Dr. Michael Hortmann, Universität Bremen, MichaelH@informatik.uni-Bremen.de

Datensicherheit durch Kryptographie

Die rechnergestützte Übermittlung kritischer Daten in Wirtschaft und Behörden, aber auch im privaten und medizinischen Bereich über öffentliche Netze war bisher kaum möglich, da kein Schutz gegen Verfälschung und unberechtigte Einsichtnahme bestand.

Aber nicht nur kommunikativ "fließende", sondern auch "statische" Daten auf materiellen Trägern wie Magnetbändern, Disketten, Festplatten, PCMCIA-Karten etc. sind häufig höchst vertraulich, sollten daher für Unbefugte nicht einsehbar und ggf. mit einem Urhebernachweis versehbar sein.

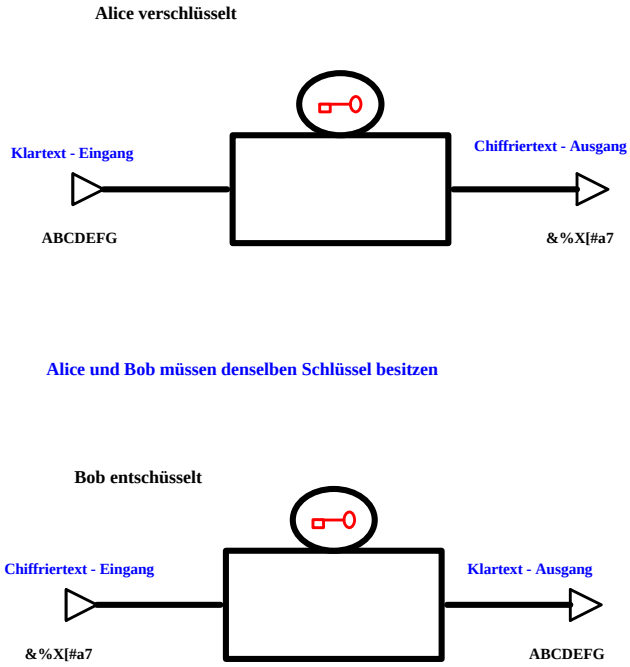
Moderne kryptographische Verfahren ermöglichen es heute jedermann, Daten sicher zu kommunizieren, aufzubewahren und vor Verfälschung zu sichern. Zusätzlich wird es auch möglich, elektronische Dokumente mit Unterschriften zu versehen und ihnen somit Urkundencharakter zu verleihen. Die Anwendung derartiger Methoden wird bald alltäglich sein und unsere öffentliche, wirtschaftliche und finanzielle Infrastruktur wesentlich mittragen. Im folgenden geben wir eine Einführung in die dazu notwendigen Methoden und Infrastrukturen, aber versuchen auch, Grenzen und Gefährdungen aufzuzeigen.

Es ist einleuchtend, daß solche neuen Möglichkeiten Konsequenzen für unser Rechtssystem nach sich ziehen. Konstrukte wie Unterschriften und Urkunden müssen dort eingebettet sein, wenn sie Rechtsverbindlichkeit erlangen sollen; entsprechende Gesetze und Verordnungen zur "Digitalen Signatur" gibt es bereits. Aber auch vor einer endgültigen gesetzlichen Regelung erweist sich der Gebrauch der entsprechenden Methoden als notwendig und sinnvoll.

Der technisch mögliche Schutz vor "unberechtigter Einsichtnahme" ist ebenfalls nicht unproblematisch. Im Gegenzug ist die Frage zu stellen, wie die "berechtigte Einsichtnahme" sicherzustellen ist. Dies beginnt beim Schlüsselmanagement für den Zugang zu den eigenen Daten. Es wäre unangenehm bis katastrophal, wenn durch verlorengegangene Zugangsschlüssel Datenverluste eintreten. Unternehmen und Behörden müssen sich aber auch dagegen schützen, daß unzugängliche oder gar unbeobachtbare Datenströme nach außen und innen neue Gefährdungen aufwerfen. Außerdem gibt es natürlich auch für die Sicherheitsbehörden Probleme, wenn in Zukunft alle digitale Kommunikation "unknackbar" verschlüsselt sein sollte. Welche Lösungen können hier öffentlichem, privatem und wirtschaftlichem Interesse gemeinsam gerecht werden?

Kryptologische Algorithmen:

Klassische Chiffriermaschine



Das obige Bild beschreibt eine "klassische Chiffriermaschine". Sie besitzt einen Dateneingang, einen Datenausgang sowie einen Schlüsseleingang. An diesem simplen Konzept können schon viele Probleme der Verschlüsselungstheorie und -praxis dargelegt werden.

