Über die Notwendigkeit genormter kryptographischer Verfahren

Michael Waidner, Birgit Pfitzmann, Andreas Pfitzmann
Institut für Informatik IV, Universität Karlsruhe,
Postfach 6980, 7500 Karlsruhe

Gliederung

1 Über die Notwendigkeit der Kryptographie
1.1 Rechtssicherheit und Datenschutz im Wandel der Zeiten
1.2 Unwandelbarer Datenschutz und Rechtssicherheit
2 Über die Möglichkeiten der Kryptographie
3 Über die Auswahl kryptographischer Verfahren
4 Literatur

Stichwörter

Anonymität, CCITT, Datenkopien, Digitale Signaturen, DIN, eigenhändige Unterschrift, Ende-zu-Ende-Maßnahmen, garantierter Datenschutz, garantierte Rechtssicherheit, Informationelles Selbstbestimmungsrecht, ISDN, ISO, Kommunikationsnetze, Kryptographie, Lauschangriff, Lichtwellenleiter, Massenüberwachung, Normung von Kryptosystemen, National Security Agency NSA, Offene digitale Systeme, Schlüsselregister, Schlüsselverteilung, sichere Geräte, Sicherheitsvalidierung, Systembetreiber Post, Trojanisches Pferd, Zentralstelle für das Chiffrierwesen ZfCh.

Zusammenfassung

Ausgehend von der zunehmenden Bedeutung offener digitaler Systeme wird die Notwendigkeit dargestellt, diese Systeme so zu gestalten, daß ihre Benutzung unbeobachtbar durch Unbeteiligte und anonym vor Beteiligten stattfinden, aber dennoch Rechtssicherheit garantiert werden kann. Diese Forderung muß in für die Betroffenen nachvollziehbarer Weise erfüllt werden, was insbesondere hinsichtlich des Datenschutzes aus dem 1983 im Volkszählungsurteil des BVG formulierten informationellen Selbstbestimmungsrecht abzuleiten ist.

Allein durch juristische Regelungen ist diese Forderung nicht zu erfüllen, doch sind in der Informatik Methoden bekannt, die geeignet sind, die Einhaltung juristischer Regelungen in für die Betroffenen nachvollziehbarer Weise zu garantieren.

Alle bekannten und u.E. brauchbaren Methoden basieren auf der Verwendung sicherer kryptographischer Techniken zum Verschlüsseln oder Unterschreiben digital codierter Information innerhalb von Ende-zu-Ende-Protokollen. Soll ein System wirklich offen, also sowohl hinsichtlich der Teilnehmer als auch hinsichtlich der Dienstanbieter beliebig erweiterbar sein, so müssen die verwendeten kryptographischen Techniken standardisiert werden, im Bereich der Bundesrepublik Deutschland z.B. durch den Betreiber der Fernmeldeanlagen, also die Deutsche Bundespost, oder im

---

erscheint in „DuD, Datenschutz und Datensicherung, Recht und Sicherheit der Informations- und Kommunikationssysteme", Vieweg & Sohn, Wiesbaden, Heft 6 / Juni 1987

größeren Rahmen durch das Deutsche Institut für Normung, DIN, und dessen internationales Pendant, die International Standards Organization, ISO.

Bisherige Arbeiten von DIN und ISO zur Normung von Kryptosystemen wurden jedoch ergebnislos eingestellt. In den USA hat statt dessen die National Security Agency, NSA, begonnen, selbst Techniken zu standardisieren, jedoch ohne deren Entwurf bekanntzugeben. Damit ist eine Sicherheitsbewertung der NSA-Techniken durch die Fachwelt erschwert oder unmöglich und zudem ein Schutz vor der NSA durch die NSA-Techniken prinzipiell unmöglich.

Vor einer Nachahmung dieses Weges beim Einsatz von Kryptosystemen in offenen digitalen Systemen zu warnen und zugleich zur Beschreitung eines Weges durch DIN oder die Deutsche Bundespost, der zur Normung bekannter und validierter Kryptosysteme führt, aufzufordern, sind die Hauptziele dieses Artikels.

1 Über die Notwendigkeit der Kryptographie

1.1 Rechtssicherheit und Datenschutz im Wandel der Zeiten

Die wirtschaftliche (und damit teilweise auch politische) Entwicklung der letzten Jahre war gekennzeichnet durch den zunehmenden Einsatz datenverarbeitender Maschinen, die immer leistungsfähiger und billiger wurden. War dieser Einsatz zunächst nur auf Firmen und Organisationen zur Automatisierung von Verwaltung oder Produktion beschränkt, so breitet er sich seit einigen Jahren in zweierlei Hinsicht auf die gesamte Gesellschaft aus.

Zum einen gewinnt die digitale Kommunikationstechnik zunehmend an Bedeutung, was in der Planung der Deutschen Bundespost (DBP) einerseits ihren Ausdruck findet, andererseits durch diese gefördert wird. Diese Planung sieht vor, die zahlreichen Kommunikationsdienste der DBP, z.B. Fernsprechen, Telex oder DATEX, und später auch Fernsehen und Bildfernsprechen in einem digitalen Netz zu integrieren (dem ISDN) und dieses Netz als Ersatz für die heutigen dienstspezifischen jedem Teilnehmer zugänglich zu machen [Schö_84, ScSc_84, ScSc_86, ScS1_84, Rose_85]. Dieses Netz wird und muß damit *offen* für jeden Bürger sein.

Zum anderen führt die Kosten- und Leistungsentwicklung innerhalb der Informationstechnik dazu, daß bald die meisten privaten Haushalte über einen kleinen, billigen, aber leistungsfähigen Rechner (PC o.ä.) verfügen können. In Verbindung mit der oben geschilderten Entwicklung hin zur Vernetzung letztendlich aller Haushalte über das ISDN wird dies für viele wirtschaftliche Bereiche, etwa Banken, Versandhandel, Informationsdienste, Presse und Verlage etc., ein Anreiz sein, das ISDN als Basis eines „elektronischen Marktplatzes" [Riha_85, TuCh_85] zu verwenden, auf dem die Benutzer kleinere Rechtsgeschäfte, wie den Kauf und Verkauf von Waren, abwickeln können*.

