

■ In den USA kämpfen Regierung, Industrie und eine elektronische Guerillatruppe seit zwei Jahren darum, wieviel abhörsichere Datenverschlüsselung ein Staat ertragen kann – eine Vorschau auf den künftigen Streit um bürgerliche Freiheiten im digitalen Zeitalter

Bericht vom Kryptokrieg

Von Steven Levy

Kriege kennt die Welt in der ersten Hälfte der neunziger Jahre mehr als genug. Es mag frivols erscheinen, zu all den Konflikten unserer Tage noch einen weiteren zu zählen, in dem bisher kein Blut floß. Aber es ist gut möglich, daß die Geschichtsbücher des 21. Jahrhunderts ihn der Erwähnung wert befinden werden. Schließlich steht nicht weni-

Privatsphäre im digitalen Zeitalter. Welche verschiedene Interessen dabei aufeinandertreffen, machten dieses Jahr die Kämpfe zwischen Staatsorganen der USA und einer Gruppe von Leuten deutlich, die man Cypherpunks nennt, einer Truppe erklärter Saboteure: Hacker, Hardwarespezialisten und High-Tech-Revolutionäre.

Wichtigste Zielscheibe ihres Zorns ist der Clipper-Chip, offiziell MYK-78 genannt – ein Computerchip, kaum größer als ein Zahn und äußerlich nicht von tausend anderen zu unterscheiden. Die Cypherpunks betrachten Clipper als das Werkzeug, mit dem Big Brother in Mitteilungen und Transaktionen der Bürger herumschnüffeln wird. Die Verfechter von Clipper wiederum, die größtenteils in der Regierung sitzen, halten ihn für die letzte Möglichkeit, das Individuum und die nationale Sicherheit vor Kriminellen, Terroristen und Spionen zu schützen. Die beiden Parteien haben sich gerade in einer Feuerpause zurechtgefunden, ausgestanden ist der Konflikt noch lange nicht.

Man muß sich vor Augen halten, daß die unaufhaltsame Computersierung aller Kommunikation nicht vor Lauschern schützt. Im Gegenteil. Firmen etwa wissen, daß die Konkurrenz durchaus ihre Telefongespräche, Daten und Faxen anzapfen könnte. Dagegen gibt es ein Mittel, das Verschlüsselung heißt – die Anwendung von Methoden einer mathematischen Disziplin namens Kryptologie. Sie sind mittlerweile billig, einfach einzusetzen und praktisch nicht mehr zu knacken.

Doch Verschlüsselung schützt Gesetzestreue und Gesetzlose gleichermaßen. Geheimdienste und Strafverfolgungsorgane nicht nur der USA argumentieren, ihre Bemühungen würden ad absurdum geführt, sobald sichere Codes in allgemeinen Gebrauch kämen, und sie fanden einen Kompromiß. Er nennt sich *key escrow*: Stets wird dabei der verwendete Schlüssel in irgendeiner Form „zu treuen Händen“ hinterlegt; die Behörden können dann im Fall des Falles darauf zurückgreifen und chiffrierte Information in Klartext zurückverwandeln.

Clipper ist die erste öffentliche Verwirklichung dieses Prinzips. Würden etwa – einfachstes Beispiel – digitale Telefone mit dem Clipper-Chip ausgerüstet, dann wäre gewährleistet, daß Gespräche nicht von Dritten abgehört werden könnten – außer von Behörden wie dem FBI. Genehmigt ihnen ein Richter eine Abhöraktion, könnten sie mit Hilfe des hinterlegten Schlüssels des verwendeten Chips die erlauchten Daten hörbar machen (siehe ZEIT Nr. 39/93, Seite 49).

1993 wurde das Konzept vorgestellt und löste schon Aufruhr in der Branche

aus. Trotzdem gab das Weiße Haus am 4. Februar 1994 dem Clipper-Chip als Standard grünes Licht. Innerhalb eines Monats trafen bei der in Sachen Clipper engagiertesten Bürgerinitiative, den Computer Professionals for Social Responsibility, 47.000 Proteststimmen ein. „Der Krieg ist ausgebrochen“, lautete die Eilmittelung Tim Mays, eines Mitbegründers der Cypherpunk-Gemeinde.

