Diskussionspapier Nr. 6

Guido Schröder

Kryptographie – Schlüssel zur Informationsgesellschaft?

–

Verschlüsselungstechnik
zwischen
Wettbewerb und Marktversagen

November 1997

Institut für Verkehrswissenschaft
an der Westfälischen Wilhelms-Universität

Am Stadtgraben 9
48143 Münster

Guido Schröder

Kryptographie – Schlüssel zur Informationsgesellschaft?

–

Verschlüsselungstechnik
zwischen
Wettbewerb und Marktversagen

1. Einleitung 3

2. Kryptographie – der Weg einer Kunst zur Wissenschaft 3

2.1 Nachrichtenverkehr im Verborgenen 4
2.2 Die Geburtsstunde der Kryptographie 6
2.3 Wann ist eine Nachricht sicher? 8

3. Nachrichtenverschlüsselung aus nutzentheoretischer Sicht 11

3.1 Nutzenkomponenten der Verschlüsselung 11
3.2 Kosten der Kryptographie 15

4. Trends zur Verschlüsselung im „globalen Dorf“ 21

4.1 Deregulierung 21
4.2 Konvergenz 22
4.3 Globalisierung 23
4.4 Virtualisierung 23

5. Wirtschaftspolitische Aspekte der Kryptographie 25

5.1 Standardisierung als Koordinationsproblem 25
5.2 Marktversagen durch asymmetrische Information 27
5.3 Externe Effekte der Nutzung 28
5.4 Der Staat als Akteur 31

6. Ausblick 33

Danksagung 33

Literaturverzeichnis 34

Weitere Diskussionspapiere 35

1. Einleitung

Seit mehreren tausend Jahren führt die Kryptographie eine Existenz im Verborgenen. Nachweislich seit dem 19. Jahrhundert vor Christi, aber wahrscheinlich schon seit den Anfängen der Kommunikation nutzen Menschen Möglichkeiten, ausgewählte Nachrichten einen bestimmten Empfänger und nur diesen erreichen zu lassen. Andererseits ist die Kryptographie als Lehre vom Ver- und Entschlüsseln von Nachrichten auch heute noch im öffentlichen Bewußtsein nahezu unbekannt. Dies ist verständlich, beschäftigten sich bis vor kurzem noch Kryptologen fast ausschließlich mit für den Privatmann realitätsfernen Anwendungen und standen daher meist im Sold von Geheimdiensten und Militärs.

Dieses Diskussionspapier will aufzeigen, warum sich das Verständnis von kryptographischen Technologien in den kommenden Jahren stark wandeln wird, und welche Bedingungen aus mikroökonomischer Sicht für den sinnvollen Einsatz von Verschlüsselungssystemen auf Seiten privater Anwender erfüllt sein müssen. Da auch Gefahren von diesen Technologien ausgehen können, wird in einem weiteren Schritt der Frage nachzugehen sein, wie eine rationale Wirtschaftspolitik zu gestalten ist, um diesen gesellschaftlichen Risikoaspekten wirkungsvoll zu begegnen.

2. Kryptographie – der Weg einer Kunst zur Wissenschaft

Eine wesentliche Eigenschaft des Menschen ist nicht nur die Fähigkeit des differenzierten Denkens, sondern auch, diese Gedanken in einer vielfältig ausgestalteten Sprache seiner Umwelt mitzuteilen. Die Entwicklung sprachlicher Verständigung ermöglichte erst die Herausbildung komplexer Gesellschaftssysteme, wie wir sie heute kennen. Zur Einführung in die im folgenden verwendeten Begriffe der Verschlüsselungstechnik dient ein kurzer Überblick über die Geschichte der Kommunikation. Viele der hier intuitiv angeführten Gründe für geschichtliche Entwicklungen werden sich im anschließenden Kapitel 3 als ökonomische Notwendigkeiten erklären lassen.

In den meisten Fällen ist das Grundprinzip der Kommunikation sehr einfach und seit mehreren zehntausend Jahren unverändert: Eine Person, die einer anderen etwas mitteilen möchte – der Sender –, benutzt einen mit der Zielperson – dem Empfänger – geteilten gemeinsamen Zeichenvorrat, um an sein Gegenüber eine Nachricht zu übermitteln.

Schon in diesem einfachen Modell wird erkennbar, daß die eigentlichen Inhalte kodiert werden, denn sie müssen vom Sender vor der Übertragung erst in die gemeinsame Sprache – die Codebasis – übersetzt werden. Aus Sicht der heutigen Informationstechnik würde sich die beschriebene Situation als eine Frage der hinreichenden Standardisierung darstellen: Der Empfänger kann den Inhalt der Nachricht nur verstehen, wenn sowohl die Schnittstelle als auch der von beiden Seiten verwendete Code in ausreichendem Maße festgelegt sind. Anders ausgedrückt: Die Teilsysteme müssen auf beiden Seiten einen gewissen Grad an Kompatibilität zum jeweiligen Kommunikationspartner besitzen – und zwar bei Bedarf nur zu diesem. Denn ein Großteil der Individualkommunikation läuft gerichtet ab, d.h. der Sender im genannten Modell will nur einen ganz bestimmten Empfänger oder eine genau umrissene Zielgruppe erreichen. Also stellt sich für ihn das Problem, unerwünschte Zuhörer auszuschließen. Das ist sehr leicht möglich, wenn sich die Beteiligten „unter vier Augen“ verständigen können, also eine räumliche Exklusion funktioniert.[1]

Können unerwünschte Mithörer nicht ohne weiteres außen vor gelassen werden, gestaltet sich eine vertrauliche Kommunikation schwieriger. Denkbar ist beispielsweise der Fall, daß die Nachricht bei der Übermittlung durch ein Gebiet transportiert werden muß, das sich der vollständigen Kontrolle von Sender und Empfänger entzieht. Diesem Problem sieht sich traditionell ein militärischer Anwender gegenüber, der seine Truppenteile über meist größere, unsichere Strecken koordinieren muß. Auf den ersten Blick verwundert es daher nicht, daß die Geschichte der vertraulichen Kommunikation zu großen Teilen in Militärgeschichtsbüchern zu finden ist.[2]

2.1 Nachrichtenverkehr im Verborgenen

Natürlich fanden sich in der Evolution der Kommunikation auch verschiedene Mittel und Wege für die Verständigung unter unsicheren Bedingungen. Als ersten Ansatz könnten beide Partner auf die Idee kommen, die Kommunikation für einen außenstehenden Beobachter versteckt ablaufen zu lassen. Für ihn würde dann ein vorgetäuschter Nachrichteninhalt die tatsächlich Botschaft verschleiern. So könnte es scheinbar um Poesie gehen, während in Wahrheit der Befehl für einen Sabotageakt gegeben wird. Denkbar wäre auch, daß eine Person einer anderen eine Beschreibung zukommen läßt, welche oberflächlich betrachtet eine Strickanleitung darstellt, dem

[1] Vgl. Problem der Exklusion in Kapitel 2, Seite 13.

[2] Etwas differenzierter wird auf weitere, vor allem ökonomische Gründe noch in Kapitel 3 einzugehen sein.

Eingeweihten jedoch durch die Ausführung der Maschen einen geheimen Text offenbart.

Die genannten Beispiele sind weniger fiktiv, als es zunächst den Anschein hat, denn beide sind historisch belegt. So war die am 5. Juni 1944 als persönliche Nachricht von der BBC gesendete Radiomitteilung „Sie verwunden mein Herz mit einer monotonen Mattheit“[3], keine Botschaft einer Wartenden für den Geliebten an der Front, sondern vielmehr die Aufforderung der Alliierten an die französische Resistance, sich für die unmittelbar bevorstehende Invasion in der Normandie bereitzuhalten.[4]

Auch das zweite Beispiel stammt aus der Zeit des Zweiten Weltkriegs. Zur Verhinderung von Inlandsspionage war auf US-amerikanischer Seite eine Behörde ins Leben gerufen worden, die sämtlichen Nachrichtenverkehr einschließlich der Briefe auf versteckte Mitteilungen zu untersuchen hatte. Zu jener Zeit war zwar der Versand von Schachstellungen, Kreuzworträtseln und Kinderzeichnungen untersagt, nicht jedoch, Briefen eine Strickanleitung beizulegen. In einem Einzelfall mußte die Zensurbehörde einen solchen Brief so lange zurückhalten, bis sicher war, daß die beigefügte Anleitung keine versteckte Nachricht enthielt. Zur Klärung dieser Frage wurde der Pullover laut Anleitung gestrickt und anschließend einer kryptologischen Analyse unterzogen – allerdings ohne Erfolg.[5]

So einfach das Mittel auch ist, die eigentliche Botschaft vor den Blicken Dritter dadurch zu verstecken, indem diesen vordergründig ein falscher Inhalt vorgespielt wird, es zeigt schnell Unzulänglichkeiten. Nachteilig ist einerseits der Aufwand, den die Kommunikationspartner für eine geheime Konversation betreiben müssen, andererseits das geringe Ausmaß an Vertraulichkeit, welches damit effektiv erreicht wird. Denn der Text ist nur so lange vor dem Zugriff eines Dritten geschützt, wie dieser nicht das Verfahren kennt, auf welche Art und Weise die Nachricht wirklich zu lesen ist. Vom Zeitpunkt der Entdeckung an ist alle nachfolgende Kommunikation – im schlimmsten Fall auch die davorliegende – völlig ungeschützt. Trotz dieser

[3] Im französischen Original: „Blessent mon coeur d´une langueur monotone“.

[4] Vgl. **Kahn** (1967), S. 543.

[5] Ein generelles Problem der Kommunikation besteht hierbei in verschärfter Form: Welche Botschaft hat der Sender wirklich gemeint? Schon bei einfachen Sender-Empfänger-Systemen müssen beide Seiten davon ausgehen, daß das Gegenüber mit der Codebasis die gleiche Bedeutung verbindet. Der Versuch, versteckte Nachrichten zu finden, wird daher zwangsläufig an die Grenze stoßen, daß Mutmaßungen über den intendierten Inhalt der Nachricht getroffen werden müssen. Inwieweit daher altertümliche Texte wie die Bibel versteckte Nachrichten in Form von Prophezeiungen enthalten – wie von Drosnin dargelegt –, wird sich mit wissenschaftlicher Gewißheit nie klären lassen. Vgl. **Drosnin** (1997).

Probleme erlebt die Steganographie als Wissenschaft, systematisch Nachrichten zu verstecken, gerade in letzter Zeit dank Computerunterstützung einen Aufschwung.[6]

2.2 Die Geburtsstunde der Kryptographie

Durch eine konsequente Weiterentwicklung der Steganographie läßt sich ein besserer Grad an Geheimhaltung erreichen. Die Kommunikationspartner könnten nämlich vereinbaren, die Tarnung aufzugeben und die verwendete Sprache so abzuändern, daß sie für Außenstehende als Mitteilung offen erkennbar, aber trotzdem unverständlich ist. In Ansätzen ist dieser Vorgang in der Realität allgegenwärtig, also weniger abstrakt, als es zunächst klingen mag. Menschen entwickeln oft ganz spontan eine eigene Art der Wortwahl und Grammatik, die für Dritte manchmal nur mit Erläuterung verständlich ist.[7] Ganz offensichtlich ist dieses Phänomen bei bestimmten Berufsgruppen, die eine spezifische Fachsprache benutzen, genauso wie bei Personen, die der gleichen sozialen Gruppe angehören, Hobbys teilen oder einfach viel Zeit miteinander verbracht haben.

Die gemeinsame Sprache wird hier einerseits zum Mittel der effizienten Kommunikation, denn das Fachvokabular ist meist besser zur Beschreibung spezifischer Inhalte geeignet als ein eher universeller Standardwortschatz. Andererseits ist sie Ausdruck der eigenen Identität über die Gruppenzugehörigkeit, dient also gleichzeitig der Ausgrenzung von Dritten, da diese sich schon durch ihre Ausdrucksweise als Laien entpuppen.