Damit wird für das ISDN und manche seiner Dienste ein *faktischer Benutzungszwang* entstehen: da es z.B. das heutige Fernsprechen enthalten soll, wird jeder heutige Fernsprechteilnehmer, also fast jeder Haushalt, zwangsläufig zum Benutzer des ISDNs; nehmen z.B. die Banken ihre Chance wahr und statten zahlreiche Läden mit POS-Terminals aus, so dürfte auch hier jeder Kaufwillige faktisch zur Benutzung neuer Bankdienste gezwungen werden (ähnlich wie heute der Besitz eines Giro-Kontos für Gehaltsempfänger fast zwingend ist, oder wie in den USA teilweise nur noch mit Kreditkarten statt Bargeld bezahlt werden kann).

Der Weg in die „Informationsgesellschaft" scheint also über offene digitale Systeme mit faktischem Benutzungszwang zu führen.

Ausgehend von dieser These ist zu fordern, daß diese neuen Systeme hinsichtlich aller wichtigen wünschenswerten Eigenschaften für die Benutzer zumindest den status quo erhalten, was an dieser Stelle im wesentlichen bedeutet:

- **Garantierter Datenschutz:** Da durch ein offenes diensteintegrierendes System der oben geschilderten Art viele Aktivitäten eines Benutzers über ein einziges technisches Medium

---

* Darüber hinausgehende Folgen, etwa hinsichtlich Telearbeit u.ä., sollen hier unberücksichtigt bleiben. Vgl. hierzu [KuRo_86].

abgewickelt werden, ist es notwendig, ihm die Unbeobachtbarkeit seiner Handlungen zu garantieren, insbesondere, da andernfalls das System nicht nur zur Beobachtung ausgewählter einzelner verwendet, sondern auch zur *Massenüberwachung* mißbraucht werden könnte. Diese Garantie muß die Verbergung der Kommunikationsinhalte vor Unbeteiligten, die Unbeobachtbarkeit der Kommunikationsbeziehungen (wer wann mit wem wie lange?) [PfPW_86] und die Möglichkeit zur Anonymität vor dem Partner innerhalb einer Kommunikationsbeziehung [PPW_87] umfassen.

- **Garantierte Rechtssicherheit:** Da über ein offenes System der oben geschilderten Art Rechtsgeschäfte abgewickelt werden sollen, ist zu fordern, daß dies in zumindest derselben Rechtssicherheit erfolgt wie heute. Was dabei „dieselbe Rechtssicherheit" heißt, d.h. wie diese in neuer Umgebung genau zu definieren ist, ist teilweise noch Gegenstand der juristischen Diskussion.

Natürlich steht der garantierte Datenschutz, insbesondere die Möglichkeit zur Anonymität, einer willentlichen Selbstidentifikation eines Benutzers, wann immer er dies möchte oder gesetzlich muß, in keiner Weise entgegen.

Ebenso bleiben notwendige gesetzliche Einschränkungen der Unbeobachtbarkeit einzelner (z.B. *Individualüberwachung* nach dem G10-Gesetz) unbetroffen:

Zum einen können innerhalb der hier betrachteten offenen Systeme kleine Benutzergruppen (wie Terroristen oder Spione, die gern als Beispiel angeführt werden) völlig unabhängig von garantiertem Datenschutz durch entsprechenden Aufwand stets für ihre eigene Unbeobachtbarkeit sorgen, so daß man ihnen mit Datenschutz höchstens die Arbeit etwas erleichtert, jedoch keinesfalls neue Möglichkeiten schafft. Das einfachste ist beispielsweise, wichtige Nachrichten durch softwareimplementierte Verschlüsselung (vgl. Kap. 2) zu schützen, solange diese schmalbandig (z.B. schriftlich oder fernmündlich, also keine Bewegtbilder) sind. Selbst wenn die Verschlüsselung von Nachrichten verboten werden sollte, so könnten solche Gruppen immer noch kurze Nachrichten unter offiziell erlaubten Nachrichten verbergen (Steganographie), z.B. indem sie die zu übertragenden Nachrichten verschlüsseln und in einer Folge von „Meßwerten", die offiziell gesendet werden dürfen, verbergen, da bei Meßwerten weniger als bei Texten auf Sinn geachtet werden muß.

Auch könnte ein Benutzer statt privater Systemanschlüsse öffentliche „Telefonzellen" verwenden oder gar das offene System zur Kommunikation ganz meiden und auf ein privates Funknetz zurückgreifen.

Außerdem erlaubt die technische Entwicklung außerhalb der betrachteten Systeme (immer kleinere und perfektere Abhörmikrofone, die Abtastung von Fensterscheiben mittels Laserstrahl und optische Überwachung durch immer bessere und billigere Kameras) eine immer leichtere Individualüberwachung.

Um beide oben genannten Forderungen zu erfüllen, kann es jedoch nicht genügen, sie nur juristisch, etwa durch Gesetze, zu präzisieren. Vielmehr sollte, wie bei allen gesetzlichen Regelungen, durch organisatorische oder technische Maßnahmen dafür Sorge getragen werden, daß diese Regelungen nicht mißachtet werden können, ohne daß davon Betroffene dies bemerken und dagegen vorgehen können.

Bei der Festlegung dieser Maßnahmen wird manchen Beteiligten (z.B. dem Gerichtswesen als ganzem) hinsichtlich der freiwilligen korrekten Erfüllung ihrer Aufgaben vertraut werden müssen, doch sollte der Kreis derjenigen, denen ein Betroffener vertrauen *muß*, möglichst klein sein. Zumindest sollte sein Vertrauen nicht durch einen einzelnen anderen, sondern höchstens durch eine Gruppe von Beteiligten, die zu diesem Zweck zusammenarbeiten müssen, verletzt werden können.

Daß ein solcher Zustand dem Ideal entspräche, sagt bereits der gesunde Menschenverstand; diesen Zustand anzustreben, ist aber speziell für den Datenschutz auch ein Gebot unserer Verfassung, interpretiert durch das Urteil des Bundesverfassungsgerichtes zur Volkszählung vom Dezember 1983, das Nachprüfbarkeit des Datenschutzes durch den Betroffenen fordert [Bund_83 Seite 272].

