



aktuell  
terminal

suchmaschine

subscribe

forum

impressum



## Bei der Kryptographie geht es um die Zukunft von Freiheit und Demokratie

Artur P. Schmidt 23.12.1997

Wir stehen heute wie bei der französischen Revolution vor der Herausforderung einer demokratischen Erneuerung, allerdings mit dem Unterschied, daß hier keine Köpfe rollen, sondern gewaltfreie Algorithmen, die das Recht auf Freiheit einfordern.

**Kryptographie, die Fähigkeit zum Verschlüsseln ('Encryption') und Entschlüsseln ('Decryption') von Daten, ist eine Strategie zur Vereinfachung komplexer Systeme und gibt demjenigen, der über diese Fähigkeit verfügt, ein Machtinstrument in die Hand. Die entscheidenden Merkmale verschlüsselter Daten sind hierbei Identifizierbarkeit, Echtheit, Akzeptanz, Überprüfung und Privatheit.**

download

Wer Menschen die Freiheit raubt, raubt diesen die Würde.

Wer Menschen die Würde nimmt, nimmt diesen das Leben.

### Kryptographie

Die Kryptographie gibt es schon seit Tausenden von Jahren. Insbesondere im militärischen Bereich wurde versucht, die geheimen Nachrichten, die von Boten überbracht werden sollten, unsichtbar zu machen bzw. geschickt zu verstecken. Im Zweiten Weltkrieg arbeiteten die Nationalsozialisten mit dem sogenannten ENIGMA-Code, um geheime Kommandobefehle zu verschlüsseln. Spätestens seit dessen Entschlüsselung durch Turing im 2. Weltkrieg, ist die Kryptographie im wahrsten Sinne des Wortes zu einer Schlüsseltechnologie avanciert.

Bei der heute üblichen asymmetrischen Kryptographie (public key cryptography) werden Schlüsselpaare für die Codierung verwendet, was den Vorteil hat, daß Nachrichten nicht mehr mit demselben Code ver- und entschlüsselt werden müssen. Eine verschlüsselte Nachricht wird "Ciphertext", eine entschlüsselte "Plaintext" genannt. Man unterscheidet dabei den öffentlichen Schlüssel ('public key'), der verwendet wird, um eine Nachricht zu verschlüsseln, und den privaten Schlüssel ('private key'), der zur Decodierung der verschlüsselten Nachricht verwendet wird und erlaubt, eine elektronische Unterschrift hinzuzufügen.

Programme wie das mittlerweile weit verbreitete PGP ('Pretty good Privacy') arbeiten nach diesem Prinzip: Wer eine vertrauliche Botschaft versenden will, erzeugt mit dem öffentlichen Schlüssel des Empfängers eine unlesbare Nachricht, die nur dieser - mit seinem geheimen Schlüssel - dechiffrieren kann. Eine fälschungssichere Signatur erzeugt der Absender wiederum mit seinem eigenen geheimen Schlüssel, wobei der Empfänger die Echtheit des Dokuments mit dem öffentlichen Schlüssel des Absenders überprüfen kann. Sowohl Sender als auch Empfänger müssen also die öffentlichen Schlüssel des jeweils anderen kennen, aber sie dürfen ihre geheimen Schlüssel nicht aus der Hand geben.

### **Online-Krieg gegen freie Bürger**

Die Diskussion um die Ver- und Entschlüsselung von Daten ist eigentlich unnötig, da das Grundgesetz in Artikel 10 Absatz 1 festlegt, daß das Brief-, Post- und Fernmeldegeheimnis unverletzlich ist. Wer Menschen abhört tastet deren Würde an und behindert die freie Entfaltung der Persönlichkeit, wobei gegen Artikel 1 und 2 des Grundgesetzes verstoßen wird. Auch wird bei einem Verschlüsselungsverbot gegen den Artikel 13 verstoßen, da die Teilnehmer der Möglichkeit beraubt werden, die Unverletzlichkeit ihrer Cyber-Wohnungen sicherzustellen.

Die Vorbereitung des Verschlüsselungsverbots verstößt auch gegen das Verbot der Führung eines Angriffskrieges (Artikel 26), denn die Einschränkung dieses Grundrechts ist nichts anderes als ein staatlich vorbereiteter Online-Krieg gegen freie Bürger. Darüber hinaus konterkariert ein staatliches Monopol über Verschlüsselungssoftware Artikel 20 des Grundgesetzes, wonach alle Staatsgewalt vom Volke auszugehen hat.

