaften keine neue Entwicklung, ja nicht einmal eine Erfindung unseres Jahrhunderts oder Jahrtausends ist, sollen einige kurze Beispiele zeigen. Schon im antiken Sparta[1] wurden sensible Informationen mit Hilfe einer *Skytale* verschlüsselt: Das Verfahren bestand darin, daß auf einen schmalen Papierstreifen geschrieben wurde, der um einen Stab (die Skytale) gewickelt war - zum entschlüsseln mußte der Empfänger eine Skytale mit demselben Radius besitzen. Caesar[2] hat für wichtige Nachrichten eine einfache Verschiebechiffre, die nach ihm benannte *Caesar-Chiffre* benutzt. Im Zweiten Weltkrieg hatte dann die Kryptologie einen wichtigen Anteil am Kriegsgeschehen — die Alliierten setzten damals alles daran, die *Enigma-Chiffre* zu knacken.

1.2 Wichtige Begriffe

Um eine Nachricht vor fremden Augen (oder Ohren) zu verbergen, kann man zwei Methoden anwenden:

- Steganographie
- Kryptographie

Die Steganographie[3] ist die Wissenschaft vom Verbergen von Nachrichten. Kryptographie[4] dagegen versucht nicht zu verbergen, daß eine geheime Nachricht vorliegt. Es wird nur versucht zu verhindern, daß ein Unbefugter die Nachricht lesen kann. *Kryptoanalyse* beschäftigt sich mit Verfahren zum Entschlüsseln verschlüsselter Nachrichten. Kryptographie und Kryptoanalyse werden unter dem Oberbegriff *Kryptologie* zusammengefasst. Neben der Geheimhaltung soll Kryptographie oft noch andere Ansprüche erfüllen:

Authentifizierung

Es sollte dem Empfänger möglich sein, die Herkunft einer Nachricht zu ermitteln; ein Eindringling sollte sich nicht als andere Person ausgeben können.

[1] um 700 vor Christus
[2] um 50 vor Christus
[3] griechisch: stegos = geheim, unsichtbar
[4] griechisch: cryptos = bedeckt, verdeckt

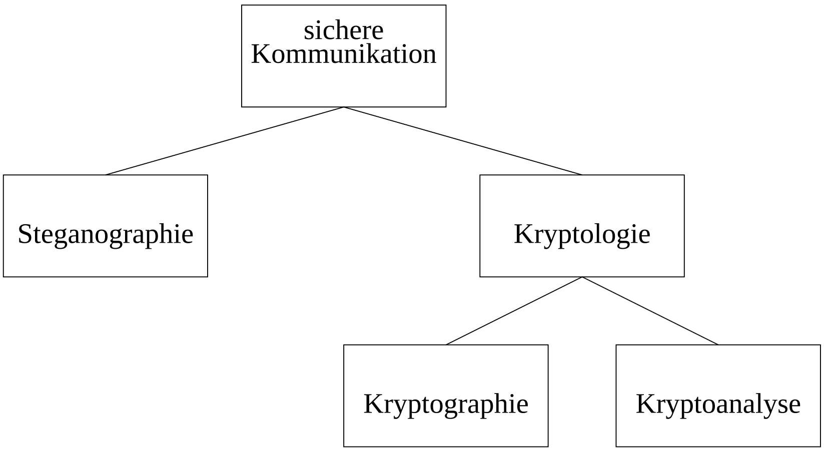

Abbildung 1.1: Forschungsgebiete

Integrität

Der Empfänger sollte überprüfen können, ob eine Nachricht bei der Übermittlung verändert wurde; ein Eindringling sollte die echte nicht durch eine gefälschte Nachricht ersetzen können.

Verbindlichkeit

Ein Sender sollte später nicht leugnen können, daß er eine Nachricht gesendet hat.

1.3 Verfahren

1.3.1 Kryptographie

Wie funktioniert einfache Kryptographie?

Jedes praktisch angewandte Chiffrierverfahren besteht aus vier grundlegenden Teilen:

- der zu verschlüsselnden Information (der lesbaren Nachricht, auch Klartext oder *plaintext*)
- der verschlüsselten (chiffrierten) Information (Geheimtext oder *ciphertext*)
- dem Verschlüsselungsalgorithmus
- dem Schlüssel (oder den Schlüsseln), repräsentiert durch eine Zahl oder eine Menge von Zeichen, die dem Verschlüsselungsalgorithmus als Parameter übergeben werden.

Die Funktionsweise der einzelnen Verfahren würden den Rahmen dieses Vortrags sprengen. Deshalb sei an dieser Stelle auf das Literaturverzeichnis ([2] [3] [8]) verwiesen. Für alle Verfahren gilt jedoch Kerkhoffs' Maxime:

> Die Sicherheit eines Verschlüsselungsverfahrens darf nicht von seiner Geheimhaltung abhängen! (von Kerkhoffs, 1883)

Es ist naiv, davon auszugehen, daß schon niemand den Code disassemblieren und den Code rekonstruieren wird. Die besten Verfahren sind diejenigen, die veröffentlicht, jahrelang attackiert und nicht geknackt worden sind [2].