Die ganze Aufregung ist letztlich die logische Folge einer Entdeckung, die ein junger Kryptologe namens Whitfield Diffie nicht nur eine Behörde, was sehr ungewöhnlich war, denn damals betrieb der Staat alle ernstzunehmenden kryptologischen Forschungen, in erster Linie in Fort Meade, Maryland, dem Hauptquartier der hochgeheimen National Security Agency (NSA). Die NSA hört angeblich alle internationalen Datenströme ab, und obwohl sie mit der Zeit größer wurde als die CIA, wußte jahrelang kaum jemand von ihrer Existenz; die Initialen stünden für „No Such Agency“, witzelte man in Washington. Sie war auf dem Feld der Kryptologie so dominierend, daß sie sogar den Daumen auf die wenigen Experten hielt, die nicht auf ihrer Gehaltsliste standen.

Whitfield Diffie war davon immer unberührt. Mittlerweile ist er 51 und arbeitet für den Workstation-Hersteller Sun Microsystems als Spezialist für Computersicherheit. Er sieht aus wie ein Romanheld von Tom Robbins mit seinen blonden schulterlangen Haaren und dem halb-langen Bart, der so etwas wie ein Erkennungszeichen unter Kryptologen sein muß.

Diffies Interesse an Kryptologie erwachte endgültig, als er 1966 ans Massachusetts Institute of Technology (MIT) kam. Er sah den niedrigen Sicherheitsstandard des dort verwendeten Großrechners: Ein Systemmanager besaß den Zugriff auf sämtliche Paßwörter für Dateien. Ein perfektes System, dachte Diffie, würde diesen „Treuhänder“ nicht brauchen. Von da an grübelte er über einem zentralen Problem der kryptographischen Praxis, nämlich der Verwaltung der Schlüssel.

Ein Schlüssel ist sozusagen die Anweisung, was ein Absender mit seinem Originaltext anzustellen hat. Er macht aus ihm scheinbar Sinnloses, den chiffrierten Text. Der Empfänger verwandelt ihn mit einem gegenteiligen Schlüssel in den Originaltext zurück. Der Schlüssel von Julius Caesar beispielsweise bestand einfach darin, jeden Buchstaben durch einen Buchstaben drei Stellen weiter hinten im Alphabet zu ersetzen. „Hilfe“ wird so zum sinnlosen „Kloih“; wer den Schlüssel kennt, dechiffriert es wieder als „Hilfe“.

Später wurden die Verfahren komplexer, aber das Problem lag immer bei der Sicherung des Schlüssels. Da jeder, der

den Schlüssel entdeckt, die codierten Texte lesen kann, muß man den Schlüssel möglichst oft ändern. Doch wie setzt man den Empfänger darüber in Kenntnis? Wenn man den neuen Code mit Hilfe des alten durchgibt und dieser schon geknackt ist, kennen die Lauscher auch gleich den neuen.

1969 kam Diffie an die Stanford-Universität im kalifornischen Palo Alto. Mitte der siebziger Jahre gelang ihm und Martin E. Hellman, Professor für Elektrotechnik in Stanford, dann der Durchbruch, der die

Beim System hat jeder Benutzer – in der Rolle des Empfängers – zwei Schlüssel: einen öffentlichen, den *public key*, den er frei an seine Absender verteilt, und einen *private key*, den er unter allen Umständen für sich behalten muß. Was mit dem öffentlichen Schlüssel durcheinandergebracht wurde, kann nur mit dem privaten wieder lesbar gemacht werden. Aus mathematischen Gründen kann ein Lauscher die codierten Daten selbst dann nicht leichter knacken, wenn er den öffentlichen Schlüssel besitzt.