Absatz 4 dieses Artikels ermutigt uns sogar zum Widerstand gegen ein Verbot der Verschlüsselung, da es jedem Staatsbürger das Recht einräumt, Widerstand gegen diejenigen zu leisten, die versuchen die demokratische Grundordnung zu beseitigen. Verwirken Regierende nach Artikel 18 des Grundgesetzes nicht sogar ihre Grundrechte, wenn diese das Brief-, Post- und Fernmeldegeheimnis einschränken? Wir werden nicht umhin

kommen, dies früher oder später vom Verfassungsgericht prüfen zu lassen.

### **Virtueller versus freier Himmel**

Mit dem Aufkommen von Cyber-Welten stehen sich zwei Mächte gegenüber. Die eine fordert den "gläsernen Bürger", die andere steht für Datenschutz und Freiheit der Teilnehmer. Entscheidend für den Ausgang dieses Machtkampfes wird die Kryptographie sein.

Die Freiheit des Internet ängstigt die herrschende Klasse, da diese ihre Machtposition gefährdet sieht. Um dem Aufbau einer Gegenmacht vorzubeugen, soll deshalb die unkontrollierbare Versammlung von Teilnehmern im Cyberspace verhindert werden. Die Versammlungsfreiheit darf jedoch nach Artikel 8 des Grundgesetzes nicht eingeschränkt werden, da der Himmel im Internet nicht frei ist, sondern virtuell konstruiert (laut Grundgesetz kann die Versammlungsfreiheit nur unter freiem Himmel eingeschränkt werden). Entscheidend wird deshalb sein, daß wir den Teilnehmern und ihren Versammlungen in den Netzen das Versammlungsrecht uneingeschränkt einräumen und daß wir es diesen selbst überlassen, wie sich diese schützen.

Genau die Personen, die dafür Verantwortung tragen, daß wir in Deutschland eine ausufernde Bürokratie haben und uns durch Verordnungen und Reformunfähigkeit selbst blockieren, fordern jetzt lautstark ein staatliches Monopol über die Kryptographie. Die Ausrede heißt: Der Staat muß seine Bürger schützen. Doch wer muß eigentlich vor wem geschützt werden? In Wahrheit muß der Bürger vor dem Staat geschützt werden, wenn der Staat dem Bürger das Recht auf Verschlüsselung verweigert.

Der Versuch einer Überwachung der Verschlüsselung, die sowieso nicht funktioniert, würde zu einer riesigen Bürokratie und unzähligen Verordnungen führen. Die Kosten einer solchen 'Big Brother'-Organisation würden mit Sicherheit Milliardenhöhe erreichen, weshalb das Geld sinnvollerweise in die kostenlose Verteilung von Wissen investiert werden sollte.

### **Kanzlerdiktatur oder Hyper-Demokratie?**

Wir stehen heute wie bei der französischen Revolution vor der Herausforderung einer demokratischen Erneuerung, allerdings mit dem Unterschied, daß hier keine Köpfe rollen, sondern gewaltfreie Algorithmen, die das Recht auf Freiheit einfordern.

Wer leichtfertig die undemokratischen Praktiken der Regierungen aus den 60er und 70er Jahre wiederholt, riskiert einen ernsthaften Konflikt mit der heutigen Online-Gemeinschaft. Niemand wird es gelingen, die Freiheit der

Gemeinschaft. Niemand wird es wagen, die Freiheiten der interaktiven Teilnehmer der Zweiten Moderne einzuschränken, vor allem nicht mit Regeln, die sich nicht kontrolliert werden können. Wer glaubt, Gesetze definieren zu müssen, die Grundrechte einschränken, ohne die Mehrheit der Menschen hinter sich zu haben, braucht sich nicht zu wundern, wenn es zum Eklat kommt.

Die heutige Regierung, ein Auslaufmodell der Adenauerzeit, von einigen Cyberpunkts auch als Kanzlerdiktatur bezeichnet, hat ihre Legitimation in virtuellen Welten längst verloren. Es muß deshalb verhindert werden, daß sich entlang der Netzknoten eine Kontrollgesellschaft etabliert. Eine Hyper-Demokratie darf nicht zu einem Vierten Reich oder zu einer Kultur der Gleichmacherei führen, sondern erfordert humanitäre und freiheitlichen Prinzipien, um Kreativität und Vielfalt zu fördern. Viele der Internetnutzer gehen nicht deshalb nicht zur Wahl, weil sie politikverdrossen sind, sondern weil sie in den Netzen längst begonnen haben, neuartige virtuelle Gemeinschaften aufzubauen, die grenzüberschreitend, global und emanzipatorisch sind. In diesen Hyper-Demokratien wird der Bürger nicht gegängelt, sondern er ist interaktiver, gestaltender Teilnehmer in Online-Gemeinschaften.