Wesentlich ist, daß Sender und Empfänger der Daten bei der "klassischen Maschine" über denselben Schlüssel verfügen müssen. Ein Qualitätsmerkmal einer klassischen Maschine, die in Hardware materiell oder nur als Softwarealgorithmus repräsentiert sein kann, ist die Schlüssellänge. So benutzt der Standardalgorithmus **DES**, der z.B. in Geldausgabeautomaten verwendet wird, 56 Bit Schlüssellänge. Einen derartigen Schlüssel könnte man darstellen als Folge von 8 Ascii-Zeichen, Folge von 16 Hex-Ziffern, oder Folge von 56 Binärziffern (Bits), z.B.

```
a&/%.B6@
61 26 2f 25 2e 42 36 40
110 0001  010 0110  010 1111  010 0101  010 1110  100 0010  011 1110  100 0000
```

was in verschiedener Kodierung dasselbe bedeutet; wobei man auch bei einem so relativ kurzen Schlüssel sieht, daß man ihn sich nur schwer merken kann, ein Problem für ein sicheres *Schlüsselmanagement*.

Die Schlüssellänge ist deshalb wesentlich, damit der richtige Schlüssel nicht durch Ausprobieren aller Möglichkeiten gefunden werden kann; bei einer Schlüssellänge von16 Bit wären

beispielsweise 65536 Möglichkeiten zu testen, was von einer Maschine offenbar schnell durchgeführt werden kann. Erschwerend kommt beim Durchprobieren hinzu, daß i.a. das Ergebnis des Dechiffrierens mit einem Testschlüssel auf Sinnhaftigkeit untersucht werden muß, was je nach der Natur der Klartextdaten für eine Maschine bzw. ein Programm schwierig sein könnte, es sei denn, man kenne bereits einen Teil des Klartexts.

Untersuchungen speziell zum DES mit 56 Bit Schlüssellänge haben gezeigt, daß Spezialhardware zur systematischen Schlüsselsuche zu vertretbaren (stets sinkenden) Preisen gebaut werden kann.

Man kann die effektive Schlüssellänge des DES durch den sogenannten **Triple-DES** Modus auf 112 Bit verdoppeln, indem man 2 unabhängige Schlüssel wählt. Die Triple-DES-Verschlüsselung erfolgt dann, indem mit dem ersten eine Verschlüsselungsoperation durchgeführt wird, dann mit dem zweiten eine Entschlüsselungsoperation, schließlich mit dem ersten wieder eine Verschlüsselungsoperation. Für 112 Bit lange Schlüssel gibt es dann keine Möglichkeit der systematischen Schlüsselsuche mehr.

Während die *Komplexität* des Schlüssels für eine klassische Chiffriermaschine wichtig ist, darf aber auch die eigentliche Verschlüsselung keine Schwächen aufweisen. Man kann dies vergleichen mit einem Schloß, bei dem ja nicht nur der Schlüssel schwierig nachzumachen sein darf; das Schloß selbst muß auch stark sein. (Die Analogie trägt noch weiter: der zu schützende Raum darf keine weiteren, schwächer geschützten Eingänge haben.)

Kryptographische Qualität:
In diesem Sinne ist DES ein sehr starker Algorithmus, der seit seiner Spezifikation in den 70er Jahren sehr genau untersucht worden ist. Es wurde kritisiert, daß nicht alle Designkriterien veröffentlicht wurden und das Verfahren deshalb mögliche Hintertüren besitzt. Der Grund für diese Zurückhaltung lag aber darin, daß die beim Design beteiligten Institutionen nicht ihr seinerzeit überlegenes Wissen über den Entwurf derartiger Kryptoalgorithmen preisgeben wollten. Auch die Beschränkung auf 56 Bit Schlüssellänge war wohl weniger darin begründet, daß sie der amerikanischen National Security Agency gerade noch brechbar erschien, als darin, daß die Implementation des Algorithmus in Hardware vorrangig war und damalige integrierte Schaltkreise größere Schlüssellängen nicht verkrafteten.

Dies führt zur Frage, wie für Außenstehende die Qualität eines Kryptoalgorithmus überhaupt beurteilbar ist. Ein wichtiges Merkmal ist die Öffentlichkeit des Verfahrens und nach Möglichkeit auch der Designkriterien. Je länger ein solches Verfahren dann öffentlich analysiert wurde, ohne wesentliche Schwächen aufzudecken, umso vertrauenswürdiger stellt es sich dar. Im Idealfall gäbe es mathematische Beweise für die Sicherheit; für die wichtigen Anwendungen ist dies heutzutage nicht der Fall. Alternativ könnte man der Institution, die den Algorithmus zur Verfügung stellt, das Qualtitätsurteil überlassen. Dies führt aber leicht zu Interessenkonflikten. Außerdem könnte man in diesem Fall auch Zweifel an der Qualität der kritischen Kryptoanalyse des offerierten Verfahrens haben. Während in der akademischen und sonstigen öffentlichen "Cryptographic Community" weltweit einige tausend Kryptologen tätig sind und sich solchen Problemen widmen, wird mit Ausnahme der amerikanischen NSA keine Firma oder sonstige hiesige Institution eine derartige "Mannschaftsstärke" aufweisen.

An der ETH Zürich wurde Ende der achtziger Jahre der IDEA-Algorithmus als potentieller

"Nachfolger" des DES entwickelt mit einer Schlüssellänge von 128 Bit; die öffentliche Kryptanalyse hat ihn als stark validiert. Während DES/3DES frei benutzt werden kann, besitzt die Firma Ascom-Tech für kommerzielle Anwendungen von IDEA Lizenzrechte (15$ proImplementation, bzw. weniger bei größerer Stückzahl).