Im Folgenden wird noch auf die Unterscheidung zweier Klassen von Verfahren eingegangen, die auch für die Kryptodebatte von Bedeutung ist.

Kryptographie mit privaten Schlüsseln (Private Key-Systeme)

Diese Verfahren werden auch als *symmetrische Verfahren* oder Verfahren mit *geheimem Schlüssel (secret key)* bezeichnet. Bei diesen Verfahren wird sowohl zum Verschlüsseln als auch zum Entschlüsseln derselbe Schlüssel verwendet. Das Problem dabei ist, daß dem Kommunikationspartner, mit dem verschlüsselte Nachrichten ausgetauscht werden sollen, auch der Schlüssel mitgeteilt werden muß. Hierfür muß ein sicherer Nachrichtenkanal benutzt werden, was einen ziemlichen Aufwand darstellt (wäre die Verwendung des sicheren Kanals kein Aufwand, dann wäre eine Verschlüsselung ja gar nicht nötig).

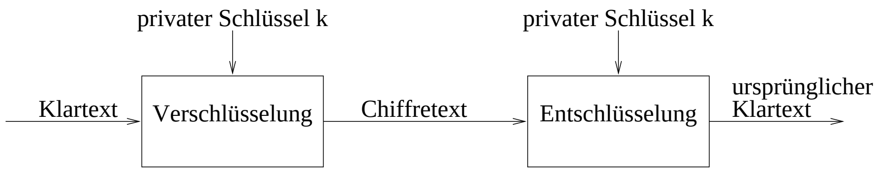

Abbildung 1.2: Ver- und Entschlüsselung mit einem privaten Schlüssel

Kryptographie mit öffentlichen Schlüsseln (Public Key-Systeme)

Auch als *asymmetrische Verfahren* bezeichnet. Bei diesen Algorithmen unterscheiden sich Chiffrier- und Dechiffrierschlüssel. Der Dechiffrierschlüssel kann auch nicht (in angemessener Zeit) aus dem Chiffrierschlüssel berechnet werden. Die Bezeichnung Algorithmen mit öffentlichem Schlüssel (Public Key-Verfahren) kommt von der Tatsache, daß der Chiffrierschlüssel öffentlich bekannt gemacht werden kann: Ein völlig Unbekannter kann mit Hilfe des öffentlichen Schlüssels (Public Key) die Nachricht verschlüsseln, aber nur der Besitzer des zugehörigen privaten Schlüssels (Private Key, Secret Key) kann die Nachricht wieder entschlüsseln. Diese Verfahren ermöglichen bei umgekehrter Anwendung auch eine Authentifizierung: Nachrichten werden mit dem privaten Schlüssel verschlüsselt und können nur mit dem zugehörigen öffentlichen Schlüssel dechiffriert werden. Dieses Verfahren wird bei *digitalen Signaturen* eingesetzt.

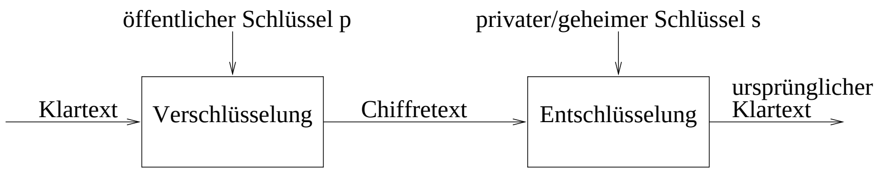

Abbildung 1.3: Ver- und Entschlüsselung bei Public Key-Verfahren

1.3.2 Kryptoanalyse

Sinn und Zweck der Kryptographie ist es, Klartext vor Schnüfflern (auch: Gegner, Angreifer, Abhörer, Lauscher, Eindringling, Feind) zu verbergen. Man setzt dabei voraus, daß die Gegner vollständigen Zugriff auf die Kommunikation zwischen Sender und Empfänger besitzen. Es ist auch sinnvoll, vorauszusetzen, daß der Gegner das Verfahren kennt[5], höchste Intelligenz, Rechenleistung und Kapitalkraft besitzt, um eine nicht für ihn bestimmte Nachricht zu entschlüsseln. Auf der eigenen Seite sollte man dagegen maximale Dummheit, Leichtsinn und Bestechlichkeit bei der Benutzung eines Verschlüsselungsprinzips voraussetzen. Kryptoanalyse ist die Wissenschaft von der Wiederherstellung des Klartexts einer Nachricht ohne Zugriff auf den Schlüssel. Die Kryptoanalyse ist erfolgreich, wenn der Klartext oder der Schlüssel ermittelt wird.