Wenn ich also Whit Diffie eine Nachricht übermitteln möchte, erhalte ich zuerst von ihm seinen öffentlichen Schlüssel. Den benutze ich, um die Mitteilung an ihn zu chiffrieren. Das entstandene Kauderwelsch kann nur von einem einzigen Menschen auf der Welt dechiffriert werden – von Whit Diffie selbst mit seinem privaten Schlüssel.

Das mathematische Prinzip, das dahinter steckt, liefert der digitalen Kommunikation übrigens auch fälschungssichere „elektronische Unterschriften“ und fälschungssicheres, anonymes „elektronisches Geld“.

In kürzester Zeit entwickelten drei Mathematiker am MIT – Ronald L. Rivest, Adi Shamir und Leonard M. Adleman – ein System, mit dem sich Diffies und Hellmans Veröffentlichungen in die Praxis umsetzen ließen. Sie gründeten eine Firma, die das System, nach den Initialen der Autoren RSA benannt, vermarktet. Der Alptraum des Geheimdienstes NSA begann.

Wie sich eine universale Verbreitung sicherer Kryptographie auf die NSA auswirken könnte, läßt sich schwer abschätzen: Der Geheimdienst würde allmählich ertauben. Schutz vor Terroristen und Schutz der nationalen Sicherheit – das führte die Regierung Clinton als Grund an, sich für das Treuhandverfahren *key escrow* zu entscheiden und auch weiterhin den Export sicherer Verschlüsselungssysteme zu beschränken.

Kritik daran kam natürlich zuvorderst von betroffenen Firmen. D. James Bidzos, der vierzigjährige Chef der RSA Data Security in Redwood, Kalifornien, sagt: „Seit fast zehn Jahren ärgere ich mich mit den Leuten von Fort Meade herum. Der Erfolg unseres Unternehmens ist das Schlimmste, was denen passieren kann.“ Die RSA-Technik wurde von Apple, AT & T, Lotus, Microsoft, Novell und anderen Herstellern übernommen, aber die

Spy vs. nerd, Spion gegen Technikfuzzi, so brachte das Magazin „Wired“ im Juni 1994 das Messerstechen um den Verschlüsselungschip Clipper parodistisch auf den Punkt

Exportgesetze legen ihnen und Bidzos' Unternehmen Handschellen an. Dabei sind die RSA-Algorithmen weitgehend wie in Moskau buchstäblich auf der Straße gehandelt. Douglas R. Miller, in der Software Publishers Association zuständig für Verhandlungen mit der Regierung, sagt: „Das einzige, was Exportkontrollen bewirken, ist, unsere Wettbewerbschancen zu ruinieren.“

Der NSA war bald klar, daß das Geschäft mit wirksamer Kryptographie einen Boom erleben würde, sobald auch billige Computer die Verschlüsselung ohne große Verzögerung erledigen könnten. So entwarf die Behörde eine Strategie für die neunziger Jahre. Sie hatte ein neues Codiersystem entwickelt, basierend auf einem Algorithmus namens „Skipjack“, der sechzehn Millionen Male sicherer sein soll als der derzeitige Standard DES (Data Encryption Standard). Skipjack ist geheim; alle Behauptungen über seine Wirksamkeit lassen sich also nicht überprüfen – auch ein Punkt der Kritiker.

Für den öffentlichen Gebrauch bekam Skipjack eine Treuhand-Hin- und hergabe eingebaut und wurde in einen Chip namens „Capstone“ integriert. Er fügt jeder verschlüsselten Information eine Kennung an, die den Abhördienst zum passenden hinterlegten Schlüssel führt. 1993 kam plötzlich die Gelegenheit, diese Technik auf den Markt zu bringen. Der Telefonriesen AT & T hatte der NSA ein kostengünstiges Chiffriertelephon namens Surity 3600 vorgestellt, das den nicht zum Export freigegebenen DES-Algorithmus verwenden sollte. Daraufhin schlug die NSA vor, AT & T solle eine andere Lösung versuchen, eine abgespeckte, billige Version des Capstone-Chips – den Clipper. Der Staat würde dafür Tausende von Telefonen zum eigenen Gebrauch kaufen und das Gerät obendrein zum Export freigeben, was weitere Kostenvorteile versprach – der Preis pro Chip liegt derzeit bei rund zwanzig Dollar. Das ließe sich bei großen Stückzahlen noch auf die Hälfte senken, versichert Mykotronx, die Herstellerfirma der Clipper-Chips.