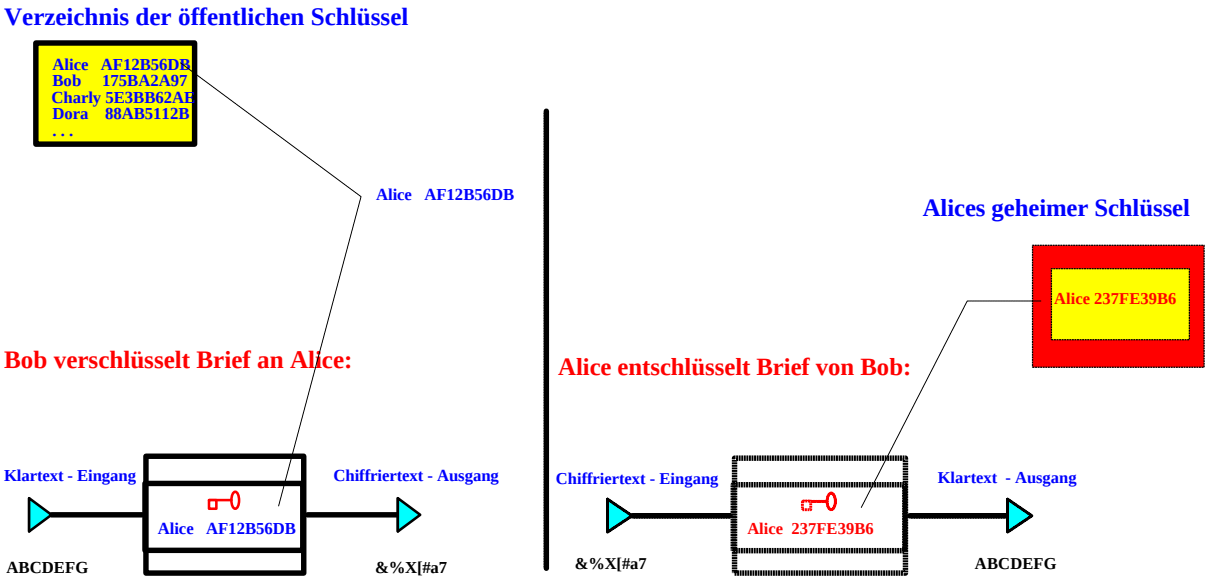
Die "klassische Chiffriermaschine" ist dadurch charakterisiert, daß Chiffrierschlüssel und Dechiffrierschlüssel identisch sind. Man wird diese Klasse von Algorithmen dort einsetzen, wo die Menge der beteiligten Kommunikationspartner relativ klein ist, so daß nicht allzuviele Schlüssel im Spiel sind, beispielsweise zum Schutz einer festen Kommunikationsstrecke (link encryption).

Grundsätzlich gilt:
Die Sicherheit eines Chiffrieralgorithmus darf nur von der Geheimhaltung des Schlüssels abhängen, nicht von der Geheimhaltung des Algorithmus, über den "der Gegner" im Zweifelsfall doch verfügt. Der Algorithmus sollte jahrelanger öffentlicher Kryptanalyse standgehalten haben. Dem Endanwender sollte eine unabhängige Institution garantieren, daß die von ihm ins Auge gefaßte Implementation des Algorithmus korrekt und frei von Nebeneffekten ist; nach Möglichkeit sollte er bei einer Softwareimplementation die Quelltexte selbst oder durch einen unabhängigen Gutachter überprüfen können.

Public Key Kryptographie

Wenn es eine unübersehbare Anzahl von Teilnehmern eines zu sichernden Kommunikationssystems gibt, reichen Methoden, die sich aus der klassischen Chiffriermaschine ableiten, nicht mehr aus. Entweder müßten sich dann mehrere Benutzer einen Schlüssel teilen, was natürlich unsicher wäre, oder es müßten Schlüsselverteilungszentralen geschaffen werden, die über "Master-Keys" verfügen und die Kommunikationsschlüssel der Benutzer kennen, was nicht unbedingt vertrauenerweckend ist; oder aber die Anzahl der Schlüssel wächst in unübersichtliche und Unsicherheit schaffende Größenordnungen. Die Idee der **Public Key Kryptographie**, die Mitte der 70er Jahre von Diffie und Hellman in den USA publiziert wurde, schafft hier Abhilfe. Sie geht davon aus, daß die klassische Chiffriermaschine derart abgeändert werden kann, daß Chiffrier- und Dechiffrierschlüssel verschieden sind, und daß letzterer aus ersterem nicht errechenbar ist.
In einem solchen Falle lassen sich die Chiffrierschlüssel sämtlicher Teilnehmer in ein öffentliches Verzeichnis schreiben, vergleichbar mit einem Telefonbuch (ebenso sind private "Notizbücher" möglich, in denen jeder die öffentlichen Schlüssel seiner Kommunikationspartner vorhält), während jeder Benutzer seien eigenen privaten Dechiffrierschlüssel geheimhält und wohl verwahrt.