Beide Effekte lassen sich sowohl bei Fachsprachen[8] als auch bei gruppenspezifischen Dialekten erkennen, welche den Träger als ein authorisiertes Mitglied dieser Kreise ausweisen und Fremden den Zutritt verwehren. Beispiele hierfür sind die vielfältigen Jugend- oder Gaunerslangs – wie das französiche l´argot oder das westfälische Masematte –, aber auch die Sprachen ethnischer Gruppen wie Innuit oder Indianer.

Daß es mit Hilfe von Sprachen auch praktisch möglich ist, die Vertraulichkeit einer Botschaft zu sichern, wurde von der U.S. Navy im Zweiten Weltkrieg ein-

---

[6] Auf die Gründe hierfür und die Folgen der Anwendung steganographischer Techniken wird weiter unten noch einzugehen sein. Vgl. Kapitel 4.4, S. 23.

[7] Für Historiker stellt sich in der Tat die Entwicklung von kryptographischen Verfahren als ein spontanes Ereignis dar, das eintritt, wenn in der betrachteten Gesellschaft ein gewisser Grad an Alphabetisierung erreicht wurde. Vgl. **Kahn** (1967), S. 84. Diese These ist nur begrenzt haltbar, da vielmehr ein ökonomisches Kalkül, wie es Gegenstand des Kapitels 3 ist, als entscheidend für die Entwicklung von Kryptographie in einer Gesellschaft betrachtet werden kann.

[8] Das früher in klerikalen Kreisen gesprochene Latein wurde zum Synonym der Unverständlichkeit auch in anderen Bereichen wie Medizin, Jagd oder Segelsport.

drucksvoll demonstriert: Dem japanischen Gegner gelang es während des gesamten Kriegsverlaufs nicht, den Nachrichtenverkehr der als Funker eingesetzten Navaho-Indianer zu entschlüsseln, da ihre Sprache über einen sehr spezifischen Klang und eine eigenständige Grammatik verfügt.[9]

In gewisser Weise lassen sich schon in der Verwendung von Dialekten und Jargons Grundzüge ausmachen, die zur Entwicklung der Kryptographie, also der Verschlüsselungstechnik als Wissenschaft, geführt haben. Wie gesehen bedeutet ein Dialekt, daß die Kommunikationspartner den übermittelten Code so verändern, daß ein Unbefugter den Inhalt nicht verstehen kann –, ihn also verschlüsseln. Anstatt die von beiden verwendete Sprache aber in gezeigter Weise zu verändern, geht die Kryptographie einen eleganteren Weg, der sich auf den ersten Blick wie eine Komplizierung darstellt: Es wird nämlich sowohl auf der Sender- wie Empfängerseite eine zusätzliche Stufe eingefügt, was nachstehende Abbildung 1 verdeutlicht.

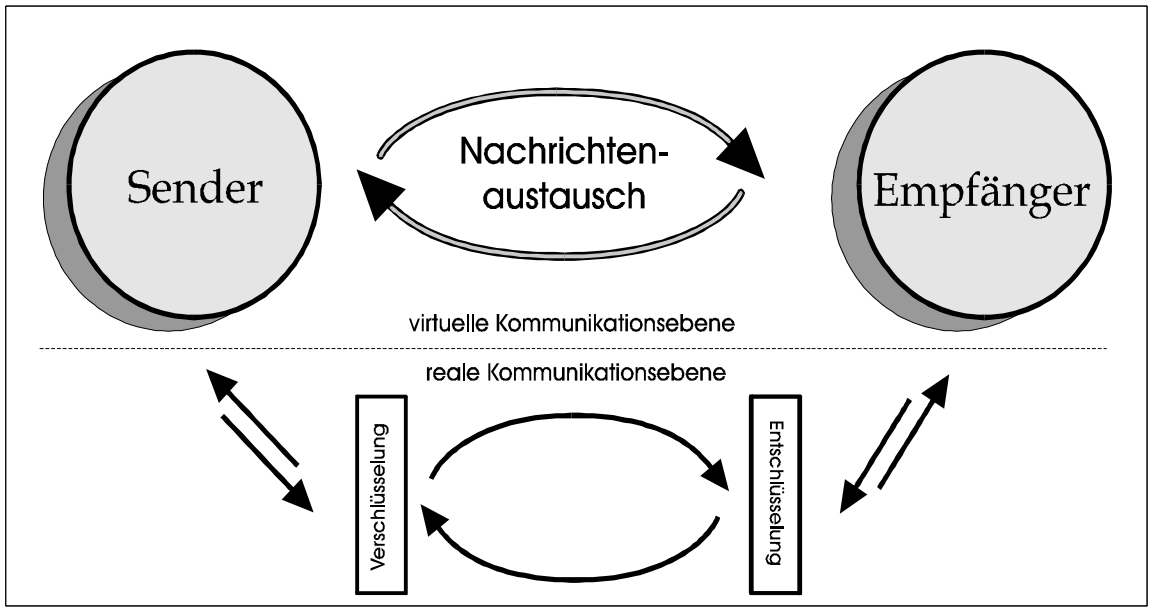


Abbildung 1: Einfaches Sender-Empfänger-Modell

Diese Stufe übernimmt die eigentliche kryptographische Arbeit, also die Verschlüsselung auf der Senderseite und die Entschlüsselung als Rückübersetzung auf der Empfängerseite. Damit ergeben sich weitreichende Vorteile gegenüber den beiden bisher beschriebenen Verfahren. Das Verstecken der Nachricht war unsicher; ein Dialekt war von den Beteiligten mühsam zu erlernen und konnte nur schwer geändert werden, falls ein unerwünschter Dritter ihn verstehen konnte. Auf das Beispiel der amerikanischen Funker bezogen, wäre das gesamte System hinfällig gewesen, wenn den Japanern ein indianischer Übersetzer zur Verfügung gestanden hätte. Da-

[9] Vgl. **Kahn** (1967), S. 549.

gegen wird ein kryptographischer Code, genauer der benutzte Schlüssel, vom verwendeten Verschlüsselungssystem generiert und verwaltet, ist also vergleichsweise schnell und leicht austauschbar. Als Folge davon ist das System wesentlich sicherer gegen Lauschversuche Dritter als eine spezifische Sprache.

Für den Laien ähnelt das beschriebene Verfahren von außen betrachtet einer „black box“ oder hier besser: einer verschließbaren Stahlkassette. Der Sender legt seine Nachricht in die Kassette und verschließt, d.h. verschlüsselt, die Nachricht mit seinem Schlüssel. In diesem Transportcontainer wandert die Nachricht vom Sender zum Empfänger – gut gesichert gegen Blicke unauthorisierter Dritter. Der Empfänger wiederum benutzt seinen Schlüssel zum Öffnen der Kassette, d.h. zum Entschlüsseln, und ist nun im Besitz der Originalnachricht. Wie sicher die Botschaft wirklich ist, hängt ganz entscheidend von der Güte des Schließmechanismus ab. Ist er sehr einfach konstruiert, kann ein Eindringling schon mit Hilfe einfacher Werkzeuge die Kassette öffnen, die Nachricht entnehmen oder diese gar durch eine eigene Nachricht ersetzen. Das Problem tritt in der Kryptographie in genau gleicher Weise auf: Ist das Verschlüsselungsverfahren – der Algorithmus – zu einfach konstruiert, bietet es real geringen oder keinen Schutz, meist ohne daß der Anwender hiervon etwas erfährt.[10]

2.3 Wann ist eine Nachricht sicher?

Dem mit wissenschaftlichen Methoden entgegenzutreten, ist das Anliegen der Kryptologie. Dabei läßt sich die kryptologische Forschung in zwei Teildisziplinen einteilen – in die Kryptographie, von der bisher die Rede war, und die Kryptoanalyse. Das Vorgehen läßt sich also folgendermaßen beschreiben: Einerseits werden kryptographische Algorithmen entwickelt, die ein – hoffentlich – hohes Maß an Sicherheit für den Anwender besitzen. Andererseits versucht die Kryptoanalyse diese neuen Verfahren mit analytischen Werkzeugen auf ihr wirklich erreichtes Sicherheitsniveau zu testen. Der Kryptologie wohnt damit seit jeher eine zwar wissenschaftlich einwandfreie, jedoch real verwirrende Schizophrenie inne: die Kryptographie versucht zusammen mit ihrem kryptoanalytischen Gegenpart zu sicheren Kommunikationsverfahren zu kommen.[11]

---

[10] Wie in Kapitel 5.2 dargelegt, kann dies zu Fällen adverser Selektion beim Angebot von kryptographischen Produkten führen. Vgl. S. 27.

[11] Dieses Problem kann – im Zusammenhang mit anderen Anhaltspunkte für ein Marktversagen – zu erheblichen politischen Problemen führen, welche sich real in Diskussionen um die Rolle staatlicher Institutionen im Bereich der kryptologischen Forschung manifestieren. Vgl. Kapitel 5.4, S. 31.

Naturgemäß geht der Kryptoanalytiker mit dem größtmöglichen Pessimismus an die Beurteilung von Verschlüsselungssystemen – Normalfall ist der „worst case“, d.h. ein unbefugter Dritter, der an den Inhalt der Botschaft zu kommen versucht, besitzt beliebig viel Zeit, und ihm stehen in unbeschränktem Ausmaß Sachverstand und Ressourcen wie Computer-Rechenleistung zu Verfügung. Natürlich sind diese Bedingungen in der Realität nicht gegeben, da ökonomische Zwänge einem Eindringling immer die Hände binden. Ebenso wird der Faktor Zeit eine entscheidende Rolle spielen, da es nicht unerheblich sein kann, ob eine Nachricht heute oder in zehn Jahren entschlüsselt wird, wenn ihr Inhalt vielleicht schon bekannt oder längst veraltet ist. Dennoch ist der schlimmste Fall eine geeignete Basis zur Bestimmung der theoretisch gebotenen Sicherheit, da das reale Schutzniveau immer hierüber liegen wird.

Diese Aussage bleibt selbst dann gültig, sollten nicht nur seine subjektiven Eigenschaften, sondern auch die äußeren Umstände dem Unbefugten zu Hilfe kommen. Das ist beispielsweise dann der Fall, wenn er nicht nur Zugriff auf die verschlüsselte Botschaft hat, sondern auch den Verschlüsselungsmechanismus kennt und diesen mit eigenen Nachrichten ausprobieren kann. Was ihn dann noch vom Inhalt der Botschaft trennt, ist der Schlüssel, den Sender und Empfänger gemeinsam besitzen. Seit dem Mathematiker Kerkhoff ist bekannt, daß in diesem schlimmsten Fall die Sicherheit des Gesamtsystems allein auf dem Schlüssel beruht.[12]

Im Umkehrschluß kann mit dieser Erkenntnis aber die Güte eines kryptographischen Systems sehr einfach quantifiziert werden. Denn die Sicherheit einer Nachricht läßt sich als die Zeit auffassen, die ein perfekt ausgestatteter Dritter durchschnittlich im für ihn idealen Fall benötigt, um an einen Nachschlüssel als Kopie des benutzten Originals und damit an den Inhalt der Botschaft zu kommen.

Bemerkenswert an dieser Definition ist nicht nur das Abstellen auf ein Szenario des schlimmsten theoretisch möglichen Falls, sondern aus ökonomischer Sicht vor allem das völlige Fehlen wirtschaftlicher Bezugsgrößen. Im „worst case“ sind Zeit und andere Ressourcen nicht mehr – wie gewöhnlich – knapp und deshalb teuer, vielmehr stehen sie dem Eindringling zu freien Verfügung. Das Ziel ist die Entschlüsselung der Nachricht, doch wird der mögliche Wert des Nachrichteninhalts in keinerlei Relation zum getriebenen Aufwand gesetzt. Obwohl diese ökonomischen Einwände real eine – möglicherweise sogar die wichtigste – Rolle spielen, ist es auf-

[12] Vgl. **Beutelspacher** (1996), S. 23.

schlußreich, für einen Moment zu unterstellen, daß ökonomische Zwänge wie Zeitbedarf und Ressourcenaufwand per Definition aufgehoben sind.