Damit sollte Clipper die Chance bekommen, zum Standardsystem der Datenverschlüsselung zu werden. NSA und FBI wissen, daß sie sichere Kryptographie nicht unterbinden können. Ihr Ziel ist jedoch zu verhindern, daß die nicht mehr zu knackenden Verschlüsselungen zur Regel werden, denn dann bräuhete selbst der dümmste Verbrecher keine Sorge mehr vor einer Überwachung zu haben. Würde der Clipper-Chip generell eingeführt, so würde nach Meinung der Behörden nur ein winziger Prozentsatz der Benutzer andere Codes verwenden.

Trotzdem war die Computerindustrie überfordert, als die High-Tech-freundliche Clinton-Regierung die Pläne der NSA billigte. Als Clipper im April 1993 zur Be-

gutachtung als nationale Norm vorgelegt wurde, waren von 320 Stellungnahmen genau zwei positiv. Trotzdem wurde die Einführung von Clipper im Februar 1994 besiegt, und der Kryptokrieg brach los. Das Frühjahr war von flammenden Diskussionen und endlosen Anhörungen bestimmt; die Regierung blieb ungerührt.

Als hätte der Konflikt noch einer Aufschaukelung bedurft, zeigte im Juni Matthew Blaze, ein Forscher der Bell Laboratories von AT & T, einen schwerwiegenden Fehler von Clipper, durch den ein technisch versierter Gesetzesbrecher die Abhörfunktion umgehen könnte. Auch das machte keinen Eindruck – der technisch versierte Verbrecher würde ohnehin seine eigene Verschlüsselung anwenden, hieß es.

Cypherpunks – so nennen sich all jene, die nicht nur protestieren, sondern auch technisch alles tun wollen, das Konzept der Treuhandkryptographie zu untergraben. Die Truppe wurde gegründet von Eric Hughes, dem 30-jährigen Kryptographen, und Tim May, einem 42-jährigen Physiker und ehemaligen Mitarbeiter des Chip-Herstellers Intel. Das war im September 1992 im Silicon Valley in Kalifornien, aber der eigentliche Treffpunkt der Cypherpunks ist das weltumspannende Internet mit seinen Diskussionsgruppen. Ihr Credo lautet: Sichere Kryptographie bietet dem Individuum die Chance, allein über seine Daten zu verfügen, und diese Freiheit dürfe niemals beschränkt werden.

Der vielleicht meistbewunderte Cypherpunk ist ein Mann, der von sich sagt, er passe nicht dazu, weil er oft einen Anzug trage. Er heißt Philip R. Zimmermann, ist vierzig Jahre alt und Berater der Boulder Company in Colorado. 1991 entwickelte er ein Chiffrierprogramm für Computerdaten, das er „PGP“ nannte (für „Pretty Good Privacy“), und er entschloß sich, es kostenfrei zu verteilen. Inzwischen hat er schon mehrere Updates vorgenommen, und die aktuelle Version umgeht erfolgreich alle Probleme mit RSA-Patenten und Exportregulierungen. So entwickelt sich PGP zu einer weltweiten Volksnorm für die Public-Key-Kryptographie, und sein Erfinder arbeitet intensiv daran, es als VoicePGP fürs Telefon verfügbar zu machen.

Zimmermann, in früheren Jahren aktiver Atonkraftgegner, ist der Ansicht, eine der wichtigsten Aufgaben von Geheimcodes sei, Informationen vor der Obrigkeit geheimzuhalten. Er hat zum Beispiel erfahren, daß birmesische Freiheitskämpfer in Trainingscamps im Dschungel den Umgang mit PGP am Laptop lernen, um ihre Daten zu schützen.