Bei beiden Forderungen ist auch zu beachten, daß neue Technologien nicht nur die neuen Systeme prägen, sondern auch die alten in ihren Eigenschaften beeinflussen. So ist z.B. zu erwarten, daß durch Fortschritte in der Sprecher- und Spracherkennung selbst bei Beibehaltung der heutigen Vermittlungstechnik und vor allem der heutigen analogen Übertragungstechnik eine umfangreiche Fernsprechüberwachung möglich würde, und daß durch Fortschritte in der Mustererkennung und

Robotik die „unfälschbare" eigenhändige Unterschrift bald nur noch Fiktion ist. Daher erfordern Datenschutz und Rechtssicherheit auf jeden Fall neue Maßnahmen.

1.2 Unwandelbarer Datenschutz und Rechtssicherheit

Wenn *Datenschutzforderungen*, d.h. Verbote, gewisse Daten zu sammeln, auszuwerten oder weiterzugeben, an jemanden bestehen, dem nicht vorbehaltlos vertraut wird, ist die einzige Möglichkeit, die Erfüllung dieser Forderungen zu kontrollieren, ihm den Zugriff auf die Daten vollständig zu verwehren. Zugreifbare Daten können nämlich beliebig kopiert werden und werden durch eine Verarbeitung nicht verändert, so daß die Kontrolle permanent erfolgen müßte. Bereits eine Lücke in dieser Kontrolle könnte zum unbemerkbaren Weitergeben führen, und einmal erstellte Kopien außerhalb des legalen Bereiches sind praktisch jeder Kontrolle entzogen.

Selbst wenn doch einmal die unerlaubte Weitergabe bemerkt wird (bzw. gerade dann), kann bereits irreparabler Schaden entstanden sein, z.B. wenn personenbezogene Daten eines Benutzers veröffentlicht wurden.

Entsprechend muß bei den die *Rechtssicherheit* betreffenden Forderungen, d.h. Verboten, gewisse Daten, insbesondere Willenserklärungen in Form von digitalen Nachrichten, zu ändern, zu vernichten oder hinzuzufügen, von vornherein gesichert sein, daß keine unentdeckbaren Manipulationen möglich sind, wobei die Echtheit von Daten sogar Dritten gegenüber bewiesen werden können muß (im Gegensatz z.B. zum heutigen Bildschirmtext-System).

Prinzipiell könnte das Verwehren des Zugriffs auf die Daten in beiden Fällen entweder physikalisch oder kryptographisch geschehen. Daher ist in jedem System zu untersuchen, wer an welchen Stellen Zugriff auf Daten hat oder sich verschaffen kann, ob er für vertrauenswürdig gehalten werden kann bzw. muß und ggf. ob man ihn physikalisch von den Daten fernhalten kann; andernfalls sind kryptographische Maßnahmen unerläßlich.

Neben dem Vertrauen auf sich selbst kann einem Benutzer eines Systems höchstens noch Vertrauen in den Systembetreiber, also die Post hinsichtlich der Kommunikation oder die Banken hinsichtlich der Zahlungssysteme, abverlangt werden, nicht jedoch in alle anderen mehr oder weniger Beteiligten, etwa in die Hersteller von Gerät und Software, oder in andere Unbeteiligte, die Gelegenheit haben, Nachrichten mitzuhören oder zu ändern.

Dies ist nicht nur ein Gebot des Schutzes des einzelnen Benutzers: jeder Staat sollte ein Interesse daran haben, daß die Kommunikation seiner Bürger (insbesondere die Geheimnisse seiner Wirtschaft) zumindest vor dem Mithören durch fremde Geheimdienste u.ä. sicher ist. Zur Zeit scheint dies nicht der Fall zu sein; z.B. hat laut [IM46_87] der amerikanische Geheimdienst über Großbritannien vermittelte Telefongespräche abgehört und wissenswerte Informationen über europäische Konkurrenten an amerikanische Firmen weitergegeben.

Der Schutz der Kommunikation zumindest vor „Lauschangriffen" auf Übertragungsstrecken ist heute nur durch Einsatz kryptographischer Techniken möglich. Insbesondere verhindert auch der Einsatz von Lichtwellenleitern zur Übertragung das unbemerkte Mithören nicht [Horg_85].

Bezüglich der Systemzentralen kann man eher hoffen, Unbefugte physikalisch von Daten fernhalten zu können, wobei allerdings eine Mindestvoraussetzung ist, daß man dem Betreiber der Zentralen vertraut.

Solange es weitere Personen gibt, die auf die zur Verarbeitung der Daten verwendete Soft- oder Hardware Zugriff haben müssen, ist dieses Fernhalten aber dennoch ein schwieriges, wenn nicht gar unmögliches Unterfangen: Hersteller, Wartungsfirmen, Betriebspersonal u.ä. können in das System leicht *Trojanische Pferde* [PoKl_78, Thom_84] einbauen, d.h. Systemteile, die Informationen unberechtigterweise sammeln, speichern, verändern und evtl. weitersenden, die aber nach herrschender Meinung kaum aufzuspüren sind (zumal die Suche nach ihnen nie beendet wäre, da ja jederzeit, z.B. nach einer Wartung, ein neues Pferdchen eingebaut worden sein kann).

Folglich müßte schon an den Geräten, die mit schützenswerten Daten in Berührung kommen, jegliche Manipulation, z.B. durch Angestellte, ausgeschlossen sein. Diese Forderung führt zur Idee der *„sicheren Geräte"*, d.h. von informationsverarbeitenden Geräten, die gewisse Daten zwar

verarbeiten und speichern, aber auf keinen Fall nach außen geben. Die Realisierung dieser Idee stößt an zwei Grenzen:

- Auch in ein sicheres Gerät könnten beim Entwurf oder der Implementierung Trojanische Pferde eingebaut werden, was bei hinreichend komplexen Systemen, wie gesagt, kaum nachzuprüfen ist.
- Da sichere Geräte ihre Daten auch bei massiven Angriffen auf ihr technisches Innenleben nicht preisgeben dürfen, muß dieses ebenso massiv geschützt werden, bis hin zur physischen Selbstzerstörung bei erkannten bzw. vermuteten Angriffen. Damit stellt sich einerseits das aus der Safeherstellung altbekannte Problem, ob wohl Konstrukteure oder Panzerknacker findiger sein werden. Andererseits könnte auch die technische Zuverlässigkeit eines solchen bisweilen zumindest seine Daten zerstörenden Gerätes zu gering sein.