Im folgenden Diagramm wird ein Public Key Chiffrier/Dechiffriervorgang illustriert:
Links möchte Bob mit Alice vertraulich kommunizieren, lädt Alices Chiffrierschlüssel (=öffentlicher Schlüssel) aus dem Schlüsselverzeichnis in die Chiffriermaschine und versendet den Chiffriertext über ein öffentliches Netz.



Rechterhand erhält Alice den verschlüsselten Text, lädt ihren Dechiffrierschlüssel (=geheimer, privater Schlüssel) aus einem geschützten Bereich in die Maschine (am besten wäre er bereits unauslesbar darin enthalten) und stellt somit den Klartext wieder her.
Da nur Alice über den richtigen geheimen Schlüssel verfügt, kann nur sie die Dechiffrierung vornehmen. Andererseits kann jeder Systemteilnehmer ihr vertrauliche Botschaften schicken.

Für das *Schlüsselmanagement* stellen sich jetzt folgende Fragen:

- Wer erzeugt die Schlüssel?
- Wodurch ist sichergestellt, daß ein öffentlicher Schlüssel wirklich zu dem intendierten Empfänger gehört?

Letzteres ist bedeutsam, damit die vertrauliche Post nicht für den falschen Empfänger lesbar wird. Dies soll im Abschnitt über *Zertifizierung* diskutiert werden.

Umgekehrt kann Alice ein Dokument mit einer *Digitalen Signatur* versehen:
Indem sie das zu signierende Dokument mit ihrem geheimen Schlüssel "chiffriert", entsteht eine Datei, die von jemandem, der die Unterschrift prüfen will, mit ihrem öffentlichen Schlüssel "dechiffriert" wird: wird hierbei der Klartext rekonstruiert, ist nachgewiesen, daß die "Signieroperation" vom Besitzer des geheimen Schlüssels, also Alice, vorgenommen wurde.

Auf diese Weise wird es möglich, Zeugnisse, Berechtigungsnachweise, Pässe, etc. per Datennetz zu versenden oder auf einfachen Datenträgern vorzuhalten.
Interessant an der Ideengeschichte ist die Tatsache, daß zunächst kein Verfahren bekannt war, das diese Trennung von Chiffrier- und Dechiffrierschlüssel ermöglichte. Erst zwei Jahre später entwickelten Rivest, Shamir und Adleman das nach Ihnen benannte RSA Verfahren, die auch heute noch bedeutsamste Realisierung eines Public Key Verfahrens.

RSA
Dieses Verfahren benutzt zahlentheoretische Operationen zur Chiffrierung/Dechiffrierung, bzw. Signaturerzeugung/Signaturprüfung. Seine Sicherheit, insbesondere die Tatsache, daß

der geheime Schlüssel nicht aus dem öffentlichen rekonstruierbar ist, beruht darauf, daß ein Produkt zweier "zufälliger" mehr als 100-stelliger Primzahlen auch bei Einsatz aller auch in absehbarer Zukunft verfügbarer Rechenleistung nicht mehr in diese Faktoren zerlegbar ist. Es läßt sich recht zuverlässig abschätzen, wie groß die Zahlen sein müssen, um Sicherheit für 20 Jahre zu gewährleisten.
Sicherheit für 5 Jahre bieten Schlüssel von 768 Bit Länge; für Anwendungen bei Zertifizierungsinstanzen oder zur Kontrolle nuklearer Waffensysteme wird man dagegen Schlüssel von 1024 oder 2048 Bit Länge wählen.

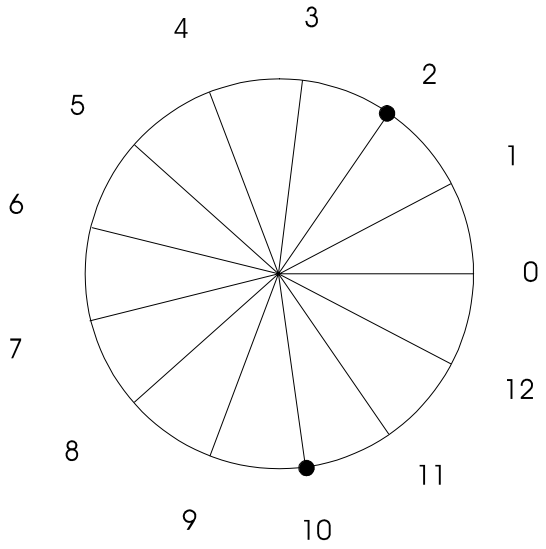
Die Sicherheit des RSA-Verfahrens wird seit 20 Jahren intensiv "beforscht"; es haben sich keine wesentlichen Schwächen ergeben. Trotzdem bleibt ein "Restrisiko": Es gibt keinen mathematischen Beweis, daß es nicht bisher unbekannte Algorithmen gibt, die es möglich machen, den geheimen Schlüssel letztlich doch auszurechnen. Bisher ist kein Public Key Verfahren und auch keine klassische Chiffriermaschine bekannt, bei der dieses Restrisiko nicht bestünde.