Brute Force Attack

Diese Methode wird auch *Key Search Attack* genannt. Es wird einfach nacheinander jeder mögliche Schlüssel durchprobiert. Dadurch, daß die Rechnerleistung in den letzten Jahren so zugenommen hat und sehr billig geworden ist, sind Verfahren, die in den siebziger Jahren noch als sicher galten, durch diese Angriffsmöglichkeit praktisch wertlos geworden. Allerdings stößt man auch schnell an Grenzen: Um bei einem 128bit-Schlüssel (der bei dem von PGP verwendeten IDEA-Alorithmus verwendet wird [9]) würde es auch bei der Annahme, daß eine Milliarde 1000-MIPS Rechner verwendet werden, 10^{13} Jahre dauern, bis alle Schlüssel durchprobiert sind (bei einer geschätzten Lebensdauer der Universums von 1.2×10^{10} Jahren).

Echte Kryptoanalyse

Meist gibt es aber wesentlich effizientere Methoden, um ein Verfahren anzugreifen. Der RSA[6] Public Key-Algorithmus kann (wenn auch mit sehr hohem Aufwand) durch Faktorisierung des öffentlichen Schlüssels angegriffen werden. Fast alle Algorithmen können mit großer Rechenleistung und ausgeklügelten mathematischen Verfahren angegriffen werden (oft helfen statistische Analysen). Unter einem *starken kryptographischen Verfahren* versteht man einen Algorithmus, der mit derzeitigen (und für die Zukunft zu erwartenden) Ressourcen und Kenntnissen nicht zu knacken ist. Im Gegensatz dazu spricht man von *schwacher Kryptographie*, wenn das Verfahren mit Hilfe kryptoanalytischer Verfahren oder eines Brute-Force-Angriffs relativ einfach zu knacken ist.

Kompromittierung

Von Kompromittierung spricht man, wenn der Schlüssel durch nicht kryptoanalytische Methoden erlangt wird. Bei starken kryptographischen Verfahren ist das der wirkungsvollste Angriff: Der Schlüssel kann gestohlen, gekauft, erpreßt... werden.

1.3.3 Steganographie

Zu den historischen Tricks gehören unsichtbare Tinte, winzige Einstiche in ausgewählten Buchstaben, kleinste Unterschiede in handgeschriebenen Zeichen, Raster.... In der Masse der in den Datennetzen verschickten Multimedia-Dateien ist es einfach, Texte in den niederwertigen Bytes einer Grafikdatei oder im Rauschen einer Sounddatei zu verstecken. Auch Texte können mit steganographischen Verfahren bearbeitet werden. Inzwischen ist eine Vielzahl steganographischer Verfahren

[5] siehe v. Kerkhoffs' Prinzip
[6] von Rivest, Shamir und Adleman entwickeltes asymmetrisches Verfahren

Abbildung 1.4: Original

Abbildung 1.5: hier wurde mit S-Tools ein Text versteckt

```
Generalbundesanwalt Kai Nehm:

"Der Gesetzgeber wird die Hersteller von
Verschlüsselungsprogrammen verpflichten müssen,
gegebenenfalls den Schlüssel bereitzuhalten, um
Daten lesbar zu machen. Das ist wie bei der
herkömmlichen Strafverfolgung: Wenn wir um
sechs Uhr morgens vor einer verschlossenen
Haustür stehen, rufen wir den Schlüsseldienst."
Jeder Schlüssel sei zu knacken: "das ist
lediglich eine Frage des Aufwands"
(DER SPIEGEL 46/96, S. 98)
```

Abbildung 1.6: der versteckte Text

vorhanden. Meist werden hierbei die Daten zunächst mit starken kryptographischen Verfahren verschlüsselt und dann versteckt oder verfremdet.

Kapitel 2

Grundrecht oder Delikt?

Im Folgenden soll erörtert werden, wo die Kryptographie im Spannungsfeld zwischen den Interessen steht. Dazu soll zuerst kurz auf die bisherige Entwicklung in den USA und in Deutschland eingegangen werden und vor diesem Hintergrund dann die Problematik erörtert werden.

2.1 Die Situation in den USA

Die Benutzung starker kryptographischer Verfahren ist nicht reglementiert. Allerdings unterliegt kryptographische Hard- und Software strengen Exportbeschränkungen. Sie werden nach ITAR (International Traffic in Arms Regulations) wie Munition behandelt. Für den Export werden in der Regel nur schwache Verfahren oder solche, bei denen die Schlüssellänge auf 40 bit beschränkt ist, zugelassen[1]. So verschlüsselte Nachrichten können ohne weiteres innerhalb einer Sekunde (dadurch *online*) geknackt werden [1]. Treibende Kraft bei den Exportbeschränkungen ist die NSA[2].