Läßt der verschlüsselte Text keinen Rückschluß auf den Schlüssel zu, was gute Algorithmen zu verhindern suchen, bleibt dem Eindringling nichts anderes übrig, als alle möglichen Schlüsselvarianten anhand des ihm bekannten Algorithmus systematisch auf ihre Eignung zu prüfen. War dieser Weg bis vor 50 Jahren praktisch ungangbar, so brach auch in der Kryptographie mit der Erfindung des Computers ein neues Zeitalter an. Erstmals im zweiten Weltkrieg war es mit Hilfe der neuen Maschinen möglich, Schlüsselkombinationen der Reihe nach, quasi mit „brachialer Gewalt“, durchzuprobieren. Daß es den Alliierten gelang, den U-Boot-Code der deutschen Enigma-Chiffriermaschinen zu brechen, war neben dem wissenschaftlichen Sachverstand vor allem auf die „Bomben“, die im englischen Bletchley Park installierten Röhrenrechner, zurückzuführen.

Für die kryptoanalytische Forschung bedeutet das aber, daß es – mit Ausnahme eines in der Praxis irrelevanten Ausnahmefalls – kein absolut sicheres Verschlüsselungsverfahren gibt. Denn bei jedem Algorithmus lassen sich alle benutzbaren Schlüsselkombinationen automatisch Schritt für Schritt testen. Wenn der berechtigte Benutzer einen funktionierenden Schlüssel besitzt, so wird der Eindringling ihn früher oder später finden. Ein ernsthafter Grund, die Sicherheit einer Nachricht in Zweifel zu ziehen, ist dies jedoch nicht. Denn beim gegenwärtigen Stand der Technik kann, selbst wenn alle weltweit verfügbare Rechenkapazität gebündelt würde, dieses „später“ sehr viel später sein und unter Umständen jenseits des Zeitpunkts liegen, an dem unser Sonnensystem aufgehört hat zu existieren. Für den Benutzer wird diese „relative“ Sicherheit – eine durchschnittlich sehr lange Zeit bis zur potentiellen Entschlüsselung – mehr als ausreichend sein, auch wenn prognostiziert wird, daß die Computertechnik weiterhin in den kommenden Jahren signifikante Geschwindigkeitssteigerungen erleben wird.

Wohl gemerkt: diese „relative“ Sicherheit existiert schon in der bisher von ökonomischen Zwängen befreiten Theoriewelt. Doch es sind gerade Überlegungen der Wirtschaftlichkeit, die neben diesen theoretischen Faktoren für das Ausmaß an effektiv erzielter Sicherheit eine entscheidende Rolle spielen. Im folgenden Abschnitt soll deshalb kurz auf das ökonomische Entscheidungskalkül des Nutzers und eines möglichen Eindringlings im Zusammenhang mit dem Schutz seiner Privatsphäre eingegangen werden. Diese mikroökonomische Fundierung ist notwendig für die spätere Beantwortung der Frage, ob es ein Marktversagen im Bereich der Krypto-

graphie gibt, welches im Zentrum des dann anschließenden Kapitels stehen wird. Sollten sich Anhaltspunkte für ein systembedingtes Nichtfunktionieren der dezentralen Koordination über Märkte ergeben, wird zu diskutieren sein, ob wirtschaftspolitische Maßnahmen dem effektiv begegnen können.

3. Nachrichtenverschlüsselung aus nutzentheoretischer Sicht

Eine erste Annäherung an die ökonomischen Grundlagen der Kryptographie liefert ein nutzentheoretischer Ansatz. Im Mittelpunkt steht dabei die Analyse der rationalen Beweggründe, weshalb sich ein individueller Nutzer generell zur Verschlüsselung seiner Kommunikation entscheidet.

Aus seiner Sicht stellt sowohl das generelle Für und Wider kryptographischer Verfahren als auch seine Entscheidungen im Zusammenhang damit – von Sicherheit der Übertragung bis zum Schlüsselmanagement – eine Investition in die eigene Kommunikationssicherheit dar, die einem ökonomischen Kosten-Nutzen-Kalkül folgt. Dies wird anhand der nachfolgenden Formel 1 deutlich:

$$U_N = U_B - K_{ges}$$

Vorteilhaftigkeit der Kryptographie (Nettonutzen)
= Nutzen aus Nachrichtengeheimhaltung - Kosten des Verfahrenseinsatzes

Formel 1: Nutzentheoretisches Ausgangskalkül

Die Gleichung beschreibt die Vorteilhafigkeit des Einsatzes von Verschlüsselungsverfahren im Vergleich zu einer unverschlüsselten Nachrichtenübertragung. Nur wenn der Nettonutzen U_N positiv wird, ist für den Nutzer eine Investition in Kryptographie sinnvoll. Bezugsbasis der Überlegungen kann der gesamte Nachrichtenverkehr zweier Kommunikationspartner sein oder nur die Verschlüsselung einer einzelnen Nachricht, wie sie zunächst unterstellt wird.

3.1 Nutzenkomponenten der Verschlüsselung

Auf der Nutzenseite finden sich die Komponenten, welche den Bruttonutzen U_B der Verschlüsselung der Botschaft ausmachen. Da eine Verschlüsselung generell eingesetzt wird, um einen Schaden zu vermeiden, der aus dem Lesen und vielleicht aus der Veränderung einer Nachricht durch einen Dritten droht, ergibt sich dieser Bruttonutzen U_B als vermiedene Opportunitätskosten der genannten Risiken. Gegen diese Risiken bietet die Kryptographie eine Art Versicherung – mit Zahlung der

„Versicherungsprämie“ K_{ges} erkauft sich der Anwender idealerweise hundertprozentigen Schutz der Vertraulichkeit. Wie in der Versicherungsmathematik üblich lassen sich hier die einzelnen Schadenskosten in ihre beiden Bestandteile Schadensausmaß und -eintrittswahrscheinlichkeit auflösen, was zu nachstehender Formel 2 führt:

$$U_B = S_B + S_V$$
$$= A_B * w(A_B) + A_V * w(A_V)$$

Bruttonutzen der Einsatzentscheidung
= vermiedener Schaden durch Bekanntwerden der Nachricht
* Wahrscheinlichkeit dieser Aufdeckung
+ vermiedener Schaden durch Veränderung des Inhalts
* Wahrscheinlichkeit dieser Veränderung

Formel 2: Aufspaltung der Opportunitätserlöse in Schadensdimensionen

Noch ohne Kostenüberlegungen einzubeziehen, lassen sich schon anhand dieser Formel einige grundlegende Aussagen ableiten.

These 1
Nur ein Bruchteil der jeden Tag übermittelten Nachrichten ist es wert, verschlüsselt zu werden.

Dieser These leuchtet unmittelbar ein, denn ein Großteil der alltäglichen Kommunikation hat nur einen Sinn in der jeweiligen Situation und zum entsprechenden Zeitpunkt. Danach geht der Wert der Nachricht gegen null und ein Außenstehender kann nur wenig oder nichts mit ihr anfangen. Ähnlich der maximalen Nutzungsdauer vieler Güter haben die meisten alltäglichen Mitteilungen ein „Verfallsdatum“, bei dessen Überschreiten sie irrelevant werden. Plastisch ausgedrückt: Nachrichten werden – sofern sie keinen historischen Wert besitzen – nach Ablauf der Haltbarkeitsfrist zu „Informationsmüll“.

Diese eingeschränkte Verwendbarkeit in Form einer hohen zeitlichen Spezifität wird begleitet von einer weiteren Restriktion bei der Nutz- und Übertragbarkeit der Information. Denn obwohl sie vielleicht nicht veraltet, kann eine Information für einen Dritten – im Extremfall für alle außer den beiden Kommunikationspartnern – völlig wertlos sein. Diese Situation tritt ein, wenn die Nachricht sehr personenspezifisch ist, also nur für Sender und Empfänger einen Nutzen besitzt. Nur in der einen Verwendung fällt also ein Nutzen an, weshalb aus Sicht der Transaktionskostenökonomie hier die Information ein sehr spezifisches Gut darstellt, das eine hohe Quasi-

rente aus der fehlenden Übertragbarkeit des Nutzens auf Dritte erwirtschaftet. Wenn das Gut aber nicht oder nur sehr eingeschränkt übertragbar ist, kann aus der Übertragung kein Schaden resultieren, womit auch die vermiedenen Opportunitätskosten gering oder gleich null wären. Bezogen auf Formel 2 gehen damit der Faktor A_B und ebenso der Nutzen der Verschlüsselung gegen Null.

These 1 läßt sich damit enger fassen: Da Nachrichten im Alltag häufig sowohl zeitlich spezifisch und als auch personengebunden sind, ist es nur selten sinnvoll, diese zu verschlüsseln. Wohlgemerkt ist diese Folgerung nur richtig vor dem Hintergrund des beschriebenen Kosten-Nutzen-Kalküls.[13]

These 2
Der Einsatz von Kryptographie in einer von Dritten nicht erreichbaren Umgebung ist wenig sinnvoll.

Um diese These zu verdeutlichen, ist es zunächst notwendig, den Ausdruck „von Dritten nicht erreichbare Umgebung“ näher zu bestimmen. Hierunter soll ein Umfeld verstanden werden, das sich in der Regel ausschließlich unter der Kontrolle von Sender und Empfänger befindet, womit sie also den unrechtmäßigen Zugriff Dritter erfolgreich verhindern können. Wie bei einem privaten Gut, bei dem der Besitzer Unbefugte von der Nutzung ausschließen kann, ist es dem Sender in vielen Fällen möglich, durch einfache Vorkehrungen dem Mithören im wahrsten Sinne des Wortes einen Riegel vorzuschieben. Denn meistens wird der Schutz der Privatsphäre durch räumliche Maßnahmen sichergestellt. Hierunter fallen alltägliche Fälle – Wände verhindern ein Mithören oder ein Gespräch findet „unter vier Augen“ statt – ebenso wie hauseigene Computernetze oder Telefonkabel, die durch Tiefseegewässer geführt werden.

Daß ein Einsatz von Kryptographie erst nötig wird, wenn die genannten Vorkehrungen nicht mehr als Schutz ausreichen, war schon angeklungen[14] und ist ohne weiteres einsichtig. Formal läßt sich diese Aussage anhand von Formel 2 beschreiben:

[13] Implizite Prämisse war bisher, daß die Sicherheit einer Nachricht nur von ihren eigenen Schutzmaßnahmen abhängt. Bei Nachrichten, deren reine Existenz schon für einen Dritten einen Informationsgehalt besitzt, ist diese Annahme jedoch nicht ohne weiteres erfüllt. Hier kann es vorteilhaft sein, den gesamten Nachrichtenverkehr zu verschlüsseln, da sonst der Akt der Verschlüsselung einen Rückschluß auf die Wichtigkeit des Nachrichteninhalts zuließe, also zwischen den einzelnen Nachrichten eine Interdependenz in Form einer Externalität bestünde.

[14] Vgl. Kapitel 2, S. 4.

Der Faktor $w(A_B)$ bezeichnet die Wahrscheinlichkeit[15] der Entschlüsselung einer Botschaft. Er kann Werte von Null, wie hundertprozentig sicher, bis Eins, völlig unsicher, annehmen. In einer Umgebung, die Dritten nicht zugänglich ist, muß dieser Faktor den Wert null annehmen, denn ein Mithören kann es hier nicht geben. Folglich ist das Risiko, durch Entschlüsselung geschädigt zu werden, gleich null – unabhängig von der eigentlichen Höhe des möglichen Schadens.