Bei der Schlüsselerzeugung für RSA werden zwei "zufällige" Primzahlen von mindestens 384 Bit Länge benötigt. Diese können auch auf einem PC leicht erzeugt werden, jedoch ist die Qualität des dazu notwendigen "Zufallsgenerators" eine kritische Komponente. Gelänge es einem Angreifer, diesen so zu manipulieren, oder sonstwie zu erreichen, daß seine Outputs für ihn vorhersagbar wären, so könnte er später den geheimen Schlüssel errechnen. (Es ist gelungen den Zufallsgenerator des Netscape Browsers zur Erzeugung sogenannter Session-Keys für das SSL-Protokoll vorherzusagen; dieser Fehler wurde inzwischen repariert). Man sieht, daß viele Komponenten bei der Sicherheit eines kryptographischen Systems zusammenwirken müssen.
Das Produkt der beiden Primzahlen dient als öffentlicher Schlüssel; eine weitere Zahl von mindestens 768 Bit Länge, die nur bei Kenntnis dieser Primzahlen errechenbar ist, dient als geheimer Schlüssel.

Andere Public Key Verfahren

Grundlage des RSA Verfahrens war die mathematische Tatsache, daß hinreichend große Primzahlen zwar leicht zu erzeugen und zu multiplizieren sind, die entsprechende Zerlegung des Produkts in seine Faktoren aber praktisch unmöglich ist. (Theoretisch haben wir auf der Schule gelernt, daß jede Zahl eindeutig in ihre Primfaktoren zerfällt). In der Mathematik sind einige andere Probleme bekannt, bei denen Rechnungen in einer Richtung leicht, in der Rückrichtung aber praktisch unmöglich durchführbar sind, falls man nicht über gewisse Zusatzinformationen, die dann als geheimer Schlüssel dienen können, verfügt. Solche Probleme können dann zur Begründung von Public Key Systemen eingesetzt werden und somit Möglichkeiten der vertraulichen Datenübermittlung für beliebig große Teilnehmerkreise und der digitalen Signatur bieten.

Eine besonders wichtige Problemklasse in diesem Zusammenhang ist das sogenannte "Diskrete Logarithmus Problem", auf dem Systeme wie Diffie/Hellman und ElGamal basieren:



Der obige Kreis ist in 13 Teile geteilt. Durch wiederholte Verdoppelung des zwischen 0 und 2 liegenden Winkels werden alle von 0 verschiedenen Punkte erreicht. Logarithmus Problem: Wie oft muß man den Winkel verdoppeln, um den Punkt 10 zu erreichen? Man findet das nur durch Ausprobieren heraus: 2 - 4 - 8 - 3 - 6 - 12 - 11 - 9 - 5 - 10, also 9 mal. Wäre der Kreis statt in 13 Teile in 200-stellig viele Teile zerlegt worden, so ließe sich das entsprechende Problem weder durch Ausprobieren noch durch sonstige den Mathematikern bekannte Methoden praktisch lösen. Andererseits ist die "Vorwärtsrechnung", den Winkel derartig oft zu verdoppeln, effektiv durchführbar und erfordert in etwa nur soviele Schritte, wie die "Verdoppelungszahl" Stellen besitzt.

Wählt man statt Kreisen wie in obiger Diskussion komplexere Objekte, sogenannte "elliptische Kurven", so vereinfachen sich sogar die notwendigen Rechnungen für dieselbe Sicherheitsstufe; solche Systeme eignen sich zur Implementation auf kryptographischen Chipkarten; ein Ansatz, den man insbesondere auch bei der Firma Siemens verfolgt.

Hybride Verfahren

Public Key Verschlüsselungs- und Signaturoperationen sind um einen Faktor 1000 aufwendiger und daher (in Software) langsamer als "klassische Chiffrieralgorithmen" wie DES oder IDEA. Zum Verschlüsseln geht man deshalb in der Praxis so vor: Mit Hilfe eines kryptographisch sicheren Zufallsgenerators wird ein "Sitzungs-Schlüssel" für einen klassischen Algorithmus erzeugt. Nur dieser Sitzungsschlüssel wird Public-Key verschlüsselt und vornweg übermittelt, die eigentlichen Daten dann klassisch verschlüsselt. Auf diese Weise erhält man den Vorteil des einfacheren Schlüsselmanagements des Public Key Verfahrens und die Geschwindigkeit des klassischen. Andererseits sind jetzt natürlich mehr Systemkomponenten im Spiel, und jede Kette ist nur so stark wie das schwächste Glied.

Auch für die Signatur wird ein entsprechender Trick benutzt: mittels einer *kryptographischen Hashfunktion* werden die zu signierenden Daten auf beispielsweise 128 Bit komprimiert. Dies muß und kann so geschehen, daß es rechnerisch nicht möglich ist, andere Ausgangsdaten zu finden, die denselben "Hashwert" liefern. Dadurch wird erreicht, daß genausogut nur dieser Hashwert signiert werden kann, anstelle der Gesamtdatenmenge. Sichere Hashalgorithmen arbeiten genauso schnell wie klassische Chiffrieralgorithmen, (sind sogar häufig von diesen

abgeleitet); die Public Key Signieroperation wirkt nur auf eine kleine Datenmenge, so daß insgesamt der gesamte Signiervorgang sehr schnell arbeitet. Allerdings kommt auch hier wieder eine zusätzliche Komponente, die Hashfunktion, ins Spiel, die kryptographisch sicher und auch korrekt implementiert sein muß. Wichtige Hashalgorithmen sind MD5 (entwickelt von R. Rivest) und der US-Standard SHA.