### **Rosinenbomber der Zweiten Moderne**

Die CIA-Agenten der Nachpostmoderne sind virtuelle Agenten im Internet, die uns die Arbeit erleichtern und uns vor ungebetenen Gästen schützen. Die Würdenträger des Cyberspace sind keine unfähigen Aufsichtsräte und Vorstände, sondern Netzwerke, die sich für die Gemeinschaft einsetzen und verdient machen. Die Heinrich Heines des telematischen Zeitalters sind Quervernetzer, die Hierarchien umgehen und sich für kostenloses Wissen für alle und für die Freiheit der Verschlüsselungsverfahren einsetzen. Die Rosinenbomber der Zweiten Moderne sind deshalb E-Mail-Rundbriefe für die Freiheit.

Es ist nicht einzusehen, warum die Geheimdienste das Recht haben sollen zu schnüffeln, dem Bürger jedoch das Recht genommen werden soll, sich davor zu schützen. Ein Verschlüsselungsverbot ist zur Verbrechensbekämpfung völlig ungeeignet, da es lediglich zu einer präzisen Überwachung ehrlicher Bürger führt. Erlaubt man statt eines generellen Verschlüsselungsverbotest nur schwache, von Sicherheitsdiensten kontrollierbare Verschlüsselungsverfahren, so wird die Mißbrauchsgefahr sogar erhöht, da die Schlüssel unsicher sind und eine Bestechung korrupter Beamter, die die Codierungen kennen, nicht ausgeschlossen werden kann. Das Argument der Geheimdienste, daß das Kryptographie-Verbot gegen Terrorgruppen und Kriminelle gerichtet ist, die sonst über das Internet gefahrlos kommunizieren könnten, ist genauso wenig

stichhaltig, da diese Verschlüsselungstechniken benutzt werden, die nicht als solche zu erkennen sind. Ein Verbot trifft also in erster Linie die Teilnehmer freier und offener Systeme.

Zusammen mit Simulationen bilden die Codierungen die entscheidende technologische Grundlage für den Wettbewerb von Hightech-Firmen. Für die Deutsche Interessengemeinschaft Internet (DIGI e.V.) führt deshalb die staatliche Beschränkung von kryptographischen Verfahren neben der Beschneidung elementarer Bürgerrechte vor allem dazu, die Position Deutschlands als Standort innovativer Wirtschaftsunternehmen zu schwächen. Nur die Verschlüsselung schafft die Grundlage, Vertrauen in die Daten zu erlangen und diese wirtschaftlich zu nutzen. Ein Verschlüsselungsverbot behindert diese Nutzung und hemmt das Wachstum der elektronischen Märkte. Darüber hinaus würde eine Regulierung die Exportchancen deutscher Sicherheitsprodukte drastisch reduzieren.

### Sag's durch die Blume

Marit Köhntopps Metapher der [Kommunikation durch die Blume](#) verkörpert am besten die intelligenteste Verschlüsselungsmethode der Zweiten Moderne: die Steganographie (= das verdeckte Schreiben) oder die Wissenschaft der unsichtbaren Kommunikation.

Im Gegensatz zur Kryptographie, bei der es um das Aufspüren, Entschlüsseln und Manipulieren von sichtbaren Daten geht, ist es das Ziel der Steganographie, Botschaften innerhalb von anderen harmlosen Botschaften zu verbergen, ohne daß ein Exo-Beobachter davon Kenntnis erlangen kann, d.h. selbst die Tatsache des Verschlüsseln ist streng geheim. Auch wenn der Beobachter vollste Kenntnis über den Aufbau und die Implementierung des steganographischen Systems hätte, könnte er verborgene Nachrichten ohne die Kenntnis des versteckten Zufallscodes nicht entdecken (Kerckhoffsches Kryptographie-Prinzip). Die Steganographie hängt somit nicht von der Kenntnis des Verfahrens ab, sondern nur von einem geheimen Schlüssel mit ausreichend großer Länge. Steganographische Verfahren haben zwei unterschiedliche Zielsetzungen für das Verstecken eines Codes: die Unsichtbarkeit einer Nachricht und das Markieren eines Dokumentes. Während bei der ersten Zielsetzung das Nichterkennen für Beobachter im Vordergrund steht, geht es bei der Markierung um das Erkennen von illegalen Kopien oder Fälschungen (z.B. bei Banknoten).