Für die generelle Entscheidung für oder wider des Einsatzes von Kryptographie bedeutet dies aber, daß Nutzenbestandteile in Form von Opportunitätserlösen, also vermiedenen Opportunitätskosten, nicht auftreten. Aussage 2 läßt sich daher in einem weiteren Schritt konkretisieren: Wenn Vertraulichkeit der Kommunikation schon durch andere – meist billigere Maßnahmen sichergestellt ist – kann es nicht mehr vorteilhaft sein, noch kryptographische Verfahren einzusetzen.

Vergleichbar ist dies mit der eingangs erwähnten Stahlkassette, die dem Schutz der Nachricht vor neugierigen Blicken dient. Die Nachricht ist gut aufgehoben, wenn der Schließmechanismus wirklich sicher ist. Kommen hieran Zweifel auf, kann es ratsam sein, die Kassette wiederum in einem Stahltresor aufzubewahren. Genau diese Sicherheitsüberlegungen bringt der Faktor $w(A_B)$ zum Ausdruck: Kryptographie setzt ein, wenn andere Mittel ein Risiko unabgedeckt lassen. Da $w(A_B)$ von der betrachteten Umgebung abhängig ist, gilt dies auch für das Ergebnis des Entscheidungskalküls.

Beispielsweise stellt sich ein von Julius Cäsar zur Geheimhaltung seiner Briefe benutztes Verfahren heutzutage als lächerlich einfacher Schutz dar, dessen Entschlüsselung in jedem modernen Lehrbuch der Kryptographie als einführende Übungsaufgabe behandelt wird. Doch für den römischen Imperator war das erreichte Schutzniveau völlig ausreichend, denn zu seiner Zeit konnte ein Großteil der Bevölkerung weder lesen noch schreiben. Er mußte also nur noch ein vergleichsweise geringes Restrisiko durch die Verschlüsselung abdecken. Im Umkehrschluß läßt sich damit die Schriftsprache im alten Rom als ein Verschlüsselungsverfahren verstehen, was geeignet war, die Botschaft wirksam vor Zuhörern und unbefugten Lesern zu schützen. In letzter Konsequenz ist es also eine Wahl des Standpunkts, ab welchem Komplexitäts- und Abstraktionsgrad man eine Kommunikationsform, welche Inhalte notwendigerweise als Symbole, Schrift oder Sprache kodiert, als kryptographisch

[15] Diese Wahrscheinlichkeit $w(A_B)$ ist keine intersubjektiv einheitliche Größe. Neben den rein objektiven Einflußfaktoren spielen Risikowahrnehmung und Risikoeinstellung eine gewisse Rolle und beeinflussen so das Ergebnis des Einsatzkalküls.

ansieht. Wie das Beispiel der Navaho-Indianer zeigt, kann im Extremfall selbst die menschliche Sprache zu kryptographischen Zwecken eingesetzt werden. Über die Kodierung der Inhalte kann sie – im richtigen Kontext eingesetzt – genauso sicher sein, wie ein hochmodernes „public-key"-Verfahren.

Damit wird eine zweite, prozeßorientierte Dimension des Faktors $w(A_B)$ deutlich. Diese Größe wird nicht nur durch das Umfeld beeinflußt, sondern auch die Sicherheit des eingesetzten Algorithmus schlägt sich in ihr nieder. In einem ungeschützten Kontext mit $w(A_B)$ deutlich größer null würde eine sichere Verschlüsselung $w(A_B)$ ex post, d.h. im Betrieb, idealerweise auf den Wert null senken. Eingesparte Opportunitätskosten sind deshalb voll im Umfang von $w(A_B)$ der Einsatzentscheidung zuzurechnen. Im Gegensatz dazu würde ein unsicherer Algorithmus ex post $w(A_B)$ nur wenig senken. Damit verbunden wäre eine Verminderung sowohl der entsprechenden Erlöse als auch der Vorteilhaftigkeit der Maßnahme. Wie bei einer Versicherung mit Selbstbehalt könnten Teile der verbleibenden Schäden nicht voll vom Nutzer überwälzt werden.

Der zweite Summand in Formel 2 bildet die Schäden ab, die durch die Veränderung einer Nachricht entstehen. Neben der eigentlichen Entdeckung kann die Beeinflussung des Nachrichteninhalts einen ebenso großen, wenn nicht sogar bedeutenderen Schaden mit sich bringen. Folglich kann die Schadenssumme S_V real größere Werte als S_B annehmen. Zum Beispiel gehört nicht viel Phantasie dazu, sich die unangenehmen Folgen für den Kontoinhaber auszumalen, wenn bei einer elektronischen Lastschrift sowohl das Empfängerkonto als auch der Betrag geändert werden. Die Risiken der Verfälschung des eigentlichen Nachrichteninhalts bildet der zweite Term in Formel 2 ab, wobei die Bedeutung der einzelnen Faktoren analog zum Fall des Aufdeckungsrisikos zu sehen ist. Die bisherigen Überlegungen lassen sich deshalb leicht auf diesen Fall übertragen.

3.2 Kosten der Kryptographie

Bis zu diesem Punkt war nur von den möglichen Nutzenkomponenten der Verschlüsselung die Rede. Auf Basis des Kosten-Nutzen-Kalkül sollen nun auch Kostendimensionen Eingang in die Betrachtung finden. Die Kosten des Einsatzes von

Kryptographie als Versicherung der Privatsphäre[16] lassen sich im wesentlichen in zwei Komponenten gliedern, wie sie durch Formel 3 dargestellt werden:

$$K_{ges} = K_{dir} + K_{ind}$$
$$= K_{fix} + K_{var} + K_s$$

Kosten beim Einsatz von Kryptographie
= direkte Kosten beim Verfahrenseinsatz + indirekte Kosten
= fixe Investitionskosten K_{fix} + variable Kosten K_{var}
+ Kosten der Schlüsselverwaltung K_S

Formel 3: Auflösung der Gesamtkosten in Komponenten

Die zur Risikogröße $w(A_B)$ angestellten Überlegungen stehen nicht zufällig in engem argumentativen Zusammenhang mit der hier analysierten Kostenseite, denn beide Teilaspekte verbindet eine wichtige Gemeinsamkeit: Beide haben in den letzten Jahren in einschneidender Weise eine Veränderung durch technischen und wissenschaftlichen Fortschritt erfahren, die das bisherige Verständnis von Kryptographie grundlegend gewandelt hat. Anhand einer Analyse von Formel 3 läßt sich diese Entwicklung nachzeichnen und gleichzeitig ein Einblick in die relevanten Kostenaspekte gewinnen. In der Formel werden Kosten im Hinblick auf ihren Entstehungsort unterschieden, wobei unter den direkten Kosten des Verfahrens alle Kosten verstanden werden sollen, die direkt bei der Anwendung der Kryptographie anfallen, also nicht Kosten im Sinne von K_S für das später besprochene Schlüsselmanagement sind.

Diese direkten Verfahrenskosten werden wiederum in einmalig auftretende und wiederholt anfallende Kosten aufgespalten, wobei sich die Kostenkategorien unter Zuhilfenahme des inzwischen vertrauten Sender-Empfänger-Modells erläutern lassen: Einmalige Verfahrenskosten fallen bei der Beschaffung und Installation der „black box“ an, die die eigentliche Verschlüsselung vornimmt. Laufende Kosten entstehen in erster Linie durch den Betrieb dieser „box“ sowie durch den zeitlichen Aufwand, den beide Kommunikationspartner bei der Ver- und Entschlüsselung erbringen müssen, beispielsweise aus den Verzögerungen im Nachrichtenverkehr.

Um die Argumentation überschaubar zu halten, war bisher der Ausdruck „black box“ ein Platzhalter für jeden beliebigen Algorithmus und jede nur denkbare Ma-

[16] In sehr ähnlichen Überlegungen läßt sich das Kalkül des Eindringlings beschreiben. Nur stellt er dem Nutzen aus der Nachrichtenaufdeckung hierfür nötige Kosten gegenüber. Wiederum ist die

schine, die diesen anwenden kann. Verglichen mit der langen Geschichte der Kryptographie ist diese Interpretation noch relativ jung. Denn bis vor 50 Jahren konnte von einer Trennung zwischen Verschlüsselungsmechanismus und Algorithmus nicht die Rede sein, schließlich waren beide untrennbar miteinander verbunden. So repräsentierte das deutsche „Enigma"-Gerät gleichzeitig Verfahren und Maschine. Bei ihrer Konstruktion war lediglich der Austausch bestimmter Teile – der Rotoren – sowie die Änderung des Schlüssels vorgesehen worden. Eine Umstellung auf ein vollkommen anderes Verschlüsselungsprogramm war schlicht unmöglich.

Aus ökonomischer Sicht bedeutet diese Eigenschaft, daß früher der Einsatz von Kryptographie eine sehr spezifische Investition zur Folge hatte, welche nur in einer Verwendungsrichtung einen Wert hatte, nämlich als Einrichtung zum Schutz der Privatsphäre. Da damals ein Massenmarkt nicht bestand, mußten die eigens zu diesem Zweck konstruierten Maschinen mit vergleichsweise geringen Stückzahlen aufgelegt werden. An eine Kostendegression durch Massenfertigung war nicht zu denken, weshalb die Maschinen teuer waren, ausgedrückt als hohe Investitionssumme K_{fix} in Formel 3.

Berücksichtigt man zusätzlich, daß gleichzeitig die laufenden Kosten sehr hoch waren, da speziell geschultes Personal die umständlich zu bedienenden Geräte handhaben mußte, wird klar, warum sich damals nur sehr wenige Nutzer auf die Verschlüsselungstechnik einließen. Denn laufende Kosten, ausgedrückt im Faktor K_{var}, verschlechterten zusammen mit den hohen und spezifischen Investitionskosten das Verhältnis von Kosten zu Nutzen. Gemäß Formel 1 ist jedoch ein wirtschaftlicher Einsatz von Kryptographie nur möglich, wenn den hohen Kosten der Technik Opportunitätserlöse in mindestens gleicher Höhe entgegenstehen, d.h. die Technik sehr wertvolle Nachrichten vor der Aufdeckung schützt. Diese Bedingung war lange Zeit nur bei einigen ausgewählten geschäftlichen Einsatzfeldern, vor allem aber im militärischen Bereich, in der Diplomatie und der Spionage erfüllt. In allen anderen Bereichen war entweder die Botschaft nicht schutzbedürftig oder aber nicht gefährdet genug, da andere Maßnahmen zum Schutz ausreichten.

Vor dem Hintergrund dieses einfachen Kosten-Nutzen-Kalküls wird verständlich, warum die Kryptographie bis zum Beginn dieses Jahrhunderts quasi keine privaten Anwendungen kannte und ihr auch heute noch ein Hauch von Abenteuer á la James Bond anhaftet. Gleichzeitig wird klar, daß die eingangs vereinfachend als spontan

Nutzenseite mit Unsicherheiten behaftet, während die Kosten sich recht eindeutig quantifizieren lassen.

bezeichnete Entwicklung der Kryptographie vielmehr einem rationalen Kalkül folgt, das nur sehr vage mit dem Grad der Schriftlichkeit einer Gesellschaft korreliert ist, es sei denn schon die Schriftsprache – wie oben angedeutet – wird als kryptographisches Verfahren verstanden.

Doch es zeichnet sich ab, daß sich in den kommenden Jahren das Bild vom Kryptologen in Tarnuniform radikal ändern wird. Hierfür genügt schon ein Blick in die jüngste Vergangenheit. Ausgangspunkt ist der rasante Fortschritt der Computertechnik. Dieser hat dazu geführt, daß heutzutage leistungsfähige Rechner so preiswert und verbreitet sind wie nie zuvor. Es liegt also nahe, den Computer als kryptographische „black box“ im Sinne obiger Definition zu verstehen, nämlich als das Zusammenspiel ausführender Hardware mit dem Verschlüsselungsalgorithmus in Softwareform. Anders ausgedrückt, ist es heute vielfach nicht mehr nötig, in spezielle Geräte zur Verschlüsselung zu investieren, ein für andere Zwecke eingesetzter Computer erfüllt diese Rolle quasi nebenbei – besser noch: im Idealfall transparent im Hintergrund ohne Zutun des Benutzers.