Somit scheidet auch die Möglichkeit, Datenschutz und Rechtssicherheit teilweise durch Geräte, die nicht physisch unter der Kontrolle des jeweils betroffenen Benutzers stehen, sondern z.B. bei der Post zentral alle Benutzer bedienen, aus. Niemand könnte für die Sicherheit einer solchen Lösung garantieren.

Übrig bleibt aus technischen Gründen allein, jedem Benutzer die Verantwortung für seinen Datenschutz und die Rechtssicherheit seiner Beziehungen selbst anzuvertrauen (was nach Abschnitt 1.1 sowieso gesellschaftlich wünschenswert ist und insbesondere auch verhindert, dem Benutzer seinen Schutz wieder einfach und von ihm unbemerkt entziehen zu können).

Die Informatik kennt zahlreiche direkt zwischen den Benutzern (also Ende-zu-Ende) anzuwendende Maßnahmen zur Gewährleistung von Datenschutz [PfPW_86] und Rechtssicherheit [PPW_87] innerhalb der hier betrachteten offenen Systeme. Sie basieren ausnahmslos auf kryptographischen Techniken, so daß die **Notwendigkeit der Kryptographie** gegeben ist.

Bei der Durchführung der notwendigen Maßnahmen können (und müssen) die Benutzer sich der Unterstützung von Rechnern bedienen. Für diese Zwecke gibt es hinreichend kleine und billige Rechner, z.B. PCs, die kaum teurer sind als Terminals, die für die Teilnahme am offenen System ohnehin nötig sind. Diese können, da um vieles einfacher als zentrale „sichere" Geräte, auch eher so zuverlässig und unter öffentlicher Kontrolle gebaut werden, daß sich jeder Benutzer zumindest darauf verlassen kann, daß sein eigener Rechner keine Trojanischen Pferde enthält.

2 Über die Möglichkeiten der Kryptographie

Die zur Erfüllung der Forderungen nach Datenschutz und Rechtssicherheit notwendigen technischen Maßnahmen zeichnen sich, wie in Kapitel 1 begründet, alle durch zwei Eigenschaften aus: sie basieren auf kryptographischen Techniken, und sie werden direkt zwischen den Benutzern des Systems abgewickelt, sind also *Ende-zu-Ende-Maßnahmen*.

Die notwendigen kryptographischen Techniken können in zwei Bereiche eingeteilt werden: *Krypto-* und *Signatursysteme*.

Ein Kryptosystem erlaubt, Nachrichten zu verschlüsseln, d.h. sie mit Hilfe eines Schlüssels so umzuformen, daß der Inhalt der verschlüsselten Nachricht nur bei Kenntnis einer gewissen geheimen, vom zum Verschlüsseln verwendeten Schlüssel abhängigen Information wahrgenommen werden kann [Denn_82, DaPr_84, Hors_85].

Wird ein Kryptosystem eingesetzt, um die Kommunikation zwischen zwei beliebigen Benutzern eines offenen Systems zu schützen, so ist offensichtlich ein Hauptproblem, wie ein sendewilliger Benutzer A in Erfahrung bringen soll, welchen Schlüssel er verwenden muß, um einem bestimmten anderen Benutzer B eine Nachricht vertraulich senden zu können. Insbesondere kann man wegen der großen Zahl möglicher Kommunikations- und Geschäftsbeziehungen nicht davon ausgehen, daß alle Benutzer bereits untereinander vertraulich Schlüssel ausgetauscht haben. Ebenso unpraktikabel ist ein Schlüsselaustausch direkt vor jeder Kommunikation über einen sicheren Kanal außerhalb des ISDNs, da dieser bei ausreichender Leistungsfähigkeit dieselben Schutzprobleme aufwirft wie das ISDN

selbst, oder aber für die Anforderungen des Verbindungsaufbaus im ISDN viel zu langsam ist (z.B. wenn man vor jedem Telefonat erst per Kurier Schlüssel austauschen müßte). Die Schlüsselverteilung muß also innerhalb des ISDNs selbst stattfinden.

Entscheidend für die Lösung dieses Schlüsselverteilungsproblems ist, ob der zum Verschlüsseln verwendete Schlüssel auf die geheime Information zum Entschlüsseln schließen läßt oder nicht. Im ersten Fall nennt man das Kryptosystem *symmetrisch* (wobei der Schlüssel i.allg. mit der geheimen Information zusammenfällt und daher selbst „geheimer Schlüssel" genannt wird), im zweiten Fall *asymmetrisch* (wobei der Schlüssel zum Verschlüsseln dann „öffentlicher", die geheime Information zum Entschlüsseln „privater Schlüssel" genannt wird).

Verwendet man ein asymmetrisches Kryptosystem, so genügt für jeden Benutzer ein einziges Paar aus öffentlichem und privatem Schlüssel. Daher kann die Schlüsselverteilung im offenen System höchst einfach und analog zur heutigen Telefonauskunft geschehen: weiß man den öffentlichen Schlüssel eines Partners noch nicht, so richtet man eine Anfrage an ein „Schlüsselregister", das unter Kontrolle durch die Öffentlichkeit steht und dem Anfrager verbindlich den gesuchten Schlüssel mitteilt. Hierzu muß der öffentliche Schlüssel des Schlüsselregisters natürlich jedem Benutzer bekannt sein, was aber durch eine verbindliche Bekanntgabe außerhalb des offenen Systems leicht möglich ist, da dieser Schlüssel für längere Zeit seine Gültigkeit behalten kann.