Dieserart sind die Argumente im Kryptokrieg. Der NSA-Berater Stewart A. Baker sagte im März 1994 auf einer Konferenz, die Kritik an *key escrow* sei „nur die Rache von den Leuten, die nicht nach

Hausaufgaben in Trigonometrie zu erledigen hatten“. Er fügte an: „Von PGP heißt es, es habe Freiheitskämpfer in Lettland und anderswo geschützt. Aber hier haben es die Strafverfolger mit einer ganz anderen Art der Anwendung zu tun bekommen – mit einem Kerl, der PGP benutzte, damit die Polizei nicht herausfinden konnte, welche kleinen Jungen er über das Netz verfuhr hatte.“

So ging es bis zum Sommer 1994. Im Juli schrieb Vizepräsident Al Gore einer prominenten Kritikerin des Projekts, der Kongreßabgeordnete Maria Cantwell, einen Brief. Er zählte darin noch einmal die Grundlagen von Regierungsentschlüssen zur Kryptographie auf. Clipper solle auf Telefone beschränkt bleiben; das Prinzip aber heiße auch für die Zukunft *key escrow*.

Die Worte waren die alten, aber der konzentrierte Ton wohl ließ manche Kritiker aufhorchen. Sie feierten das Schreiben als Rückzug der Regierung. Andere warnten: In der Sache habe sich nichts geändert, und das Weiße Haus bestätigte das auf Nachfrage. Trotzdem klangen die akuten Gefechte ab, und der Konflikt um Clipper erlebt eine Feuerpause. Das Programm ist ebenso angelauten wie eine neue Studienphase. Die Frage wird sein, ob Clipper-Telefone auch im Markt ankommen und ob die von der Regierung benannten Treuhandorganisationen am Ende die Millionen Chip-Schlüssel gesammelt haben werden, die das Programm zum Erfolg braucht.

Die Regierung Clinton hat mit anderen Teilen ihres Plans zur Strafverfolgung im digitalen Zeitalter mehr Glück. Anfang Oktober brachte sie mit einigen Kompromissen ihre „Digital Telephone Bill“ durch; dieses Gesetz schreibt Telekommunikationsfirmen vor, das FBI beim Abhören aller digitalen Leitungen, verschlüsselt oder nicht, zu unterstützen.

Bobby Inman, Exdirektor der NSA und bekannt für seine fallweise freimütigen Worte, sagte bei einem Vortrag Mitte November, es gehe der Regierung vor allem darum, dem FBI weiter zu ermöglichen, die Drogenmafia in den USA abzuhören – um so bitterer, daß Clipper nun zum „Mini-Desaster“ geworden sei.

Es ist bekannt, daß die NSA verbesserte Versionen von Skipjack vorbereitet hat und an einem noch leistungsfähigeren Chiffriersystem namens „Baton“ arbeitet. Deren Zeit könnte noch kommen.

Es war Whitfield Diffie, der die Cypherpunks warnte: Sie mögen, da sie Clipper auf allen Ebenen bekämpfen, eine Schlacht gewinnen – aber im eigentlichen Krieg kein Stück vorankommen.

© New York Times Magazine, Übersetzung aus dem Englischen: Regine Reimers

Bulkware

Seiokronto pafriplo

Handbücher gehören zu den großen Rätseln der Computertechnik. Sie wollen erklären, sind sehr oft aber nur zum Raten geeignet. Jede Buchhandlung kann den Beweis führen. Dort stehen tonnenweise Bücher herum, die alle den Anspruch haben, die Käufer besser als die „Dokumentation“ in die „Logik“ eines bestimmten Programmes einzuführen. Und alle glänzen mit „praxisnahen Beispielen“, gegen die Erika Mustermann aus Musterstadt eine blasse Nummer ist.