Diese Entwicklung läßt sich mit Hilfe von Formel 3 veranschaulichen. Da der mögliche Nutzer nur noch in Software statt in ein vollintegriertes System aus Hard- und Software investieren muß, sinkt die einmalige Investitionssumme K_{fix} beträchtlich. Zusätzlich kann der Preis des einzeln beschafften Verschlüsselungsprogramms deutlich niedriger ausfallen als der Softwarepreis im Paket.

Dies wird verständlich, wenn man sich die Eigenschaften dieses Gutes vor Augen führt. Software ist, wie jedes Informationsgut, sehr vorleistungsintensiv, verursacht aber bei der Reproduktion nur geringe Grenzkosten. Der Softwareproduzent kann mit steigenden Absatzzahlen also Fixkostendegressionsvorteile erzielen, die er in der Konkurrenzsituation teilweise an die Kunden weitergeben muß. Besonders bei weitverbreiteten Computerplattformen wird sich so ein Preis einspielen, der deutlich unter dem Softwarepreis in einer vollständig integrierten „black box“ liegt.

Verbunden mit dem Rückgang der Investitionssumme K_{fix}, aber wahrscheinlich noch wichtiger als dieser, ist die Verringerung der laufenden Kosten K_{var}. Denn diese Kosten fallen bei jedem Verschlüsselungsvorgang an, wachsen also linear mit der Nachrichtenmenge. Bedeutsamer als diese Mengenkomponente ist der bisher noch außen vor gelassene Aspekt der Kostenrelevanz. Denn anders als einmalige Investitionskosten versinken die laufenden Kosten nicht bei getroffener Investitionsentscheidung, sondern bleiben permanent entscheidungsrelevant.

Wird die eingangs unterstellte Prämisse – die Übertragung einer einzigen Nachricht – zugunsten größerer Realitätsnähe aufgegeben, bedeutet das für den Anwender, daß er sich diesen Kosten beim Betrieb ständig gegenüber sieht und sie in Relation zum Nutzen setzen muß. Sinken also die Kosten K_{var} durch benutzerfreundliche Programme oder durch eine automatische Verschlüsselung im Hintergrund – wie bei Mobiltelefonen –, ist mit einem intensiveren Einsatz von Kryptographie zu rechnen, da das Kosten-Nutzen-Kalkül viel eher eine wirtschaftliche Nutzung verspricht. Folglich ist es möglich, schon Nachrichten zu verschlüsseln, deren Inhalte weniger schützenswert sind (geringere Opportunitätserlöse) als militärische Meldungen, also beispielsweise private Post, Telefonate oder normale Geschäftsvorgänge. Die Verbreitung günstiger Computertechnik könnte letzten Endes also dazu führen, daß auch die Kryptographie den privaten Konsumentenmarkt erreicht oder, wie es ein inzwischen weltweit benutztes Programm verspricht, „encryption for the masses“[17].

Um für diesen Massenmarkt geeignet zu sein, war jedoch noch eine weitere Hürde in Richtung Benutzerfreundlichkeit und einfache Anwendung zu nehmen – das Schlüsselmanagement. Im beschriebenen Standard-Modell benutzen sowohl Sender wie Empfänger den gleichen Schlüssel, um an den Nachrichteninhalt zu gelangen. Dies ist ein nur scheinbar einfacher, in der Praxis aber sehr umständlicher Weg, denn zwischen Sender und Empfänger muß eine Möglichkeit bestehen, den Schlüssel heimlich auszutauschen. Das bedeutet konkret, daß für die Schlüsselübergabe die gleichen Bedingungen einer sicheren Übermittlung gegeben sein müssen wie später für die Nachricht selbst. Wenn aber Sender und Empfänger vertraulich kommunizieren können, warum übermitteln sie auf diesem Weg nicht auch die Nachricht?

Schwerer noch wiegt ein weiteres Problem, das das bislang verwendete Sender-Empfänger-Modell nicht offenbart: mit jedem hinzu tretenden Kommunikationspartner muß ein zusätzlicher Schlüssel generiert und sicher verteilt werden. Der hierfür nötige Aufwand, ausgedrückt als Kosten K_s in Formel 3, treibt das System schon für wenige Nutzer an die Grenze der Handhabbarkeit.

Aus diesem Grund waren die Fragen des Schlüsselmanagements lange Zeit ein intensives Forschungsgebiet der Kryptologie, bis im Jahre 1976 die Wissenschaftler Diffie und Hellmann[18] eine ebenso einfache wie geniale Lösung fanden, welche auf

[17] Bekannt wurde dieser Slogan durch das Programm Pretty Good Privacy (PGP). Hierauf wird im Zusammenhang mit Standardisierungsproblemen noch in Kapital 5.1 auf Seite 25 einzugehen sein.
[18] Vgl. **Diffie/Hellman** (1976).

den ersten Blick nicht wie eine ernsthafte Verbesserung aussieht: Der vormals benutzte Universalschlüssel wird ersetzt durch ein Schlüsselpaar, das auf die Kommunikationspartner aufgeteilt wird. Der Empfänger behält seinen geheimen Teilschlüssel, wohingegen die zweite Schlüsselhälfte öffentlich an alle potentiellen Kommunikationspartner, bisher Sender genannt, verteilt wird.

Vom Prinzip her läuft eine Nachrichtenübertragung wie folgt ab: Eine Nachricht von einem der Sender wird mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und kann dann nur von ihm mit dem geheim gehaltenen Teilschlüssel entschlüsselt werden. Das oben benutzte Bild der abschließbaren Stahlkassette wandelt sich jetzt zu einem Briefkasten, der über zwei Schlösser verfügt – einem auf der Einwurf- wie auf der Entnahmeseite. Der Briefschreiber – der Sender – besitzt einen Schlüssel, den Einwurfschacht zu öffnen und den Brief – die Nachricht – in den Kasten zu werfen. Danach hat er keinen Zugriff mehr hierauf, nur noch der Inhaber des geheimen Schlüssels – der Empfänger – kann an den Inhalt des Briefkastens gelangen und die Nachricht entnehmen.

Diese scheinbar komplizierte Vorgehensweise erlaubt eine Antwort auf die gestellten Fragen. Ein vertraulicher Kanal zur Schlüsselübergabe ist nun nicht mehr erforderlich, denn die öffentliche Schlüsselhälfte muß, besser noch, soll nicht geheim gehalten werden. Außerdem sinkt die nötige Schlüsselzahl, wenn viele Personen sich verständigen wollen, da jeder neue Kommunikationspartner nur einen weiteren Schlüssel in die Runde – seinen „public key“ – einbringt, statt mit jedem Mitglied einen Universalschlüssel auszuhandeln und diesen dann sicher zu übermitteln.

Aus ökonomischer Sicht stellt sich diese Entwicklung folgendermaßen dar: Das alte Universalschlüsselprinzip war extrem transaktionskostenintensiv. Sowohl die Verwaltung der vielen Schlüssel als auch deren sichere Übertragung, abgebildet als Schlüsselmanagement in Formel 3, ließen die Kosten K_s dieser Technologie schnell mit der Nutzerzahl in die Höhe steigen. Wie schon bei den direkten Kosten K_{fix} und K_{var} sorgten auch diese Transaktionskosten als indirekte Verfahrenskosten dafür, daß Kryptographie für den privaten Anwender unwirtschaftlich war. Die Entwicklung von Verfahren der „public key“-Verschlüsselung hat dazu geführt, daß die Kosten für das Schlüsselmanagement nicht nur absolut stark gesunken sind, sondern außerdem bei Anwachsen der Nutzergruppe nur moderat steigen.

Die neue Technologie war nicht nur ein Durchbruch durch das vereinfachte Schlüsselmanagement, sie bereitete auch den Weg für völlig neue Einsatzfelder der Kryptographie. Im Universalschlüsselkonzept gab es keinen Schutz vor Verände-

rung der Nachricht durch einen legitimen Inhaber des Schlüssels – nämlich den Empfänger. Er kann mit dem Schlüssel sowohl ent- als auch verschlüsseln, folglich auch den Inhalt beliebig verändern, ohne daß dies beweisbar wäre. Rechtsverbindliche Dokumente waren in einer Welt der Universalschlüssel also ohne weitere Hilfsmittel nicht zu erstellen, Fälschungssicherheit gab es nicht. Dies änderte sich mit dem Zwei-Schlüssel-Konzept, da der Empfänger die Nachricht zwar lesen, der Inhalt von ihm jedoch nicht beeinflußt werden kann. Entwicklungen wie digitale Unterschriften oder E-Cash, wie sie Gegenstand des folgenden Kapitels sind, wären ohne „public key"-Verschlüsselung undenkbar.

4. Trends zur Verschlüsselung im „globalen Dorf"

Die veränderte Rolle der Kryptographie aus einer rein individualistisch geprägten Kosten-Nutzen-Relation heraus verstehen zu wollen, wäre jedoch zu kurz gegriffen. Denn Schritt für Schritt haben sich in den letzten Jahren die Bedingungen verändert, unter denen Kommunikation zwischen Menschen stattfindet. Diese Veränderungen lassen sich – soweit im Rahmen dieses Beitrags relevant – in den vier Hauptentwicklungslinien

- Deregulierung,
- Konvergenz,
- Globalisierung und
- Virtualisierung

zusammenfassen. Diese werde im Folgenden der Reihe nach erläutert.

4.1 Deregulierung

Waren in den 80er Jahren die Märkte für Telekommunikation noch in vielen Ländern in Hand staatlicher Monopolunternehmen, so hat sich diese Situation inzwischen stark gewandelt. Heutzutage sind weltweit alle wichtigen Fernmeldemärkte dereguliert. Die einstigen Staatsunternehmen mit ihrer mittlerweile vielfach privatisierten Eigentümerstruktur müssen sich dem Wettbewerb stellen. Der Eintritt neuer Konkurrenten in die geöffneten Märkte sorgte für einen Preisverfall bei den bisherigen Produkten und bei gleichzeitiger Ausweitung des Angebots, beispielsweise im Bereich mobiler Kommunikation. Durch die gewonnenen ökonomischen Freiheiten wuchs der Telekommunikationsmarkt mit überdurchschnittlichen Raten und bescherte den neuen Techniken eine nahezu ubiquitäre Verbreitung. Folge dieser ständigen Verfügbarkeit war die Veränderung von gesellschaftlichen Kommunikationsprozessen weg von persönlichen Kontakten.

Die neuen Dienste brachten für den Nutzer neben vielfältigen Möglichkeiten aber auch neue Probleme mit sich. Denn mit der Deregulierung hat in der Telekommunikation die Spezialierung und Arbeitsteilung zugenommen. Was aus volkswirtschaftlicher Sicht zu begrüßen ist, kann aber unter Sicherheitsaspekten von Nachteil sein, denn Informationen, die über mehrere Firmengrenzen gereicht werden, sind tendenziell gefährdeter als bei dem Transport durch einen einzigen Anbieter.

Von Seiten des Nachfragers ist damit immer weniger durchschaubar, wer seine Nachrichten in welcher Weise transportiert und wie sicher die Kommunikation ist. Durch die Öffnung des Marktes wird es für ihn immer aufwendiger, das Umfeld seiner Kommunikation – im Sinne des oben aufgezeigten Kalküls – zu kontrollieren.