Bei symmetrischen Kryptosystemen, wozu alle klassischen Kryptosysteme gehören, wird hingegen für jede Kommunikationsbeziehung ein eigener Schlüssel benötigt, den kein Dritter kennen darf. Hier sind zur Schlüsselverteilung im wesentlichen zwei Lösungsansätze bekannt:

Der einfachere Ansatz verwendet zur Schlüsselverteilung ein asymmetrisches Kryptosystem wie oben beschrieben, d.h. einer der beiden an einer Kommunikationsbeziehung Beteiligten wählt einen Schlüssel des symmetrischen Kryptosystems und sendet ihn dem anderen, verschlüsselt mit dessen öffentlichem Schlüssel. Der klassischere Ansatz sieht hingegen die Verwendung einer Schlüsselverteilzentrale vor, mit der jeder Benutzer vor Beginn seiner Teilnahme außerhalb des offenen Systems einen Schlüssel vereinbart hat. Auf Anfrage generiert sie einen Schlüssel für eine Kommunikationsbeziehung und teilt ihn den künftigen Kommunikationspartnern unter Verwendung der mit den jeweiligen Benutzern vereinbarten Schlüssel vertraulich und authentiziert mit [DaPr_84]. Da eine solche Zentrale durch Kenntnis aller verwendeten Schlüssel potentiell alle gesendeten Nachrichten entschlüsseln kann, ist aus Datenschutzgründen diese Lösung zumindest für die hier betrachteten Systeme nicht akzeptabel. Ein Ausweg ist die Verwendung vieler unabhängiger Schlüsselverteilzentralen, die je einen Schlüssel generieren und beiden Kommunikationspartnern mitteilen. Die Kommunikationspartner verwenden als Schlüssel die Summe aller mitgeteilten Schlüssel, so daß alle Schlüsselverteilzentralen zusammenarbeiten müßten, um die Summe zu errechnen und die Kommunikation zu überwachen oder unbemerkbar zu manipulieren.

Ein Signatursystem ist der digitale Ersatz (genauer: die digitale Verbesserung) der eigenhändigen Unterschrift. Seine Definition ist ähnlich der eines asymmetrischen Kryptosystems: auch hier verfügt ein Benutzer über eine nur ihm bekannte Information, den Signierschlüssel, mit Hilfe dessen er aus einer Nachricht deren sogenannte *Signatur* herstellen kann. Im Unterschied zur eigenhändigen Unterschrift ist also die Signatur nicht nur von der Person, sondern auch von der Nachricht abhängig, so daß diese nicht unerkannt verfälscht werden kann.

Das Gegenstück zum öffentlichen Schlüssel ist hier ein Testschlüssel, den jeder kennen darf und anhand dessen bei Vorlage einer Nachricht und einer (vermeintlichen) Signatur die Korrektheit derselben feststellbar ist.

Analog zum Schlüsselverteilungsproblem für Kryptosysteme sind hier die Testschlüssel gesichert zu verteilen. Insbesondere ist zu beachten, daß bei der Verteilung der Schlüssel eines asymmetrischen Kryptosystems das öffentliche Schlüsselregister sinnvollerweise bereits ein Signatursystem zur „verbindlichen", d.h. vor unerkennbarer Verfälschung geschützten Mitteilung gesuchter Schlüssel verwendet.

Realisierungen von Krypto- und Signatursystemen sind aus der Fachliteratur in großer Zahl bekannt. Bekannteste Vertreter sind hierbei RSA [RSA_78] als Signatursystem und asymmetrisches Kryptosystem sowie DES (data encryption standard, [DES_77]) als symmetrisches Kryptosystem.

Beide Systeme lassen sich ohne große Schwierigkeiten auf jedem PC in Software implementieren, können dann aber nur für schmalbandige Kommunikation verwendet werden und verhindern

während der Verschlüsselung natürlich die sonstige Benutzung des PCs (obere Grenze dürfte das Verschlüsseln mit DES von Telefongesprächen mit 64 kbit/s sein).

Dies mag zwar den Anforderungen geschlossener und mit genügend vielen oder leistungsfähigen PCs ausgestatteter Benutzergruppen genügen; um effizient zu ver- und entschlüsseln oder die für breitbandige Dienste notwendigen Verschlüsselungsraten zu erreichen, müssen die Systeme aber in Hardware implementiert werden. Für beide Systeme stehen Hardwareimplementierungen zur Verfügung, mit denen gegenwärtig RSA 64 kbit/s (bei einer Schlüssellänge von 660 bit, [SeGo_86]) und DES 15 Mbit/s [AT&T_86, Abbr_84] zu verschlüsseln erlaubt, so daß hinsichtlich der Leistung der Einsatz eines Systems wie RSA zur Schlüsselverteilung und Signaturbildung sowie von DES zur Verschlüsselung großer Datenströme möglich ist. Mit dem Masseneinsatz der hardwareimplementierten Kryptosysteme wäre zugleich auch deren Preisgünstigkeit (vermutlich unter DM 1 zusätzliche Produktionskosten je Gerät) garantiert.

Die Sicherheit beider Systeme ist im strengen Sinne nicht bewiesen.

DES ist, wie die meisten schnellen symmetrischen Systeme, ein auf organisiertem Chaos beruhendes System, das allerdings seit seiner Veröffentlichung 1977 in der kryptologischen Fachwelt zahlreichen Versuchen ausgesetzt war, es zu brechen. Zumindest allen veröffentlichten Versuchen hielt es dabei stand, was als Validierung betrachtet werden kann.

Die Sicherheit von RSA beruht im Gegensatz dazu auf (wenn auch teilweise unbewiesenen) Annahmen über den Lösungsaufwand zahlentheoretischer Probleme. Es wird allgemein vermutet, daß das Brechen von RSA, d.h. das Ableiten des privaten aus dem öffentlichen Schlüssel, so schwer ist wie die Gewinnung der Primfaktoren einer gegebenen Zahl. Eine Faktorisierung von Zahlen, die aus sehr großen Primfaktoren zusammengesetzt sind, ist bisher praktisch unmöglich.