2.1.1 Der Clipper-Chip

Die US-Regierung versucht, den von der NSA entwickelten Clipper-Chip als Standard zu etablieren. Der verwendete Verschlüsselungsalgorithmus wird von der NSA geheimgehalten. Die Einführung des Clipper-Chips ist verbunden mit dem EES (Escrowed Encryption Standard): Jeder Clipper-Chip hat eine Seriennummer, die mit der verschlüsselten Nachricht übertragen wird. Die Strafverfolgungsbehörden und die Geheimdienste können über diese Seriennummer in einer Datenbank auf die Schlüssel zugreifen. Allgemein versteht man unter einem *Key Escrow System* die Speicherung eines Schlüssels für den späteren Zugriff (autorisierter) Stellen. Dieses Konzept ist auch unter der Bezeichnung *Government Access to Keys* (GAK) zu finden.

2.2 Die Situation in Deutschland

Der Export von Verschlüsselungssystemen ist genehmigungspflichtig; allgemein zugängliche sowie über das Internet vertriebene Software ist allerdings von der Genehmigungspflicht ausgenommen [5]. Die Fernmeldeverkehr-Überwachungs-Verordnung verpflichtet alle Betreiber von Fernmeldeanlagen, verschlüsselte Daten abhörenden Behörden im Klartext zur Verfügung zu stellen. „Verschlüsselungsverfahren sind

[1] so z.B. die Verfahren RC2/RC4 im Netscape SSL mit einer Schlüssellänge von 40 bit

[2] National Security Agency, auch:„No such Agency“ oder „Never Say Anything“

jedoch keine Fernmeldeanlagen im Sinne des FAG[3], denn mit ihrer Hilfe werden keine Nachrichten übertragen, sondern sie werden lediglich als Mittel zur Verfremdung von Daten vor ihrer Übermittlung verwendet.“ [14]. Sie dienen lediglich zur Herstellung des Übermittlungsobjektes, sind aber selbst keine Fernmeldetechnik. Betreiber sind nicht verpflichtet, Schlüsselduplikate aufzubewahren, „solange den Teilnehmern das Verschlüsseln unabhängig vom Übertragungsdienst von Endgerät zu Endgerät ermöglicht wird“.

Nach Informationen des SPIEGEL [11] berät seit Monaten der *Staatssekretärsausschuß für das geheime Nachrichtenwesen und die Sicherheit* über Vorlagen zu einem möglichen Kryptogesetz. Inoffziellen Informationen zufolge sind dabei zur Zeit drei Varianten in der Diskussion:

Variante 1 (Krypto-Regulierung-light)

Dieser Vorschlag beinhaltet ein Key Escrow-System, in dem Anbieter von Verschlüsselungsdienstleistungen die Daten den Behörden in unverschlüsselter Form zur Verfügung stellen müssen. Auch Zertifizierungsstellen (sogenannte *Trust Center*) müssen die zertifizierten Schlüssel aufbewahren und im Bedarfsfall herausgeben. Hersteller, Vertreiber und Nutzer von Verschlüsselungssystemen wären von dieser Regelung nicht betroffen. Diese Lösung wird anscheinend nur vom Bundeswirtschaftsministerium befürwortet.

Variante 2 (Krypto-Regulierung-streng)

Zusätzlich zur Variante 1 wird eine Genehmigungspflicht für Herstellung und Vertrieb von Kryptosystemen eingeführt: Eine Zulassung erhalten nur schwache Verfahren und Key-Escrow-Systeme. Die Nutzung nicht genehmigter Verfahren durch den Endnutzer wird nicht explizit verboten.

Variante 3 (Quasi-Total-Verbot)

Hier kommt zu Variante 2 noch ein grundsätzliches Nutzungsverbot ungenehmigter Verfahren hinzu. Dieser Vorschlag wird anscheinend vom Bundeskanzleramt, vom Bundesnachrichtendienst (BND), vom Verfassungsschutz und vom Bundesamt für Sicherheit in der Informationstechnik (BSI) favorisiert.