Schlüsselmanagement

Zum Schlüsselmanagement gehören sichere Erzeugung , Transport, Aufbewahrung, Gebrauch, Backup, Vernichtung, Revozierung kryptographischer Schlüssel. Wenn wir in Zukunft solche Schlüssel für rechtsverbindliche Signaturen einsetzen, kann es durchaus vernünftig sein, sie in offiziell zertifizierten und lizensierten *Trust Centern* erzeugen zu lassen, wo in professioneller Weise eine sichere Umgebung und kryptographische Qualität garantiert wird.

Schlüssel-Zertifizierung

Wenn man beispielsweise eine von der Universität Bremen digital signierte Promotionsurkunde prüfen will, muß der entsprechende öffentliche Signierschlüssel der Universität bekannt sein. Für öffentliche Schlüsselverzeichnisse muß sichergestellt werden, daß die dort vorgehaltenen Schlüssel auch authentisch sind. Dies kann aber ohne besondere Sicherheitsanforderungen an den Betreiber des Schlüsselverzeichnisses garantiert werden. Es genügt nämlich, wenn die Zuordnung Name - Schlüssel ihrerseits die digitale Unterschrift einer Zertifizierungsinstanz trägt, der wir für diesen Fall vertrauen. Solche Zuordnungen samt weiteren Informationen und zusätzlicher Unterschrift einer Zertifizierungsinstanz heißen Zertifikate, im Schlüsselverzeichnis werden also Zertifikate gespeichert. Indem sich Zertifizierungsinstanzen gegenseitig oder hierarchisch geordnet zertifizieren, wird es möglich, öffentliche Schlüssel einer "fremden" Person oder Institution zu verifizieren.

Ein wichtiger Standard für den Umgang mit Zertifikaten und Zertifizierungshierarchien ist ISO X.509. Weitere Forderungen an *Trust Center* als Zertifizierungsinstanzen für rechtsverbindliche Signaturschlüssel beinhaltet das im Referentenentwurf vorliegende *Digitale Signaturgesetz.* In der zugehörigen *Elektronischen Unterschriftsverordnung, §126a Abs. 2 BGB* wird auf die Sicherheit der technischen Verfahren, Details der Beantragung, Ausstellung, Inhalt, Gültigkeitsdauer, Haftungsbeschränkungen, Sperrung und Widerruf von Zertifikaten, Zulassung von Zertifizierungsinstanzen und Anerkennung ausländischer Signaturverfahren eingegangen.

Schlüssel-Hinterlegung

Die eigenen privaten kryptographischen Schlüssel müssen einerseits geheim bleiben, dürfen aber auch nicht verlorengehen. Man könnte sie also auf verschiedenen Datenträgern in Schließfächern verschiedener Banken oder bei Notaren deponieren. Sinnvoller wäre es, bei so immateriellen Objekten wie kryptographischen Schlüsseln systemimmanenter vorzugehen. Banken und Notare werden in Zukunft Treuhanddienste für digitale Dokumente anbieten; wesentliche geldwerte Objekte werden in Zukunft nur noch in dieser Form vorliegen. Das zu schützende Dokument kann jetzt mit Hilfe spezieller Algorithmen, sogenannter

Schwellenschemata, zerlegt werden, beispielsweise in 3 Teile, die bei verschiedenen Treuhändern (verschlüsselt verschickt per Email) hinterlegt werden. Der Benutzer kann, wenn es nötig wird, seine Information mit Hilfe der bei zwei Treuhändern hinterlegten Teile rekonstruieren, d.h. eine Hinterlegungsinstanz darf ausfallen. Kein Treuhänder kann aus der nur bei ihm hinterlegten Teilinformation irgendein Wissen über das Originaldokument ableiten.

Wenn in Zukunft sämtliche digitale Kommunikation nur noch verschlüsselt abläuft, bleibt die Frage: wie kann staatlich legitimierte Überwachung von Kommunikation dann noch stattfinden?
Zu verlangen, daß jeder seine Schlüssel a priori an die Polizei oder eine andere Behörde herausrückt, dürfte politisch nicht durchsetzbar sein. Verschlüsselte Kommunikation überhaupt zu verbieten (Frankreich, Rußland), ist aber technisch nicht durchsetzbar (*Steganographie*). Es wird daher für ein *Kryptogesetz* Kompromißvorschläge geben, wie bei der sogenannten *Clipper Initiative* in den USA. Beispielsweise könnten nach der Erzeugung der eines Schlüsselpaars zur sicheren Kommunikation bei einer zentralen Instanz Teilschlüssel an zwei Treuhandinstitutionen abgegeben werden. Bei einer genehmigten Abhöraktion wird sich der "Bedarfsträger" gegenüber diesen Treuhändern legitimieren, die Herausgabe der Teilschlüssel erreichen und so die Abhörmaßnahme durchführen können.