Es sei angemerkt, daß sich mit demselben Prinzip wie DES viele weitere symmetrische Kryptosysteme, deren Sicherheit größer ist als die von DES, bilden lassen (z.B. LUCIFER-artige, vgl. [FeNS_75, HeKW_85]) und daß es weniger bekannte asymmetrische Kryptosysteme [GoMi_84, BlGo_85] und Signatursysteme [GoMR_84] gibt, für die bewiesen wurde, daß ihr Brechen so schwer wie Faktorisieren ist. Leider gibt es zur Zeit weder praktikable symmetrische noch irgendwelche asymmetrischen Kryptosysteme, deren Sicherheit ganz ohne unbewiesene Annahmen über den Lösungsaufwand zahlentheoretischer Probleme bewiesen werden kann.

3 Über die Auswahl kryptographischer Verfahren

Um Einschränkungen hinsichtlich der möglichen Kommunikationspartner zu vermeiden [1. Mose 11,1–9], werden in einem verteilten System alle Ende-zu-Ende-Maßnahmen (d.h. alle Ende-zu-Ende-Protokolle) üblicherweise vom Betreiber des Systems standardisiert. Dies gilt auch für das ISDN, dessen Protokolle auf internationaler Ebene von den Postverwaltungen (CCITT) genormt werden, und muß daher auch für die notwendigen Maßnahmen zum Datenschutz und zur Rechtssicherheit gelten.

Zu fordern ist also, daß der Betreiber eines offenen Systems, hinsichtlich des ISDNs also die Deutsche Bundespost, zumindest jeweils ein geeignetes asymmetrisches Kryptosystem (zur Schlüsselverteilung), ein symmetrisches Kryptosystem (zur schnellen Verschlüsselung) sowie ein Signatursystem standardisiert und den möglichen Anbietern von Diensten und Herstellern von Endgeräten zur Verfügung stellt. Besonders wichtig ist dies, weil die Systeme nur dann effizient genug verschlüsseln, wenn sie hardwaremäßig realisiert sind.

Welche Eigenschaften *kryptographische Standards* haben müssen, ergibt sich aus dem in den vorigen Kapiteln Gesagten:

Die Erfüllung der Forderungen aus Kapitel 1 verlangt, daß jeder Benutzer selbst für die Qualität seines Datenschutzes und seiner Rechtssicherheit verantwortlich ist. Um ihm dies zu ermöglichen, müssen die verwendeten und zu standardisierenden Ende-zu-Ende-Maßnahmen möglichst gut sein und der Benutzer sich über die Qualität der Maßnahmen auch sicher sein können.

Dies ist im wesentlichen eine Forderung an die Entwerfer der Maßnahmen, insbesondere der verwendeten kryptographischen Techniken, heißt aber auch, daß jeder Benutzer deren Grad an Sicherheit dem Stand der Kryptographie entsprechend beurteilen (lassen) können muß.

Hieraus folgt wiederum, daß die standardisierten Techniken veröffentlicht werden müssen, denn ein Benutzer (oder auch die kryptologische Fachwelt) kann nur beurteilen und ggf. als unsicher verwerfen, was er kennt.

Nach alledem wäre zu erwarten, daß national wie international die Arbeit an öffentlichen Standards beginnen, ja sogar schon längst abgeschlossen sein müßte.

International und national (durch ISO und DIN) wurde auch versucht, RSA und DES zu normen, doch sind diese Versuche im Begriff, abgebrochen zu werden bzw. bereits abgebrochen (nur an der Normung von Protokollen, die Kryptosysteme *verwenden*, soll noch gearbeitet werden). Lediglich ein Register ist geplant, in das sowohl vollständig veröffentlichte Kryptosysteme als auch solche, deren genaue Beschreibung geheim bleiben soll, aufgenommen werden. Für letztere Klasse von Kryptosystemen enthielte es nur einen Namen und ggf. die für die Verwendung in Protokollen relevante äußere Spezifikation, z.B. „symmetrische Blockchiffre mit 64 Bit Block- und 56 Bit Schlüssellänge". Während bisher mit der Normung auch eine gewisse Aussage über die Güte der Kryptosysteme gegeben war, soll die Aufnahme in das geplante Register hierüber keinerlei Aussage machen.

Statt dessen versuchen den Geheimdiensten nahestehende Institutionen, namentlich die *National Security Agency* (NSA) in den USA und anscheinend auch die *Zentralstelle für das Chiffrierwesen* (ZfCh) in Bonn, die künftigen Anwendungen kryptographischer Techniken möglichst vollständig unter ihre Kontrolle zu bekommen: die NSA bzw. ZfCh wollen in Zukunft auch in nichtstaatlichen und nichtmilitärischen Bereichen indirekt vorschreiben, welche Kryptosysteme verwendet werden.

Zumindest die NSA hat, gedeckt durch einen offiziellen Auftrag der amerikanischen Regierung, den Mangel an guten genormten Kryptosystemen zu ihrem Vorteil genutzt [Kola_85, Horg_86, Riha_87]:

Die NSA möchte einige Kryptosysteme festlegen (bzw. hat dies zum Teil auch schon getan), die allgemeinen Einsatz im privaten Bereich der USA finden sollen, deren genaue Beschreibungen aber geheim bleiben sollen – angeblich, um ein Brechen der Systeme zu erschweren und Gegnern keine guten Algorithmen zu verraten. Die Ver- und Entschlüsselungsalgorithmen würden dazu nur in vor Ausforschung geschützten Chips bzw. Geräten ausgeliefert.