> „Man könnte sich kaputtlachen, wenn man nicht wüßte, daß es tatsächlich so gemeint ist.“ (Dr. Burkhard Hirsch, Vizepräsident des Deutschen Bundestages [6])

2.3 Diskussion

2.3.1 Motivation und Argumentation der Befürworter einer Kryptoregulierung

Begründet wird der Wunsch nach einer Kryptoregulierung in der Regel mit den Interessen der Verbrechensprävention und der Strafverfolgung. Von den Befürwortern wird die Regelung als Anpassung der Rechtslage an die technische Entwicklung gesehen. Mit einer solchen Regelung soll verhindert werden, daß den Sicherheitsbehörden die Möglichkeit zum Abhören und Überwachen im Bereich der Telefon-, Fax- und Datenkommunikation verlorengeht. Laut Bundesinnenminister Kanther gehe es nicht an, daß Verbrecher und Extremisten abhörsicher in neuen Netzen telefonieren oder sich durch moderne Verschlüsselungsverfahren von den Strafverfolgern

[3] Fernmeldeanlagengesetz

abschirmen könnten[19]. Laut Erwin Marschewski, dem innenpolitischen Sprecher von CDU/CSU besteht Handlungsbedarf, um „Lücken bei der Überwachung moderner Kommunikationssysteme zu schließen". Besonders Terroristen, Anbieter harter Pornographie, Drogenhändler und das organisierte Verbrechen allgemein würden ihre Aktivitäten zunehmend durch Verschlüsselung schützen. Der Präsident des Bundesamtes für Verfassungsschutz, Peter Frisch, befürchtet, ohne ein Krypto-Gesetz müsse der Staat „hilflos zusehen, wenn Extremisten auf diesem Weg zu Gewalt aufrufen".

Andererseits konnte wohl bisher kein konkreter Fall angeführt werde, wo die Anwendung starker Kryptographie die Aufklärung einer Straftat behindert hätte [18]. Auch ist der Nutzen von Abhörmaßnahmen für die Strafverfolgung durchaus umstritten. Laut Diffie [1] sind sie von recht geringer Bedeutung. Ein Vergleich zwischen USA und Deutschland ist in diesem Zusammenhang auch interessant: 1995 wurden in den USA (240 Millionen Einwohner) 1229 Telefonüberwachungen angeordnet, im gleichen Zeitraum waren es in der Bundesrepublik (80 Millionen Einwohner) 3667 Anordungen; 1996 stieg die Zahl dann sogar auf 6428 an [18] (für 1996 liegen für die USA noch keine Zahlen vor). In den USA spielen laut Diffie selbst diese wenigen Telefonüberwachungen in den Gerichtsverfahren kaum eine Rolle. In welcher Weise dies für die Bundesrepublik zutrifft, ist schwer zu ermitteln, da - im Gegensatz zu den USA - eine Kontrolle der durchgeführten Maßnahmen nicht stattfindet.

2.3.2 *Informationelle Selbstbestimmung* als Menschenrecht

> „It's personal. It's private. And it's no one's business but yours." (Philip Zimmermann [4])

Eine E-Mail ist öffentlicher als eine Postkarte. Praktisch auf jedem Knotenrechner besteht die Möglichkeit des Mitlesens - im Gegensatz zur Postkarte ist auch eine automatische Überwachung sehr einfach. Ein Telefongespräch, das man über ein schnurloses Telefon ohne eingebaute Verschlüsselung führt, kann vom Nachbarn mit einem überall zu kaufenden Funkempfänger so einfach mitgehört werden wie eine Radiosendung. Kryptographie ist die einzige Möglichkeit, sicherzustellen, daß die Nachricht nur vom Empfänger gelesen wird. Wer Daten wie Kontonummern, Kreditkartennummern, Adressen über Datennetze schickt, über sein Gehalt diskutiert, über Chef oder Kollegen lästert... ist sehr daran interessiert, daß die Daten nur vom beabsichtigten Adressaten gelesen werden. „Der Einsatz teilnehmerautonomer Verschlüsselungsverfahren zur Sicherung elektronischer Kommunikation ist nach geltendem Recht nicht nur zulässig, er steht sogar unter dem Schutz des Fernmeldegeheimnisses. [...] Der Bürger hat keinen Anspruch auf eine staatliche Leistung, wohl aber einen grundrechtlichen Anspruch darauf, daß es der Staat prinzipiell unterläßt, seine individuellen Schutzbemühungen zu beeinträchtigen" führt der Jurist Johann Bizer aus [16]. Die Nutzung starker kryptographischer Verfahren stellt somit eine Inanspruchnahme des im Grundgesetz zugesicherten Brief-, Post- und Fernmeldegeheimnisses dar:

> Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich. (Art.10 Abs.1 GG)

Ein Verbot nicht zugelassener Kryptoverfahren würde bisherige Rechtsprinzipien auf den Kopf stellen. Der schleswig-holsteinische Datenschutzbeauftragte weist in seinem Tätigkeitsbericht darauf hin, daß es in der deutschen Rechtsordnung bisher keine vergleichbare Vorschrift gibt, die „den Bürger verpflichtet, der Polizei vorsorglich seine Geheimnisse anzuvertrauen". Die bisherige Einschränkung des Briefgeheimnisses erlaubte allein die Kontrolle von Sendungen. Weder sind dadurch bestimmte Schreibformen vorgeschrieben, noch bestimmte Sprachen oder Ausdrucksformen verboten. Keine Strafnorm verbietet es, mit Geheimtinte zu schreiben oder andere Verfahren zu nutzen, um Nachrichten zu verheimlichen. Wer Briefe öffnet, hat alle nötigen Entschlüsselungsarbeiten selbst zu leisten - kein Absender muß ihm dabei auch noch durch einen „Brief nach Vorschrift“ helfen. Burkhard Hirsch fragt zurecht: „Ist Früh-Aramäisch schon Verschlüsselung? — Wahrscheinlich nein, aber fast.“ Zugespitzt kann man formulieren: Darf der Staat uns vorschreiben, in welcher Sprache wir uns zu unterhalten haben?