An einem solchen Szenario wäre folgendes zu verbessern:
Es muß und kann gewährleistet werden, daß die ausgehändigten Schlüssel nur ein bestimmtes "Zeitfenster" für das Abhören ermöglichen.
Eine zentrale Erzeugung der Schlüssel sollte nicht erzwungen werden. Der Benutzer sollte den Treuhändern auch Teile selbsterzeugter Schlüssel übergeben können. Dies kann in vertrauenswürdiger Weise geschehen (*faire Kryptosysteme*).
Die Treuhandinstitutionen dürfen nicht ausschließlich der Exekutive unterstehen.

Steganographie

Es handelt sich um verschiedene algorithmische Verfahren, um verschlüsselte Informationen in digitalisierten Analogdaten, also Bild oder Tondaten, so zu verstecken, daß jemand, der nicht über den Dechiffrierschlüssel verfügt, gar nicht feststellen kann, daß diese Information überhaupt vorhanden ist. Mit der allgemeinen Verfügbarkeit solcher Methoden wird ein Verbot "nicht zugelassener Kryptoverfahren" sinnlos, da man nicht den intendierten Gegner, also organisierte Kriminalität, gegnerische Geheimdienste, etc. gar nicht treffen würde.

Ein Gegenargument ist hier, daß man zwar die geschützte Kommunikation krimineller Elemente untereinander so nicht verhindern könne, wohl aber ihre Kontakte mit der legalen Außenwelt, beispielsweise beim Buchen von Mietwagen, Hotels, etc.

US-amerikanische Exportpolitik:

Die amerikanische Computer- und Softwareindustrie war lange Zeit führend in Entwicklung und Realisierung moderner computergestützter Kryptoverfahren. Da der Export entsprechender "starker" Hardware und Software (auch nach Westeuropa) jedoch unter Waffenkontrollgesetze fällt, durften bisher nur "abgespeckte" Versionen exportiert werden, was der Wissenschaft und Industrie in Europa ein Aufholen ermöglichte. Beispiel für

unsichere Exportsoftware: die Firma Netscape verwendet in ihrer Client und Server Software zum Aufbau sicherer Datenverbindungen im World Wide Web den an sich starken Algorithmus RC-4. Für Exportversionen wurden hierfür aber die Schlüssellängen auf 40 Bit reduziert, ein für uns sicher nicht akzeptables Verfahren. Einige Pariser Studenten haben kürzlich demonstriert, wie relativ einfach hier eine erschöpfende Schlüsselsuche durchführbar ist.

Spezielle Public Key Implementationen

PEM (Privacy Enhanced Mail) wurde als Internet Standard für sichere Email entwickelt und in den Internet Standard Dokumenten RFC 1421-1424 spezifiziert. PEM benutzt RSA und DES, sowie im wesentlichen X.509 für das Schlüsselmanagement. Der praktische Wert ist dadurch eingeschränkt, daß es eine globale hierarchische Zertifizierungshierarchie voraussetzt, die längst noch nicht existiert. Die Implementation **SecuDE** der GMD ist z.Zt. frei verfügbar und kann zu Testzwecken eingesetzt werden. Für den zu schützenden zukünftigen Datenverkehr für Abrechnungsdaten zwischen Krankenhäusern und Krankenkassen wird die PEM Spezifikation vorgeschlagen.

PGP (Pretty Good Privacy) ist ein Public Domain Softwarepaket, das auf praktisch allen Hardware/Betriebssystemplattformen lauffähig ist. Es ist ein hybrides System auf der Basis RSA/IDEA, mit einem ausgefeilten dezentralen Schlüsselmanagement, welches es sofort einsetzbar macht. Wegen der IDEA-Komponente sind bei kommerziellem Einsatz Lizenzgebühren an die Schweizer Firma Ascom-Tech zu zahlen (bis zu 15$/Maschine).
PGP hat sich als de facto Standard im Internet durchgesetzt, da es keine externen Infrastrukturen voraussetzt. Der Source Code liegt vollständig vor und wird seit Jahren im Internet kritisch diskutiert (sci.crypt, alt.security.pgp). Kryptographische Qualität und Software Engineering sind ausgezeichnet, Source Code und vorkompilierte Versionen durch digitale Signaturen der Leiter der Entwicklungsteams gegen Manipulationen geschützt. PGP wird von den Landesdatenschutzbehörden empfohlen und in Pilotprojekten in den Landesfinanzverwaltungen in Baden Württemberg, Niedersachsen und Bremen eingesetzt. Vom Autor dieses Artikels stammt eine Version, die Blockchiffrierkomponente IDEA gegen den lizenzfreien 3DES austauscht.

Kryptographische Chipkarten

Wenn es um das sichere Aufbewahren geheimer Schlüssel geht, sind reine Softwaresysteme gefährdet, insbesondere vernetzte Rechner. Dabei werden Schlüssel ihrerseits verschlüsselt im Dateisystem verwahrt, aber im Arbeitsspeicher des Rechners kurzzeitig im Klartext benutzt, nachdem durch Paßworteingabe die Entschlüsselung des Schlüssels freigegeben wurde. Sehen wir von elektromagnetischen Abstrahlungen des Rechners ab, so sind Angriffe gegen den geheimen Schlüssel durch Viren, trojanische Pferde, den Systemverwalter, oder andere möglich.