Die Schlüsselgenerierungsalgorithmen sollen sogar völlig bei der NSA verbleiben, die Benutzer der Systeme müssen sich für jede Kommunikationsbeziehung von der NSA Schlüssel zuweisen lassen. Dies ist vermutlich dadurch realisiert, daß die Geräte selbstgewählte Schlüssel mit großer Wahrscheinlichkeit ablehnen. Teilweise wird gesagt, daß Benutzer auch Algorithmen zur Erzeugung von Schlüsseln erhalten können, die damit erzeugten Schlüssel aber schlechter seien als die von der NSA gelieferten [Kola_85]. Letzteres könnte daran liegen, daß für die Schlüsselerzeugungsalgorithmen keine ausforschungssicheren Geräte vorgesehen sind und die NSA sie nicht vollständig verraten möchte, es könnte einfach eine abschreckende Behauptung sein, oder die ausforschungsgeschützten Chips könnten für diese nach den nicht völlig geheimen Algorithmen erzeugten Schlüssel ganz andere, leichter zu brechende Ver- und Entschlüsselungsalgorithmen enthalten. Sicherheitsargumente dafür, die Schlüsselerzeugungsalgorithmen nicht auch in die ausforschungsgeschützten Chips aufzunehmen, gibt es nicht, Leistungs- oder Kostenüberlegungen könnten aber eine Rolle spielen.

Schon die Sicherheitsargumente für die Geheimhaltung der Algorithmen sind sehr zweifelhaft:

Zum einen ist die Wahrscheinlichkeit sehr groß, daß ein Angreifer mit ausreichenden finanziellen oder technischen Mitteln die Algorithmen doch erfährt, entweder durch Spionage oder durch Brechen des Ausforschungsschutzes (die Bewertung der Sicherheit von Geräten ist heutzutage noch viel problematischer als die von Kryptosystemen). Zum anderen verliert man durch die Geheimhaltung den schon erwähnten Vorteil einer Sicherheitsvalidierung durch den heutzutage recht großen öffentlich arbeitenden Teil der kryptologischen Fachwelt, durch die ein Algorithmus mit Schwächen (und nur ein solcher bedürfte ja des zusätzlichen Schutzes durch Geheimhaltung, um ein Brechen zu erschweren) vermutlich ausgeschieden wird, bevor es überhaupt zu seiner Standardisierung kommt. Das Argument, den Gegnern keine guten Algorithmen verraten zu wollen, ist zudem irrelevant, solange es eine genügende Auswahl an guten Algorithmen gibt, wie dies zur Zeit der Fall zu sein scheint (vgl. Kapitel 2).

Es ist natürlich auch denkbar (wie dies auch schon bei DES diskutiert wurde), daß absichtlich ein System gewählt werden soll, das zumindest insoweit Schwächen hat, daß es der NSA auch in dem

Fall, daß sich die Schlüsselzuteilung durch die NSA nicht durchsetzen sollte, noch gestattet, ausgewählte Nachrichten zu entziffern, und das Risiko, daß dies nach einer Weile auch Gegner können, bewußt eingegangen wird (für militärische Geheimnisse sollen andere Systeme verwendet werden), ein öffentliches Bekanntwerden dieses Punktes aber unerwünscht ist.

Wenn natürlich die Schlüssel tatsächlich von der NSA zugewiesen würden, wären solche absichtlichen Schwächen überflüssig: Dann wäre die NSA ohnehin in die einzigartige Lage versetzt, jede für sensitiv gehaltene Nachricht mühelos mitlesen zu können. Ein solches System wäre damit die offizielle Installation eines „Großen Bruders" [Orwe_49].

Inwieweit die ZfCh ihrem amerikanischen Bruder nacheifern wird, ist offiziell nicht bekannt, doch hat sie erreicht, daß das DIN die Normung von DES ersatzlos einstellte und auch in der ISO für einen solchen, alle symmetrischen Kryptosysteme betreffenden Entschluß stimmte.

Ziel dieses Aufsatzes war, zu zeigen, daß

- aus juristischen Gründen (Informationelles Selbstbestimmungsrecht, Wahrung der Rechtssicherheit) wie auch technischen Notwendigkeiten der Einsatz standardisierter kryptographischer Verfahren in den betrachteten offenen Systemen zwingend und
- der Weg der NSA, zu Standards zu gelangen, technisch unpraktikabel und zumindest hinsichtlich offener Systeme mit faktischem Benutzungszwang in der Bundesrepublik Deutschland sogar verfassungswidrig ist.

Unsere Hoffnung ist, daß die Deutsche Bundespost als Systembetreiber sich dieser Sicht anschließt und daraus die Konsequenz zieht, veröffentlichte und validierte Verfahren zu standardisieren. Die erste unserer Hoffnungen scheint erfüllt zu werden: Verantwortliche der Post teilen* diese Meinung. Es ist zu hoffen, daß bald auch die zweite in Erfüllung gehen möge.

Für ihre Diskussionsbereitschaft und Kritik danken wir Holger Bürk, Dr. Klaus Echtle, Prof. Dr. W. Görke, Lothar Krause und Dr. K. Rihaczek.

4 Literatur

Abbr_84 C. R. Abbruscato: Data Encryption Equipment; IEEE Communications Magazine Vol. 22, No. 9, September 1984, Seite 15 bis 21

AT&T_86 AT&T: Einchip-Prozessor zur Verschlüsselung digitaler Signale; Design&Elektronik, Markt& Technik, Ausgabe 21 vom 14. 10. 1986, Seite 8 bis 11

BlGo_85 Manuel Blum, Shafi Goldwasser: An Efficient Probabilistic Public-Key Encryption Scheme Which Hides All Partial Information; Advances in Cryptology, Proceedings of Crypto 84, A Workshop on the Theory and Application of Cryptographic Techniques, August 19-22, 1984, University of California, Santa Barbara, Edited by G. R. Blakley and David Chaum, Lecture Notes in Computer Science LNCS 196, Springer-Verlag Heidelberg, 1985, Seite 289 bis 299

Bund_83 Das Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 – 1 BvR 209/83 u. a.; "DuD, Datenschutz und Datensicherung, Informationsrecht, Kommunikationssysteme", Heft 4, Oktober 1984, Seite 258 bis 281, Vieweg & Sohn, Wiesbaden

DaPr_84 D. W. Davies, W. L. Price: Security for Computer Networks, An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer; John Wiley & Sons, Chichester, New York, 1984

Denn_82 Dorothy E. Denning: Cryptography and Data Security; Addison-Wesley Publishing Company, Reading, Mass.; 1982

* so geäußert am 30. März 1987 in Köln in einem Vortrag von Günter Giller, Bundespostministerium Bonn, anläßlich des 4. Symposiums „Sicherheitsaspekte in Datennetzen" der Gesellschaft für Datenschutz und Datensicherung (GDD)