2.3.3 Interessen der Wirtschaft

In den Niederlanden und in Südafrika sind Vorhaben für Krypto-Gesetze am massiven Protest der Industrie gescheitert. Auch in Deutschland haben sich schon viele Verbände und Unternehmen, so zum Beipiel auch die Deutsche Bank und der Daimler-Benz Konzern gegen die Pläne der Bundesregierung ausgesprochen. Im Folgenden soll daher auf einige Punkte eingegangen werden, die die wirtschaftlichen Aspekte der Verschlüsselung zeigen.

Wirtschaftsspionage

Vertraulichkeit ist ein Wirtschaftsfaktor [7]. Wenn vertrauliche Konstruktionspläne, Marketingstrategien, Kundendaten oder ähnliches der Konkurrenz in die Hände fallen, kann das für Unternehmen Millionenverluste bedeuten. Schon durch die US-Exportbeschränkungen sind nichtamerikanische Unternehmen hier im Nachteil, da für sie in der Regel keine Standardsoftware mit starken kryptographischen Verfahren zur Verfügung steht. Eine deutsche Krypto-Regulierung würde diese Situation noch verschärfen. Der Fachverband Informationstechnik im VDMA[4] und ZVEI[5] warnt: „Die Verwendung sicherer Verschlüsselungsverfahren ist im Hinblick auf die Bedeutung der Ressource Information und die gleichzeitige Bedrohung durch Wirtschafsspionage für die deutsche Wirtschaft unerläßlich. Eine Regulierung schafft nur unnötigen Verwaltungs- und Kostenaufwand in beträchtlicher Höhe und mindert die Exportchancen deutscher Sicherheitsprodukte. Sie trifft nur gesetzestreue Unternehmen und Bürger, deren Verfahren darüber hinaus unsicherer werden (jede legale Zugriffsmöglichkeit kann auch mißbraucht werden, zum Beispiel durch ausländische Dienste)“ [20]. Hinterlegunsstellen für Schlüssel sind naheliegende Angriffsziele für Hacker und Geheimdienste. Die Konzentration von Schlüsseln an einem Ort birgt hier ein großes Risiko.

Electronic Commerce

Viele Unternehmen setzen große Erwartungen in das Internet: Die Akzeptanz des *Internet-Banking*, der *Virtuellen Märkte* usw. hängt stark vom Vertrauen der Kunden in die Sicherheit der verwendeten Verfahren ab. Eine zentrale Speicherung von Schlüsseln oder eingebaute „Hintertüren“ wären hier sicher schädlich. Wenn immer mehr technisch inkompatible nationale Regelungen entstehen, bleibt der globale Electronic Commerce nur Wunschdenken.

Export

Durch eine Reglementierung würden die Exportchancen der deutschen Industrie gemindert. Bei der heutigen Bedeutung von Sicherheitstechnologien wäre das ein beachtlicher Standortnachteil. Betroffen sind Softwareprodukte, Hardware, Smart-Cards, Kabel- und Satellitendekoder (...).

[4] Verband Deutscher Maschinen- und Anlagenbau e.V.
[5] Zentralverband Elektrotechnik- und Elektronikindustrie e.V.

Besondere Berufsgruppen

Eine zusätzliche Problematik ergibt sich bei Berufsgruppen, die mit vertraulichen Daten umgehen. Für Ärzte, Rechtsanwälte, Notare, Steuerberater und Journalisten... sieht DFN-CERT[6] in der Verschlüsselung die Voraussetzung für die Nutzung der Datennetze [21]. In den USA gibt es schon das Problem, daß sich Versicherungsunternehmen Zugang zu Gesundheitsdaten verschafft haben. Das FIfF[7] befürchtet, daß zum Beispiel das Bankgeheimnis und die ärztliche Schweigepflicht auf das Fernmeldegeheimnis reduziert werden. Ein Kryptogesetz höhle also nicht nur das Fernmeldegeheimnis aus, sondern zugleich eine Vielzahl anderer Schutzrechte. „Ein solches Gesetz wäre ein trojanisches Pferd für den Rechtsstaat in der Informationsgesellschaft“ [18].