4.2 Konvergenz

Der Begriff der Konvergenz bezeichnet das Zusammenwachsen ursprünglich getrennter Technologien oder Medien. Im Bereich der Technologien läßt sich dies beispielsweise an den immer vielfältiger werdenden Einsatzmöglichkeiten des Personal Computers verdeutlichen. Bei Markteinführung ursprünglich als reines Großrechnerterminal konzipiert, entwickelte sich der PC weiter zu einer eigenständigen Rechnerfamilie, wurde dann um Multimediafähigkeiten erweitert und wird mittelbis langfristig mit dem Fernseher und dem Fax fusionieren, welches wiederum mit dem Telefon und dem Anrufbeantworter zusammengewachsen ist. Möglich wurde diese Entwicklung nicht nur durch die Miniaturisierung elektronischer Bauteile und die damit steigende Leistung der PCs, sondern vor allem durch den fortschreitenden Einsatz von Mikroelektronik in fast allen Bereichen des täglichen Lebens. So finden sich heute Computerchips in den meisten Telefonen, Videorecordern und Fernsehern. Der Wunsch nach Vernetzung von seiten der Computeranwender und die Digitalisierung des Fernsehsystems – zur Übertragung von besseren und vor allem mehr Programmen – werden die letzten Hürden ebnen auf dem Weg zur Verschmelzung der beiden einstmals eigenständigen Systeme.

Ganz ähnlich ist der Grundgedanke der Konvergenz bezogen auf das Gebiet der Medien. Dort bezeichnet er die Annäherung der Individualkommunikation – der Kontakt zwischen Einzelpersonen – an die Massenmedien Presse, Radio und Fernsehen. Dieser Vorgang läßt sich am Beispiel des Internets veranschaulichen. Das „Netz der Netze“, gewachsen aus dem Zusammenschluß von vielen kleinen Teilnetzen und damit Ergebnis der technologischen Konvergenz im obigen Sinne, ermöglicht einen einfachen Nachrichtenaustausch zwischen verschiedenen Benutzern. Hier ist es ebenso einfach möglich, einer Einzelperson zu schreiben, wie mit einer ganzen

Gruppe zu diskutieren oder auf Knopfdruck eine Mitteilung Tausenden von Nutzern zugänglich zu machen. Daneben sind im Internet heute nahezu alle „klassischen“ Medien vertreten wie Presse, Radio und Fernsehen.

4.3 Globalisierung

Damit ist das Internet nicht nur für die Konvergenz, sondern auch für den Trend zur Globalisierung ein anschauliches Beispiel. Wird nämlich von anderen Aspekten der Globalisierung abgesehen, ist die weltweite Verfügbarkeit der Ware Information ein Trend, der nahezu untrennbar mit dem Begriff Internet oder „Datenautobahn“ verbunden ist.

Wie im genannten Fall der Massenmedien können heute Informationen rund um den Globus in Sekundenschnelle übertragen werden. Da es für den Nutzer keinen Unterschied macht, ob er ein Dokument aus Berlin oder Tokyo bezieht, wächst bei ihm die Illusion der räumlichen Nähe zu diesen Städten. Jede Internetseite ist nur einen Mausklick entfernt – unabhängig von der realen Distanz. Für diese Fiktion der Raumlosigkeit durch scheinbar nachbarschaftliche Nähe hat Marshall McLuhan den Begriff „globales Dorf“ geprägt.

4.4 Virtualisierung

Doch das Netz ist noch weit davon entfernt, ein Dorf zu sein. Denn dem normalen Verständnis der Wortes nach assoziiert man hiermit nicht nur Nähe – die gibt es in der Stadt auch –, sondern vor allem Überschaubarkeit und Vertrauenswürdigkeit, also nicht die Anonymität einer Großstadt. McLuhans Bild trifft daher – noch – nicht zu, aber es ist absehbar, daß sich dies ändern wird.

Der Überschaubarkeit ein Stück näher zu kommen, haben sich intelligente Navigationshilfen und Suchwerkzeuge zur Aufgabe gesetzt. Relevanter in diesem Zusammenhang sind aber die Bemühungen zur Sicherung der Vertrauenswürdigkeit im Netz, denn sie bedienen sich häufig kryptographischer Methoden. Unabdingbare Bestandteile von Vertrauenswürdigkeit sind Möglichkeiten, die sicherstellen, daß

- eine Person die ist, für die sie sich ausgibt (Identität),
- Dokumente – allgemein beliebige Daten – vor nicht beabsichtigter oder unbefugter Veränderung geschützt sind (Authentizität und Integrität),
- Personen kommunizieren können, ohne daß unberechtigte Dritte hierauf Zugriff haben (Schutz der Privatsphäre).

Diese drei Teilaspekte sind eng miteinander korreliert. Während bisher der Schutz der Privatsphäre im Zentrum der Diskussion gestanden hat, ist es nur ein

kleiner Schritt, mit der vorgestellten „public key“-Kryptographie auch die beiden Funktionen Identität und Authentizität abzudecken.

Wie dies geschehen kann, läßt sich beispielhaft am Verfahren der digitalen Unterschrift erläutern. Mit einer Unterschrift bestätigt der Zeichnende – und nur er – (Identität) die Echtheit und Richtigkeit des Textes (Authentizität). Das Dokument ist oberhalb der Signatur so wiedergeben, daß Streichungen, Änderungen und Hinzufügungen nicht möglich sind (Integrität).

Im Bereich der elektronischen Medien sichert eine Prüfsumme das materiell nicht greifbare Dokument vor Veränderungen jeglicher Art. Entscheidende Idee hierbei ist die Umkehr des oben beschriebenen Kommunikationsvorgangs: Der Sender verschlüsselt die Prüfsumme mit seinem privaten Schlüssel und fügt diese Digitale Unterschrift dem Klartext bei. Da aber der öffentlich verfügbare Schlüssel das Gegenstück zum geheimen Schlüssel darstellt, kann jeder Interessent die Gültigkeit der Unterschrift nachprüfen. Er ermittelt eine zweite Prüfsumme über den ihm vorliegenden Text und entschlüsselt mit dem „public key“ die übermittelte, erste Prüfsumme. Sind beide Zahlen gleich, ist der Text authentisch. Da nur der Sender in der Lage ist, eine korrekte Kennzahl zu erstellen, ist seine Unterschrift fälschungssicher und an nur dieses Dokument gebunden. Zu Beschreibung dieses Vorgangs wurde das Bild eines gläsernen Tresors gebraucht: Bei Leistung der Unterschrift wird das Dokument in einem durchsichtigen Tresor deponiert, zu dem nur der Eigentümer einen Schlüssel hat. Obwohl für alle sichtbar, konnte nur der berechtigte Schlüsselinhaber das Schriftstück einschließen.[19]

Die sich mit der digitalen Unterschrift bietenden Möglichkeiten sind vielfältig und werden den schon jetzt erkennbaren Trend zur Virtualisierung weiter vorantreiben. Viele Anwendungsgebiete liegen in den Bereichen des täglichen Lebens, die gegenwärtig noch die Übertragung papiergebundener Information voraussetzen. Hierzu zählen beispielsweise rechtsverbindliche Geschäfte wie Bestellungen, Überweisungen oder Bürgschaften. Möglich werden aber auch elektronisch gestellte Anträge bei Behörden, z.B. Steuererklärungen, ebenso notarielle Beglaubigungen – von Gesellschaftsverträgen bis zu Testamenten – wie fälschungssichere Ausweise – Reisepässe und Führerscheine.

Aus den vier angesprochenen Trends resultiert eine sich in Zukunft stark wandelnde Rolle der Kryptographie in der Gesellschaft. Global werden immer mehr Daten in elektronischer Weise bearbeitet und Kommunikationskanäle, die vorher von-

[19] Vgl. **Beutelspacher/Schwenk/Wolfenstetter** (1995), S. 17.

einander getrennt verliefen, in wettbewerbsbedingt offenen Märkten zusammenwachsen. Hieraus resultiert aus Nutzersicht ein vermehrtes Bedürfnis nach Vertraulichkeit und Sicherheit der übermittelten Daten. Obwohl es durch die reine Flut der übertragenen Daten und durch benutzerfreundliche Technik tendenziell leichter wird, mit Hilfe steganographischer Verfahren Nachrichten in anderen Daten zu verstecken, wird nach jetzigem Kenntnisstand nur die Verschlüsselungstechnik diesem steigenden Bedarf an Schutz vertraulicher Daten gerecht werden können. Auf dem Weg zur Informationsgesellschaft kommt der Kryptographie daher eine Schlüsselrolle zu.

5. Wirtschaftspolitische Aspekte der Kryptographie

Nachdem in Kapitel 3 auf technologische Besonderheiten der Kryptographie und in Kapitel 4 auf generelle Entwicklungstrends im Bereich der Kommunikation eingegangen wurde, steht nun das theoretische Wissen bereit zu untersuchen, ob es bei Produktion oder Anwendung des Gutes Kryptographie zu Fällen des Marktversagens kommen kann.

Um die Argumentation zunächst auf eine rein ökonomische Ebene zu beschränken, wird davon ausgegangen, daß durch eine hinreichend große Anbieterzahl ein funktionsfähiger Wettbewerb für „black boxes“ existiert, d.h. neben anderen Bedingungen vor allem das Fehlen künstlicher Marktein- und -austrittsbarrieren. Nachdem auf die Probleme dieses idealtypischen Marktes eingegangen wurde, sollen die getroffenen Prämissen im Laufe des Abschnitts 5.4 zugunsten einer realitätsnäheren Betrachtung gelockert werden.

5.1 Standardisierung als Koordinationsproblem

Eine Kommunikation zwischen Sender und Empfänger kann nur stattfinden, wenn beide die gleiche Sprache sprechen, was oben als geteilte Codebasis bezeichnet wurde. Der Schutz der Verschlüsselungstechnik vor unerwünschten Dritten kann für den Sender einer Nachricht auch eine unangenehme Komponente haben: Nicht nur alle Eindringlinge, sondern auch der beabsichtigte Empfänger wird ausgeschlossen. Dieser Fall tritt insbesondere dann ein, wenn sich beide Seiten vor der Nachrichtenübermittlung nicht auf das verwendete Verfahren geeinigt haben, die trennende Schnittstelle also nicht hinreichend standardisiert ist.

Die für einen Standard notwendige Übereinkunft stellt aber eine Vorleistung in eine sichere Kommunikation dar, wie alle bisher im Faktor K_{fix}[20] zusammengefaßten Komponenten. Ebenso wie die Investition in spezifische Hardware ist sie eine fixe Kostengröße, die vollständig mit Aufnahme der Kommunikation versunken ist. Analog der obigen Argumentation werden hohe Verhandlungskosten in Gestalt von Transaktionskosten den Faktor K_{fix} wachsen lassen, was die Kosten-Nutzen-Relation eines Anwenders verschlechtert. Im Extremfall ist denkbar, daß zwar Kryptographie kostenlos verfügbar ist; trotzdem unterbleibt die Verschlüsselung der Kommunikation, da die Koordination zwischen den Partnern unter Wirtschaftlichkeitsaspekten zu teuer ist.

Aus Sicht jedes einzelnen ist die Standardisierung der Kommunikationsschnittstelle eine spezifische Investition in die angestrebte Nachrichtenübertragung zum jeweiligen Partner. Im Fall des einfachen Sender-Empfänger-Modells ist der Öffentlichkeitsgrad dieser Investition 50 Prozent – jeder Verhandlungspartner kann mindestens zu gleichen Teilen vom Vereinheitlichungserfolg profitieren.

Dieser Öffentlichkeitsgrad nimmt stark mit der Zahl der potentiellen Kommunikationspartner zu, weshalb der persönliche Anreiz jedes einzelnen drastisch sinkt, seinen Standard durchzusetzen. Bei beliebig vielen Anwendern ist der Nutzen, der auf jeden entfällt, nahe Null, während die Koordinationskosten K_{fix} nach wie vor voll anfallen und mit steigender Partnerzahl sogar überproportional anwachsen. Durch die einzelwirtschaftlich immer weiter auseinander klaffende Kosten-Nutzen-Relation wird die Standardisierung der Verschlüsselungstechnik zu einem vollständig öffentlichen Gut, das primär von niemandem bereitgestellt wird. Lösungsmöglichkeiten für dieses Standardisierungsproblem – insbesondere die Bereitstellung von Standards als Kollektivgut – sind in der Ökonomie in hinreichender Zahl entwickelt und analysiert.[21]

Interessanter an dieser Stelle ist deshalb nicht die Frage, ob sich theoretisch ein Marktversagen einstellen kann, sondern die Erkenntnis, daß dies real nicht der Fall ist. Gegenwärtig existiert nämlich ein einheitlicher Standard in Form des weltweit millionenfach eingesetzten Programms PGP (Pretty Good Privacy). Die genannten Koordinationsprobleme wurden dadurch überwunden, daß der Autor, Phil Zimmermann, seine Software zur asymmetrischen Verschlüsselung möglichen Nutzern kostenlos zur Verfügung stellte. Da es zum Zeitpunkt der Veröffentlichung im Jahre

[20] Vgl. Kapitel 3, S. 17.