Die Steganographie ist eine typische Endo-Technologie, da sie nur dem eingeweihten interaktiven Nutzer die Kenntnis über den geheimen Code zubilligt und der Abhörer nicht die geringste Chance hat, ohne diesen geheimen Code Nachrichten zu entschlüsseln. Da die Menge der versteckten Daten sehr viel kleiner ist als die Nachricht, in die sie vernackt werden können

... können aber auch die Täuschung, in die sie verpackt werden, können durch Täuschungsmanöver eine Vielzahl von möglichen Interpretationen auf einem Bild oder in einem Text untergebracht werden.

Die meisten Kommunikationskanäle wie Telefonverbindungen und Radiosender rufen ein 'Rauschen' hervor, weswegen sie sich ebenfalls für eine steganographische Verschlüsselung eignen. Das Rauschen kann durch ein Rauschen ersetzt werden, welches ununterscheidbar vom ursprünglichen Rauschen ist, jedoch einen geheimen Schlüssel enthält. Allerdings muß ein derartiges steganographisches System die Eigenheiten des Übertragungskanals kennen und das Rauschen um diese Eigenheiten korrigieren, wenn der geheime Code unentdeckt bleiben soll. Effiziente Verfahren erfordern deshalb, die für Nachrichten gewählte Übertragungsmethode genauestens durch statistische Methoden zu analysieren, damit im "Rauschen" keine Daten erkannt werden können. Eine weitere Verbesserung der Verschlüsselung kann durch die rekursive Anwendung eines Steganographie-Programms auf sich selbst oder durch Überlagerung unterschiedlicher Verschlüsselungs-Software erreicht werden.

## Fazit

Netzsicherheitsexperten lehnen die Einschränkung der Verschlüsselungsfreiheit strikt ab, da die Verschlüsselung für eine sichere Betreuung von Rechnern in den Datennetzen unumgänglich ist.

Nur durch Datenverschlüsselung ist zu verhindern, daß Hacker über bestehende Verbindungen in fremde Rechner eindringen und Daten manipulieren. Digitale Signaturen erlauben eine sichere Überprüfung von Senderdaten sowie einen effektiven Schutz der Daten. Deshalb kann Rechtssicherheit in der Wissens-Ökonomie nur dann erreicht werden, wenn die Teilnehmer als einzige auf ihren privaten Schlüssel zugreifen können. Dies ist die Grundlage für die Wahrung der Teilnehmer-Identität und der Transaktionssicherheit in Netzen.

Da der Einsatz exzellenter kryptographischer und steganographischer Verfahren nicht nachweisbar ist, kann es keine überprüfbare Reglementierung der Verschlüsselungstechnologien geben. Sämtliche Bestrebungen von Regierungen kryptographische oder steganographische Verfahren staatlich zu kontrollieren, bleiben wirkungslos und setzen die Politiker der Kritik aus, daß sie es mit der freiheitlichen Grundordnung nicht sehr ernst nehmen.

Entscheidungen über Technologien sollten deshalb nur dann gefällt werden, wenn man die Folgewirkungen von Entscheidungen kennt, da sonst die Freiheit und die Würde der

Entscheidungen kennt, da sonst die Freiheit und die Würde der interaktiven Teilnehmer nicht gewährleistet werden kann. Nur wenn es den Bürgern gelingt, ihre Daten sicher zu ver- und entschlüsseln, hat der Orwellsche Überwachungsstaat keine Chance. Diesen Artikel widme ich Peter Surava (dem Schweizer Freiheitskämpfer gegen den Totalitarismus).

Alles über die [Kryptographie-Diskussion](#)

Über [Steganographie](#)

Marin Köhntopp: [Steganographie als Verschlüsselungstechnik](#)

forum   
add message

No Messages

[↑ top](#)

Copyright © 1996-2000. All Rights Reserved. Alle Rechte vorbehalten  
Verlag Heinz Heise, Hannover  
last modified: 24.11.2000



redaktion