2.3.4 Probleme eines *Krypto-Gesetzes*

Im Folgenden soll noch kurz auf einige konkreten Probleme eingegangen werden, die sich bei der Einführung einer Krypto-Regulierung ergeben würden.

Verfassungswidrig?

Die Juristen Bizer, Rieß und Roßnagel halten eine Beschränkung kryptographischer Verfahren für verfassungswidrig [15]. Die Hauptargumente sind hierbei die Verletzung von Grundrechten. Angeführt werden die wirtschaftliche Entfaltungsfreiheit (Art. 12,1 und Art. 2,1 GG), die Vertraulichkeit der Kommunikation (Art. 10 GG) und das informationelle Selbstbestimmungsrecht (Art. 2,1 und Art. 1,1 GG).

Wie hoch soll die Strafe sein?

Eine berechtigte Frage ist auch, wie hoch die Strafe für die Benutzung unterlaubter Verschlüsselung sein soll, damit potentielle Straftäter und Terroristen abgeschreckt werden.

> „Die Strafandrohung in einem ‘Krypto-Gesetz’ möchte ich sehen, die so hoch ist, daß ein Straftäter lieber im Klartext über seine Pläne korrespondiert, als das Risiko einzugehen, eine nicht registrierte Verschlüsselung zu benutzen“ (Burkhard Hirsch [6])

In die gleiche Richtung zielt der Vergleich einer Krypto-Regulierung mit dem Versuch, Bankräuber durch eine Geschwindigkeitsbegrenzung zu behindern. Von den Befürwortern einer Regulierung kommt gegen diese Argumentation der Einwand, daß sich auch schon aus dem Nutzerkreis illegaler Verfahren interessante Rückschlüsse auf verdächtige Personenkreise ergeben würden.

Nicht kontrollierbar

Durch den Einsatz von Steganographie kann jede Krypto-Regulierung unterlaufen werden. Aber es geht sogar noch einfacher: Durch Mehrfachverschlüsselung (zuerst mit dem verbotenen, dann mit dem erlaubten Verfahren) oder durch Datenkompression kann die Nutzung der verbotenen Verfahren recht wirksam verschleiert werden. Es dürfte auch sehr schwierig sein, den Nachweis zu führen, daß ein verbotenes Verfahren benutzt worden ist — dafür wäre wohl nämlich im allgemeinen eine Dechiffrierung notwendig.

[6] Computer Emergency Response Team des Deutschen Forschungsnetzes
[7] Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

Schwächung der elektronische Unterschrift

Wie oben beschrieben kann das Public Key-Konzept gleichzeitig zur Verschlüsselung und zur digitalen Unterschrift verwendet werden. Wird der geheime Schlüssel hinterlegt, dann ist auch ein Mißbrauch der digitalen Unterschrift nicht ausgeschlossen.

Zeitliche Beschränkung

Die bisher vorhandenen Konzepte lassen eine zeitliche Begrenzung der Überwachungsmaßnahme nicht zu. Bei einer Offenlegung des Schlüssels gegenüber den Sicherheitsbehörden ist die Überwachung so lange möglich, bis der Schlüssel geändert wird.

Exponentielles Wachstum der Verdächtigen?

Die Offenlegung des privaten Schlüssels eines Verdächtigen macht zwar dessen eingehenden Datenverkehr lesbar, nicht aber den ausgehenden. Hierzu müssen auch die privaten Schlüssel aller Kommunikationspartner offengelegt werden, bei weitergehenden Ermittlungen dann auch noch die Schlüssel deren Partner.

Sicherheit der hinterlegten Schlüssel

Voraussetzung für eine sichere Schlüsselgenerierung und -hinterlegung ist eine sichere Systemumgebung, die es offensichtlich (noch) nicht gibt. Hierbei stellt sich natürlich auch die Frage der Haftung gegenüber dem Benutzer, falls verschlüsselte Daten widerrechtlich offengelegt werden.

Internationale Zusammenarbeit

Ein nationales Kryptogesetz wird den Problemen des internationalen Datenverkehrs kaum gerecht werden können. Selbst wenn andere Länder analoge Regelungen treffen würden, stellt sich doch die Frage, ob viele Staaten bereit sein werden, den Straftverfolgungsbehörden anderer Staaten Krypto-Schlüssel zur Verfügung zu stellen. Bei den bisherigen Problemen in der Zusammenarbeit bei der Verbrechensbekämpfung sind hier zumindest Zweifel angebracht.

2.4 Schlußfolgerungen

Die Argumente für die Nutzung starker kryptographischer Verfahren, für die freie Wahl der Verfahren und der Schlüssel überwiegen die dadurch entstehenden Probleme bei weitem. Alle vorgeschlagenen Reglementierungen würden dem Bürger und der Wirtschaft unverhältnismäßige Nachteile bringen, sich im Kampf gegen das organisierte Verbrechen aber als völlig nutzlos erweisen.