1991 kein frei verfügbares „public-key"-Programm im Internet gab, verbreitete sich PGP innerhalb eines Monats über den ganzen Erdball und überwand damit in kürzester Zeit die zur Durchsetzung eines Standards notwendige kritische Masse.

5.2 Marktversagen durch asymmetrische Information

In der bisherigen Argumentation hatten sowohl Sender wie auch Empfänger die Verschlüsselungstechnik nachgefragt, d.h. sie traten als Käufer auf den Markt für Kryptographie. Anders als bei den meisten Gütern können diese Käufer aber die Qualität der Ware nur schwer beurteilen: vor dem Kauf gar nicht und beim Einsatz auch nur sehr eingeschränkt. Denn die Güte eines Verschlüsselungsalgorithmus, soweit überhaupt veröffentlicht, kann nur von Kryptoanalytikern beurteilt werden; seine Implementierung als Software ist selbst für Informatiker extrem mühsam, wenn nicht gänzlich unmöglich, da der Algorithmus als Quelltext – in für Menschen lesbarer Form – nicht zu Verfügung steht.

Als Folge hiervon erwirbt der Käufer ein Vertrauensgut im Sinne von Darby und Karni, über dessen Qualität nahezu vollständige Unklarheit herrscht.[22] Aus der ökonomischen Theorie ist bekannt, daß Märkte mit stark asymmetrischer Informationsverteilung zwischen Verkäufer und Käufer dazu tendieren, daß sich die schlechtere Qualität durchsetzt. Denn ein potentieller Nachfrager ist nicht in der Lage, gute Qualität zu erkennen, und folglich nicht bereit, hierfür entsprechend zu zahlen. Durch die fehlende Zahlungsbereitschaft scheiden Produzenten hochwertiger Produkte aus dem Markt aus oder fertigen nur noch qualitativ schlechtere Ware. Langfristig pendelt sich der Markt auf einem niedrigen Qualitätsniveau ein.

Für das Verhandensein eines deutlichen Informationsvorsprungs zugunsten des Verkäufers gibt es auf dem Markt für Kryptographie starke Anzeichen. So gelang es in den 80er und 90er Jahren dem deutschen Bundesnachrichtendienst (BND) über Verbindungen zur Schweizer Firma Crypto AG, sowohl Libyen und als auch dem Iran Verschlüsselungssysteme zu verkaufen, die aufgrund ihrer minderen Qualität in der Ökonomie als „Zitronen" bezeichnet worden wären. Im genannten Fall boten die Systeme deutlich weniger Sicherheit als es den Auftraggebern lieb sein konnte, denn die Architektur der Maschinen ließ kundigen Dritten eine Hintertür offen. Folglich war jegliche Korrespondenz, die mit Hilfe der neu erworbenen Maschinen verschlüsselt wurde, von Deutschland aus mitzulesen, was wahrscheinlich auch

[21] Vgl **Thum** (1994), S. 467 ff.

[22] Vgl. **Darby/Karni** (1973), S. 68.

geschah.[23]

Ansatzmöglichkeiten, den Fällen der adversen Selektion zu begegnen, sind in der Ökonomie vielfältig bekannt[24], weshalb an dieser Stelle nur auf eine Lösungsvariante eingegangen werden soll. Um einer symmetrischen Verteilung der Information zwischen Anbieter und Nachfrager näher zu kommen, kann die besser informierte Seite – meist der Anbieter – der anderen Marktseite Informationen zur Verfügung stellen.

In diesem Zusammenhang wird deutlich, warum das Programm PGP seinen inzwischen legendären Ruf erwerben konnte. Denn einen großen Anwenderkreis brachte der Software neben der kostenlosen Nutzung vor allem eine Besonderheit: ihre zweifelsfrei nachprüfbare Sicherheit. Jeder Nutzer kann die frei erhältlichen Quellcodes des Programms einsehen und auf Fehler und Hintertüren überprüfen. Wichtiger noch: Er kann darauf vertrauen, daß die im Internet aktiven Kryptologen die Software gründlich analysieren und jede Ungereimtheit unverzüglich publizieren. Wenn PGP Sicherheitslücken hätte, wären diese in den sechs Jahren seines Bestehens aufgedeckt worden. Statt dessen schützt das Programm in seinem weltweiten Einsatz sogar Daten, die über Leben und Tod von Menschen entscheiden, wie zum Beispiele bei amnesty international, der Untergrundbewegung von Burma oder der Exilregierung von Tibet.[25]

5.3 Externe Effekte der Nutzung

Bisher war unterstellt worden, daß es sich bei Produkten zur Sicherung der Privatsphäre um normale Güter handelt. Dies ist jedoch de facto nicht so, denn beispielsweise unterliegt der Export von Kryptographie aus den Vereinigten Staaten der Ausfuhrkontrolle, der US Export Administration Regulation. Mit einiger Verspätung hat die dort schon seit Jahren anhaltende „Krypto“-Debatte auch die Bundesrepublik erreicht. Daß aus politischen Kreisen der Ruf nach Regulierung dieser Technologie – meist unter Bezug auf die innere und äußere Sicherheit – laut wird, läßt sich mit den bislang angeführten Argumenten des Marktversagens nicht erklären.

Aus ordnungspolitischer Sicht kann sowohl die staatliche Bereitstellung wie auch Produktion des Gutes „Sicherheit“ – innere wie äußere – im Rahmen der Kollektivguttheorie gerechtfertigt werden. In diesem Sinne verfügt das Gut über die beiden Eigenschaften der Nicht-Rivalität im Konsum und der Nicht-Exkludierbarkeit von Zahlungsunwilligen, ist damit also ein Kollektivgut in Reinform. Aufgrund von

[23] Vgl. **Koch/Sperber** (1995), S. 283 ff.
[24] Vgl. **Fritsch/Wein/Ewers** (1996), S. 219 ff.
[25] Vgl. **Savall** (1996).

Trittbrettfahrerverhalten kommt ein privater Markt zur Bereitstellung dieses Gutes nicht zustande und die private Herstellung wird aufgrund der Höhe der erwarteten Gefährdungskosten – beispielsweise durch rivalisierende private Polizeitruppen oder Armeen – erst gar nicht in Erwägung gezogen.[26]

Damit bleibt der Staat in der Pflicht, für innere und äußere Sicherheit zu sorgen. Zur Erfüllung dieser Aufgabe werden traditionell Eingriffe in die Privatsphäre hingenommen, allerdings unter sehr restriktiven Bedingungen. So bedarf es der richterlichen Genehmigung zur Verletzung von Brief- oder Fernmeldegeheimnis, welche nur bei schweren Straftaten erteilt wird. Doch der politisch erreichte und vielleicht auch gesellschaftlich akzeptierte Kompromiß zwischen dem Schutz der Individualrechte auf der einen Seite und der Wahrung von öffentlicher Sicherheit auf der anderen droht angesichts der beschriebenen wissenschaftlichen und technischen Veränderungen im Bereich der Verschlüsselungstechnik zu Lasten der letzteren zu kippen.

Denn natürlich schützen kryptographische Systeme den Nachrichteninhalt ohne Ansehen der Person, womit die Kommunikation von Verbrechern genauso sicher ist wie die unbescholtener Bürger. Sollten sich die oben diskutierten Trends hin zu einem verstärkten Einsatz von Kryptographie bewahrheiten, ist damit zu rechnen, daß die genannten staatlichen Ermittlungsmaßnahmen in den kommenden Jahren an Wirksamkeit einbüßen. Polizeiliches Abhören mit richterlicher Genehmigung wäre also in einer Gesellschaft, in der die gesamte Kommunikation elektronisch und verschlüsselt abläuft, reine Zeitverschwendung, da es auch für den Staat keinen Weg gibt, die verwendeten Codes zu brechen. Auf der anderen Seite wären die Daten normaler Nutzer erheblich besser geschützt als heute, was Straftaten von Dokumentenfälschung über Betrug bis hin zur Industriespionage erheblich erschweren dürfte.[27] Einer möglicherweise erschwerten Strafverfolgung stünde damit ein Vereitelungseffekt bei bestimmten Straftaten gegenüber.

Da der resultierende Nettoeffekt in den seltensten Fällen gleich null sein dürfte, kann sich hier ein Fall von Marktversagen einstellen: Der Einsatz von kryptographischen Produkten kann mit negativen externen Effekten auf das übergeordnete Ziel der inneren und äußeren Sicherheit als staatlich bereitgestelltes Kollektivgut verbunden sein. Möglichkeiten für ein staatliches Eingreifen in den Markt sind in den vergangenen Jahren vielfältig diskutiert worden, wobei die erwogenen

[26] Vgl. **Grossekettler** (1993), S. 18.

[27] Die Rolle dieser Schäden war Gegenstand des mikroökonomischen Nutzenkalküls in Kapitel 3.

politischen Maßnahmen von Pflichten zur Hinterlegung von Nachschlüsseln über Exportbeschränkungen bis hin zu generellen Einsatzverboten reichen.

Aus wissenschaftlicher Sicht kann ein Tätigwerden des Staates aufgrund negativer Externalitäten nur dann gerechtfertigt werden, wenn es gelingt, auf folgende Fragen eine befriedigende Antwort zu finden:

a) Legitimierung des Regulierungsziels: Bislang war das Oberziel innere Sicherheit als gegeben unterstellt worden. Doch wie wird der Stellenwert dieses Ziels beispielsweise in einer fiktiven, Rawlsschen Urvertragssituation beurteilt, wenn es in Konflikt mit einem anderen Oberziel treten kann, wie in diesem Fall der individuellen Freiheit? Die in Deutschland lange geführte Diskussion um die Einführung staatlicher Überwachungsmaßnahmen im Rahmen des Lauschangriffs zeigt, daß es hierauf keine eindeutige, intersubjektiv gültige Antwort gibt. Da der Zielkonflikt nicht aufgelöst werden kann, muß jede politische Maßnahme beiden als wichtig erkannten Zielen Rechnung tragen.

b) Relevanz des Problems im Lichte dieses Ziels: Haben die eingeschränkten staatlichen Ermittlungsmöglichkeiten wirklich eine negative Konsequenz für das erreichte Sicherheitsniveau?

   Im konkreten Fall ist zu beantworten, wie wichtig die Überwachung der Individualkommunikation für die Verbrechensbekämpfung real ist. Spielt beispielsweise die Telefonüberwachung, wie in den USA, nur eine untergeordnete Rolle, sind voraussichtlich eingeschränkte Ermittlungsmöglichkeiten wenig problematisch.

c) Effektivität der Regulierung: Bewirkt das staatliche Eingreifen eine Verbesserung im Sinne einer Annäherung an das Ziel?

   Hat beispielsweise eine staatlich verhängte Pflicht zur Hinterlegung eines Nachschlüssels bei einem Treuhänder im Rahmen der privaten Nutzung von Kryptographie eine nennenswerte Wirkung auf das als schützenswert erkannte Sicherheitsziel?