In einer kryptographischen Chipkarte ist der geheime Schlüssel des Benutzers unauslesbar eingeschrieben und verläßt auch bei Entschlüsselungs- und Signieroperationen nie diese gesicherte Umgebung. Dies ist ein wichtiges Sicherheitsmerkmal. Leider haben solche Karten

kein eigenes manuelles Input und Displaysystem. Die Karte unterschreibt also blind, was der Rechner ihr zur Unterschrift reicht: dies kann bei einem manipulierten Rechner durchaus etwas anderes sein als das, was der Benutzer eingegeben hat oder auf dem Display sieht. Zukünftige PDAs (Personal Digital Assistants) werden hier Abhilfe schaffen; auch der **ME-Chip** der Firma ESD bietet zumindest sicheren Input. Eine wünschenswerte weitere Eigenschaft, die gegenwärtigen Karten nicht besitzen, ist die Erzeugung der Schlüssel auf der Karte. Daß die Schlüssel also zunächst anderweitig erzeugt und dann auf die Karte gebracht werden müssen, gefährdet sie in jener "Lebensphase". RSA fähige kryptographische Chipkarten gibt es bei uns von **Philips, Siemens, Gemplus und CE-Infosys**.

Neuartige Physikalische Verfahren

Quantenkryptographie sendet zur Informationsübermittlung einzelne Photonen über Glasfaser. Zwischen Sender und Empfänger herrscht ein "quantenkohärenter Zustand". Abhörversuche zerstören die Information, allerdings auch für den Empfänger. Es gibt inzwischen Teststrecken über 30 km.

Auch zur Realisierung "starker Zufallsgeneratoren" könnten in Zukunft Methoden der Quantenoptik dienen.

Quantencomputer sind zur Zeit intensiv studierte, aber nicht praktisch realisierte Objekte der physikalischen und informationstechnischen Grundlagenforschung. Würden sie realisiert, so wäre beispielsweise das RSA-Public-Key System und andere kryptographische Algorithmen nicht mehr sicher. Die Forschung bemüht sich einerseits um Verfahren "safe against quantum attacks", andererseits um neuartige, erst auf Quantencomputern lauffähige Kryptoalgorithmen.

Software vs. Hardware

Software ist i.a. billig und flexibel, Hardware oft teuer und oft umständlich zu handhaben.
Wenn es auf Geschwindigkeit ankommt, sind manchmal nur Hardware-Lösungen möglich, man denke an die Übertragungsgeschwindigkeiten bei ATM oder TV. Softwareverschlüsselung wird z.Zt. kaum wesentlich 100 kByte/sec übertreffen, was natürlich für die meisten und sehr wichtige Anwendungen völlig ausreicht. Bei reinen Softwareimplementationen sind die kryptographischen Schlüssel, wie oben erwähnt, leichter ausspähbar und sollten nach Möglichkeit durch Hardware, z.B. kryptographische Chipkarten geschützt werden.

Kontrolle verschlüsselter Datenströme

Wenn in einer Organisation eine kryptographische Infrastruktur, beispielsweise ein Public Key System mit Untereinheiten wie Verzeichnis öffentlicher Schlüssel, Zertifizierungsinstanz, Treuhandinstanz, etc. eingeführt wird, müssen im Vorfeld verschiedene Punkte geklärt und in einem "Policy Statement" festgehalten werden:

- Sollen die Schlüssel zentral, dezentral, oder von den Benutzern selbst erzeugt werden?
- Wie soll das Hinterlegungssystem für die privaten Schlüssel gestaltet und konfiguriert werden?

- Unter welchen Umständen wird auf den privaten Schlüssel eines Benutzers zugegriffen?
- Sollten nach außen gehende verschlüsselte Daten zugleich immer mit einem oder mehreren "Supervisor Schlüsseln" zu rekonstruieren sein, auf die unter definierten Umständen zugegriffen werden kann?

Verwandte Fragen stellen sich natürlich grundsätzlich bei Verwendung organisationsinterner und organisationsübergreifender digitaler Kommunikation. Da diese bisher im Klartext geschieht, wird sich beispielsweise Industriespionage bisher kaum auf diesem Wege abspielen. Bei Einsatz "starker Kryptographie", für die allein die Täter über die Schlüssel verfügen, sieht dies aber anders aus und man wird dies in den Schlüsselhinterlegungsszenarien berücksichtigen müssen.

Schluß:
Es gibt viele weitere Aspekte der Anwendung von Verschlüsselungsverfahren, auf die hier nicht weiter eingegangen wird: digitales (anonymes) Geld und Finanztransaktionen, Verwendung von Pseudonymen in der Beziehung zwischen Individuen und Institutionen, technische Datensicherheit in der Medizin, digitale Wahlen, die frei und geheim sind, bei denen aber jeder Wähler die Korrektheit der Zählung kontrollieren kann, Zeitstempeldienste, und vieles andere mehr. Wir haben uns hier auf die Vorstellung und Diskussion einiger grundlegender Mechanismen beschränkt.

Klar sollte geworden sein, daß kryptographische Algorithmen, Protokolle, Technologien und Infrastrukturen zur Sicherung unserer Informationsgesellschaft und der Realisierung der informationellen Selbstbestimmung der Bürger eine wesentliche Rolle spielen werden.