Selten sind die Beispiele in der Literatur nur halb so inhaltstark wie die latinisierten Leerfloskeln, mit denen Desktop-Publishing-Programme aufwarten, wenn eine Seitenfüllung optisch geprüft werden soll. Der Blindtext „Obemus gontum nipsit“ hat noch mehr Charakter als die simple Hauskaufanzeige, mit der einst die Textverarbeitung Write in Windows 1.0 den Benutzer das Tippen lehrte. Auch daß man das japanische „Essen“ in Hiragana-Schrift einkopieren durfte, verlieh der Sache wenig Praxis-appeal.

Um eine Art Besserung bemühte sich der Hersteller Microsoft erst mit der Version 3.1 von Windows: Die dort gezeigte Kombination eines Ausschnittes aus dem „Zauberlehrling“ mit einem allgemeinen Polynom aus der höheren Mathematik kann als Praxis pur gelten.

Die belgische Firma Infosystems operierte anno 1986 bei ihrer Textverarbeitung Genius mit Morgenstern „Lalula“. „Markieren Sie das Wort biffi und kopieren es hinter hulelumi; löschen Sie dann seiokronto und fügen lalula ein.“

Wenn es darum ging, die hohe Schule der Datenbankabfrage zu lehren, waren amerikanische Präsidenten als Füllmaterial beliebt. Der Hersteller Gupta erzielte große Effekte, als er mangels Präsidentenmasse den Datenbestand mit lokalen Adressen ergänzte. Frage ans Lernprogramm: Wie viele US-Präsidenten kommen aus

Das Trainingsprogramm des Norton Administrator for Networks stattet die US-Präsidenten mit vernetzten Computern aus. Washington und Monroe bekommen wahre Boliden mit toller Graphikhardware und großen Festplatten, während sich Richard Nixon an einem Uraltrechner mit monochromer Grobkorngrafik abplagt. Die Beispielspräsidenten bringen ihre Festplatten zum Überlaufen oder verletzen Lizenzbestimmungen; der Leser lernt, ihnen beizeiten auf die Finger zu klopfen. Ein Warmstart von Clinton per Fernsteuerung ist hier kein Problem.

Die Datenbankfirma Oracle ist mittlerweile bei der Pizza als Demonstrationsobjekt angelangt. Das hat Vorteile: Pizza kennt jeder, und die Varianten sind endlos. Außerdem kann man mittels Multimedia wunderbar zeigen, was aus dem Ofen kommt.

Der Chef von Oracle persönlich führte unlängst im US-Fernsehen die Leistungen seines neuen Systems vor. Er stellte aus der Oracle-Datenbank an einem Multimediarechner eine lekere Pizza zusammen (Thunfisch, Ananas und Chili). Der Showmaster, befragt, was er von der Sache halte, sagte: „Mir wird schlecht.“

Das deutschsprachige Handbuchwesen ist im internationalen Vergleich sauber und bekömmlich. Und vor allem gewaltfrei. Die Übersetzer des russischen Programms PTS/DOS Extended wollten sich gewiß nach diesen Usancen richten, als sie aus dem gefährlichen „Datei löschen“ ein freundliches „Datei abwischen“ machten.

PTS/DOS, ein Clone des guten alten Betriebssystems MS-DOS, bietet auch ein Einstiegsprogramm an, das von zwei Nagern bewältigt werden kann, der rechtschändigen und der linkschändigen Maus. So wird sich denn mancher DOS-Benutzer vor dem Drücken der verschiedenen Mauspfoten den Kopf zerbrechen.

Bei der Trennung von rechts und links im Kopf hilft, was vor Jahren die deutsche Version des Telekommunikationsklassikers Procomm postulierte. Das Vorwort des Handbuchs befähigte sich mit der spezifischen Schwermut der Deutschen. Sie erklärte sich, so wurde da wortreich gemutmaßt, „aus dem zwiespältigen Verhältnis der Deutschen zum Computer. Einerseits erscheint ihm (dem Deutschen) die neue Technologie recht interessant, doch insofern quält ihn die ungewisse innere Angst, als anerkannter Dichter und Denker zukünftig nur noch die linke Hälfte wert zu sein.“ Das sollte uns allen zu dichten und zu denken geben.