DES_77 Federal Information Processing Standards Publication 46 (FIPS PUB 46): Specification for the Data Encryption Standard; January 15, 1977

FeNS_75 Horst Feistel, William A. Notz, J. Lynn Smith: Some Cryptographic Techniques for Machine-to-Machine Data Communications; Proceedings of the IEEE Vol. 63, No. 11, November 1975, Seite 1545 bis 1554

GoMi_84 Shafi Goldwasser, Silvio Micali: Probabilistic Encryption; Journal of Computer and System Sciences Vol. 28, 1984, Seite 270 bis 299

GoMR_84 Shafi Goldwasser, Silvio Micali, Ronald L. Rivest: A "Paradoxical" Solution to the Signature Problem; 25th Annual Symposium on Foundations of Computer Science, IEEE Computer Society, October 24-26, 1984, Seite 441 bis 448

HeKW_85 Franz-Peter Heider, Detlef Kraus, Michael Welschenbach: Mathematische Methoden der Kryptoanalyse; DuD-Fachbeiträge 8, Vieweg, Braunschweig, 1985

Horg_85 John Horgan: Thwarting the information thieves; IEEE Spectrum Vol. 22, Nu. 7, July 1985, Seite 30 bis 41

Horg_86 John Horgan: NSA explains encryption program to IEEE Privacy Subcommittee; The Institute, IEEE, Vol. 10, Nu. 9, September 1986, Seite 2

Hors_85 Patrick Horster: Kryptologie; Reihe Informatik/47, Herausgegeben von K. H. Böhling, U. Kulisch, H. Maurer, Bibliographisches Institut, Mannheim, 1985

IM46_87 Europe's leaky commercial data; I'M, Information Market, published by Directorate General XIII, Commission of the European Communities; Issue 46, Dec. 1986 – Feb. 1987, Seite 9

Kola_85 Gina Kolata: NSA to Provide Secret Codes; Science Vol. 230, October 1985, Seite 45 bis 46

KuRo_86 Herbert Kubicek, Arno Rolf: Mikropolis; Mit Computernetzen in die "Informationsgesellschaft"; 2. Auflage, VSA-Verlag, Hamburg 1986

Orwe_49 George Orwell: 1984

PfPW_86 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Technischer Datenschutz in diensteintegrierenden Digitalnetzen – Warum und wie?, "DuD, Datenschutz und Datensicherung, Informationsrecht, Kommunikationssysteme", Vieweg & Sohn, Wiesbaden, Heft 3, Juni 1986, Seite 178 bis 191

PoKl_78 G. J. Popek, C. S. Kline: Issues in Kernel Design; Operating Systems, An Advanced Course, Edited by R. Bayer, R. M. Graham, G. Seegmüller; Lecture Notes in Computer Science LNCS 60, 1978; Nachgedruckt als Springer Study Edition, 1979; Springer-Verlag, Heidelberg, Seite 209 bis 227

PPW_87 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen; "Computer und Recht (CR)", Verlag Dr. Otto Schmidt KG, Köln, 1987

Riha_85 Karl Rihaczek: Der Stand von OSIS; DuD, Datenschutz und Datensicherung, Informationsrecht, Kommunikationssysteme, Friedr. Vieweg & Sohn, Braunschweig, Heft 4, August 1985, Seite 213 bis 217

Riha_87 Karl Rihaczek: Datensicherheit amerikanisch; DuD Datenschutz und Datensicherung, Recht und Sicherheit der Informations- und Kommunikationssysteme, Friedr. Vieweg & Sohn Verlagsgesellschaft Braunschweig, Heft 5, Mai 1987, Seite 240 bis 245

Rose_85 K. H. Rosenbrock: ISDN – Die folgerichtige Weiterentwicklung des digitalisierten Fernsprechnetzes für das künftige Dienstleistungsangebot der Deutschen Bundespost; GI/NTG-Fachtagung "Kommunikation in Verteilten Systemen – Anwendungen, Betrieb und Grundlagen –", 11.-15. März 1985, Tagungsband 1, D. Heger, G. Krüger, O. Spaniol, W. Zorn (Hrsg.), Informatik-Fachberichte IFB 95, Springer-Verlag Heidelberg, Seite 202 bis 221

RSA_78 R. L. Rivest, A. Shamir, L. Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems; Communications of the ACM Vol. 21, No. 2, February 1978, Seite 120 bis 126

Schö_84 Helmut Schön: Die Deutsche Bundespost auf ihrem Weg zum ISDN; The Deutsche Bundespost on its Way towards the ISDN; Zeitschrift für das Post- und Fernmeldewesen Heft 6 vom 27. Juni 1984

ScSc_84 Christian Schwarz-Schilling (ed.): Konzept der Deutschen Bundespost zur Weiterentwicklung der Fernmeldeinfrastruktur; Herausgeber: Der Bundesminister für das Post- und Fernmeldewesen, Stab 202, Bonn, 1984

ScSc_86 Christian Schwarz-Schilling (ed.): Mittelfristiges Programm für den Ausbau der technischen Kommunikationssysteme; Herausgeber: Der Bundesminister für das Post- und Fernmeldewesen, Bonn, 1986

ScS1_84 Christian Schwarz-Schilling (ed.): ISDN – die Antwort der Deutschen Bundespost auf die Anforderungen der Telekommunikation von morgen; Herausgeber: Der Bundesminister für das Post- und Fernmeldewesen, Bonn, 1984

SeGo_86 Holger Sedlak, Ulrich Golze: Ein Public-Key-Code Kryptographie-Prozessor; Informationstechnik it, 28. Jahrgang, Heft 3/1986, Seite 157 bis 161

Thom_84 Ken Thompson: Reflections on Trusting Trust; Communications of the ACM Vol. 27, No. 8, August 1984, Seite 761 bis 763

TuCh_85 Murray Turoff, Sanjit Chinai: An Electronic Information Marketplace; Computer Networks and ISDN Systems Vol. 9, Nu. 2, February 1985, Seite 79 bis 90