   In den vergangen Jahren ist von verschiedenen Seiten argumentiert worden, daß die Bedingung der Effektivität nicht erfüllt ist, da es für Verbrecher genug Mittel gibt, die staatlichen Maßnahmen zu umgehen und jegliche Korrespondenz geschützt ablaufen zu lassen. Die hierbei denkbaren Wege sind vielfältig. Verbrecher könnten eine mit illegalem Verfahren verschlüsselte Nachricht mit einem legalen Algorithmus

„überschlüsseln“ oder diese mit Hilfe der Steganographie verstecken. Außerdem ist eher zweifelhaft, ob sich bei schweren Straftaten der Einsatz von legalen Algorithmen auf dem Gesetzeswege erzwingen läßt.[28] Die Regulierung trifft damit nur den gesetzestreuen Bürger.

d) Effizienz der Regulierung: Gibt es Mittel, die kostengünstiger wirken oder weniger in die Rechte von Individuen eingreifen als die Regulierung? Wenn es möglich ist, durch andere, billigere Maßnahmen die weggefallenen Möglichkeiten zu kompensieren, ist die Regulierung des Marktes für kryptographische Produkte kaum zu rechtfertigen.

Der Frage, wie eine Schüsselhinterlegung bei einem Treuhänder ökonomisch zu beurteilen ist, sind amerikanische Kryptographie-Experten nachgegangen. Ihrer Meinung nach wäre ein staatliches System zur Erlangung von Nachschlüsseln nicht nur jenseits der gegenwärtigen Möglichkeiten und Erfahrungen in diesem Bereich, sondern vor allem komplizierter, teurer und unsicherer als jedes vergleichbare System ohne Schlüsselhinterlegung.[29] Damit gibt es zumindest deutliche Hinweise, die das politische Regulierungsinstrument der Schlüsselhinterlegung als ineffizient kennzeichnen.

Als Fazit bleibt festzuhalten, daß es von wissenschaftlicher Seite zumindest erhebliche Zweifel an der Effektivität und Effizienz eines staatlichen Eingreifens in den Markt für kryptographische Produkte gibt. Wenn aber die Regulierung keine Wirksamkeit zeigt, ist der Eingriff in die Rechte der betroffene Bürger unverhältnismäßig und damit verfassungswidrig.[30]

5.4 Der Staat als Akteur

Erschwerend kommt noch hinzu, daß gerade der Staat keine neutrale Position einnimmt, wenn es darum geht, die externen Effekte der Kryptographie auf übergeordnete gesellschaftliche Ziele zu beurteilen. Denn obwohl er in seiner Gesamtheit als Hüter der inneren und äußeren Sicherheit auftritt, verfolgen seine Repräsentanten im allgemeinen – auch – eigene Zwecke mit ihren politischen Handlungen. Dieses Eigeninteresse zusammen mit einem erheblichen Spielraum bei der Beurteilung des potentiellen Ausmaßes der erwarteten Gefährdung hat zu Beginn der 90er Jahre in

[28] Vgl. **Lorenz-Meyer** (1997).
[29] Vgl. **Abelson et al**. (1997).
[30] Vgl. **Bizer et al**. (1997).

den USA zu einer lang anhaltenden, sehr hitzig geführten Diskussion geführt.[31] Den auf Regierungsseite beschworenen Szenarien der Ohnmacht des Staates bei der Terrorismusbekämpfung – damit dem Zusammenbruch jeglicher Sicherheit – standen auf der Seite von Bürgerrechtlern und liberalen Wissenschaftlern nicht weniger bedrohliche Bilder eines Überwachungsstaates Orwellschen Ausmaßes gegenüber.[32]

Auf Deutschland hat diese Diskussion übergegriffen, als im Dezember 1996 bekannt wurde, daß im Bundesinnenministerium Vorbereitungen getroffen werden, den Einsatz von Kryptographie generell unter Genehmigungsvorbehalt zu stellen.[33] Wie in den USA ist das Ziel die innere Sicherheit – hier die Bekämpfung der Organisierten Kriminalität. Schon vor Verabschiedung des neuen Digitalen Signaturgesetzes war absehbar, daß Innenminister Kanther nicht nur auf Seiten der Opposition, sondern auch in der Koalition mit seinem Vorhaben auf Widerstand stoßen würde. Nachdem das Gesetz auch den Bundesrat am 4. Juli 1997 passiert hatte, war klar, daß deutsche Pläne zur Genehmigungspflicht für Kryptoprodukte vorläufig vom Tisch waren.[34] Doch auch in Zukunft wird die von Bundesinnen- und Wirtschaftsministerium gebildete Taskforce „Kryptopolitik“ einen schwierigen Spagat zu absolvieren haben.

Denn kryptographische Produkte sind nicht nur eine potentielle Gefahr für die innere Sicherheit, sondern stellen mittlerweile auch einen bedeutenden Wirtschafts- und Standortfaktor dar. Das mußten auf schmerzhafte Weise die Vereinigten Staaten nach ihrem Exportverbot sicherer Software erfahren – sehr zur Freude von Softwarehäusern außerhalb der USA. Aufgrund grundsatzpolitischer Überlegungen, aber nicht zuletzt aus Standortinteresse verfolgt die Europäische Union seit jüngstem eine Politik des freien Wettbewerbs im Bereich der Kryptographieprodukte. Als Antwort auf die amerikanische Politik wird eine Regulierung im Bereich der Kryptographie als hinderlich für den freien Fluß von Informationen und Diensten im gemeinsamen Markt empfunden.[35]

---

[31] Einen aktuellen Überblick über die rechtliche Situation der Kryptographie weltweit bietet **Möller** (1997).

[32] Die in der Diskussion benutzten Vergleiche reichten von „the first holy war of the information highway“ bis „the Bosnia of telecommunication“. **Levy** (1995), S. 266, 277.

[33] Vgl. **o.V**. (1996), S. 7.

[34] Vgl. **Schulzki-Haddouti** (1997), S. 1.

[35] Vgl. **EU-Kommission** (1997), S. 17.

6. Ausblick

Ökonomische Ansätze im Bereich der kryptologischen Forschung sind bis zum heutigen Tage nur vereinzelt zu finden. In der bisherigen Analyse hat sich gezeigt, daß nur die Möglichkeit real auftretender negativer Externalitäten einen Grund liefern könnten, den Einsatz von Kryptographie nicht dem Markt zu überlassen. Die in der politischen Diskussion vorgeschlagenen Regulierungsinstrumente überzeugen aber keineswegs beim Versuch, der Gefährdung der inneren Sicherheit wirksam zu begegnen. Sollten sich aber objektive Anzeichen für ein Stumpfwerden staatlicher Überwachungsmaßnahmen im Kampf gegen Verbrechen und Terrorismus zeigen, ist die ökonomische Forschung gefordert, dem Gesetzgeber bessere Instrumente an die Hand zu geben.

Danksagung

Für die freundliche Unterstützung bei der Entwicklung dieses Diskussionspapiers und beim Kampf gegen fast allgegenwärtige Tippfehler danke ich Brigitte Nussbaum, Caroline Pellmann, Carsten Rolle, Henning Tegner und Bea Schallenberg.

Hinweise auf verbliebene Fehler und Unzulänglichkeiten sind sehr willkommen. Diesbezügliche Anmerkungen und Verbesserungsvorschläge können unter folgender Adresse gemacht werden.

Institut für Verkehrswissenschaft
c/o Guido Schröder
Am Stadtgraben 9
48143 Münster

Telefon 0251- 83-2 28 18
Telefax 0251- 83-2 83 95
E-Mail: 10gusc@wiwi.uni-muenster.de

Literaturverzeichnis

Abelson et al. (1997): „The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption“, Final Report 27.5.1997, http://www.crypto.com/key_study/report.shtml.

Beutelspacher, Albrecht (1996): „Kryptologie“, Braunschweig/Wiesbaden.

Beutelspacher, Albrecht/Schwenk, Jörg/Wolfenstetter, Klaus-Dieter (1995): „Moderne Verfahren der Krytpographie – Von RSA zu Zero-Knowledge“, Braunschweig/Wiesbaden.

Bizer, Johann et al. (1997): „Kryptoregulierung ist verfassungswidrig“, Stellungnahme Bizer/Mertes u.a. vom 13.1.1997, http://www.telesec.de/kryptreg.htm.

Darby, Michael R./Karni, Edi (1973): „Free Competition and the Optimal Amount of Fraud“, in: The Journal of Law and Economics 16, S. 67-88.

Diffie, Witfield/Hellman, Martin E. (1976): „New directions in cryptography“ in: IEEE Transactions on Information Theory, Vol. IT-22, No. 6, S. 644-654.

Drosnin, Michael (1997): „Der Bibel Code“, München.

EU-Kommission (1997): „Sicherheit und Vertrauen in elektronische Kommunikation“, Ein europäischer Rahmen für Digitale Signaturen und Verschlüsselung, COM (97) 503 DE, angenommen von der Kommission am 8.10.1997, http://www.ispo.cec.be/eif/policy/.

Fritsch, Michael/Wein, Thomas/Ewers, Hans-Jürgen (1996): „Marktversagen und Wirtschaftspolitik“, München.

Grossekettler, Heinz (1993): „Privatisierung, Deregulierung und Entbürokratisierung – Zeichen des Zeitgeistes oder ordnungpolitische Daueraufgabe“, in: Wissenschaftliche Gesellschaft für Marketing und Unternehmensführung, Arbeitspapier 80, Münster.

Kahn, David (1967): „The Codebreakers - The Story of Secret Writing“, New York.

Koch, Egmont R./Sperber, Jochen (1995): „Die Datenmafia – Computerspionage und neue Informationskartelle“, Hamburg.

Levy, Steven (1994): „The Cypherpunks vs. Uncle Sam“ in: Hoffman, Lance J. (Hrsg.) (1994): „Building in Big Brother – The Cryptographic Policy Debate“, New York et. al.

Lorenz-Meyer, Lorenz (1997): „Das Kreuz mit der Kryptographie“, Spiegel Online Archiv-Dokument 3/1997, http://www.spiegel.de/special/heft2/krypto.html.

Möller, Ulf (1997): „Kryptographie: Rechtliche Situation, politische Diskussion“, http://www.fitug.de/ulf/krypto/verbot.html.

o.V. (1996): „Bonn will neue Medien nicht blockieren – CDU fordert <Kryptogesetz> für verschlüsselte Daten“, in: Handelsblatt vom 3.12.1996, S. 7.

Savall, Achim (1997): „Verschlüsseln rettet Menschen“, in: Computer@Co, Beilage der Süddeutschen Zeitung, Dezember 1996, http://www.computer-co.de.

Schulzki-Haddouti, Christiane (1997): „Entspannung in Sachen Kryptographie – Verschlüsselungsverfahren: Innenministerium präsentiert Kompromiß - Freiwillige Zertifizierung beim Bundesamt für Sicherheit“, in: VDI-Nachrichten vom 27.6.97, S. 1.

Thum, Marcel (1994): „Möglichkeiten und Grenzen staatlicher Standardisierung“, in: Ökonomik der Standardisierung, Tietzel, Manfred (Hrsg.), Homo Oeconomicus, Band XI (3), S. 465-499.

Weitere Diskussionspapiere

1. Hans-Jürgen Ewers (1991): Freiheit und Effizienz – Variationen zu einem altem Thema
2. Hans-Jürgen Ewers / Klaus Rennings (1991): Die monetären Schäden eines Super-GAU´s in Biblis
3. Andreas Brenck (1991): Moderne umweltpolitische Konzepte: Sustainable Development und ökologisch-soziale Marktwirtschaft
4. Henning Tegner / Detlev Grewing (1995): Umweltchemikalienhaftung und Risikostandards
5. Carsten Lehmann / Hansjörg Rodi (1997): ÖPNV in der Marktwirtschaft – Ein Ordnungsentwurf mit kritischer Würdigung der jüngsten Reformen

Ältere Diskussionspapiere können beim Institut bestellt werden, aktuellere Veröffentlichungen stehen im Internet zum Download bereit.

Institut für Verkehrswissenschaft
Am Stadtgraben 9
48143 Münster

Telefon 0251- 83-2 29 90
Telefax 0251 - 83-2 83 95
Internet www-wiwi.uni-muenster.de/
~10/index.htm