2.5 Hamburger Erklärung

Wer sich für die freie Wahl von Verschlüsselungsverfahren und für die freie Wahl und Geheimhaltung der Schlüssel aussprechen möchte, kann die *Hamburger Erklärung für Verschlüsselungssicherheit* unterstützen. Informationen gibt es unter `ftp://troll.hz.kfa-juelich.de/pub/KRYPTO/hh.htm` oder bei DFN-CERT an der Universität Hamburg. Die Erklärung kann PGP-signiert bis 30. Mai 1997 an `krypto@cert.dfn.de` (Subject: Fuer Verschluesselungsfreiheit) geschickt werden.

2.6 Pretty Good Privacy (PGP)

Zum De-Facto-Standard beim Verschlüsseln von Email hat sich das Programm PGP von Phil Zimmermann entwickelt. Das Programm verwendet eine Kombination aus dem asymmetrischen RSA[8] und dem symmetrischen IDEA-Verfahren[9]. Das Programm ist *Freeware* und für alle großen Plattformen verfügbar. Aufgrund der komplizierten Situation bezüglich Patentrecht und Exportbestimmungen gibt es verschiedene Versionen für die USA und für den Rest der Welt, die aber gleich sicher und untereinander kompatibel sind. Mehr Informationen über PGP finden sich in [9] und [4]. Die aktuelle internationale Version ist `PGP 2.6.3i` ist unter

`ftp://ftp.uni-stuttgart.de/pub/security/unix/pgp/`

zu finden. Für Macintosh und Windows 95/NT ist auch das Programm PGPfone verfügbar, das es erlaubt, verschlüsselte Telefonate zu führen.

Abbildungsverzeichnis

[8] mit einer Schlüssellänge von 512, 768 oder 1024bit
[9] mit einer Schlüssellänge von 128bit

Literaturverzeichnis

[1] DAWSON, ED: Cryptography: Policy and Algorithms, Springer, 1996

[2] SCHNEIER, BRUCE: Angewandte Kryptographie, Addison-Wesley, 1996

[3] SCHÖNLEBER, CLAUS: Verschlüsselungsverfahren für PC-Daten, Franzis, 1995

[4] ZIMMERMANN, PHILIP: The Official PGP User's Guide, MIT Press, 1994

[5] SCHWARZ, MARTIN: Die Rechtslage der Kryptographie in der BRD
http://www.informatik.fh-muenchen.de/ schwarz/inf/krypto/krypto.html

[6] HIRSCH, BURKHARD: Krypto-Gesetz macht keinen Sinn
http://www.liberale.de

[7] iX 04/97,p.128ff: Die Diskussion um Kryptographie, Heise-Verlag, 1997

[8] BEUTELSPACHER, ALBRECHT: Kryptologie, Vieweg, 1996

[9] GARFINKEL, SIMSON: PGP, Pretty Good Privacy, O'Reilly & Associates, Inc., 1995

[10] JOHNSON, MICHAEL: USA Crypto-Policy-FAQ
http://www.eff.org/pub/Privacy/us_crypto-policy.faq

[11] DER SPIEGEL 12/1997,p.80: Schlüssel für den Staat

[12] HUHN, MICHAELA / PFITZMANN, ANDREAS: Technische Randbedingungen jeder Kryptoregulierung, erschienen in Datenschutz und Datensicherheit 20/1, Vieweg, 1996

[13] RSA DATA SECURITY, INC.: Answers to Frequently Asked Questions About Cryptography Export Laws
http://www.rsa.com

[14] BIZER, JOHANN: Kryptokontroverse - Der Schutz der Vertraulichkeit in der Telekommunikation. In: Kritische Justiz 1995, Heft 4

[15] BIZER, RIESS, ROSSNAGEL: Beschränkungen kryptographischer Verfahren sind verfassungswidrig
http://www.provet.org/kk/stenahme.htm

[16] BIZER, JOHANN: Rechtsprobleme der Vertraulichkeit elektronischer Kommunikation. In: Patrick Horster (Hrsg.): Trust Center - Grundlagen, Rechtliche Aspekte, Standardisierung und Realisierung, Vieweg 1995

[17] MÖLLER, ULF: Kryptographie: Rechtliche Situation
http://www.thur.de/ulf/krypto/verbot.html

[18] Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF): Pressemitteilung vom 10.04.1997

[19] AP-Meldung, Hannoversche Allgemeine Zeitung vom 13.2.1996

[20] Position zur Einführung des *Gesetzes zur digitalen Signatur* und zur Regulierung von Verschlüsselungsverfahren, FAZ vom 11.10.1996, S.19

[21] Hamburger Erklärung für Verschlüsselungsfreiheit, DFN-CERT, Universität Hamburg