

# Electronic Cash und Kryptologie

- [Vorwort](#)
- [Einkaufen und Bezahlen per Electronic Cash](#)
- [Mehr Sicherheit durch Verschlüsselung](#)
- [Smartcards mit Kryptoprozessor](#)
- [Elektronisches Geld auf der Chipkarte](#)
- [Sicherheitpaket für das Internet](#)
- [Sicherheit bei Electronic Cash](#)
- [Zuverlässigkeit bei Electronic Cash](#)
- [Das Sicherheitsproblem der Secret-Key-Systeme bei Smart-Cards](#)
- [CyberCash](#)
- [PGP, eine Übersicht](#)
- [Wozu PGP](#)
- [Die Funktionsweise von PGP](#)
- [Die Funktionsweise des RSA-Verfahrens](#)
- [Zahlenbeispiel](#)
- [Das IDEA-Verfahren](#)
- [Der Schutz von öffentlichen Schlüsseln](#)
- [Der Schutz von geheimen Schlüsseln](#)
- [Angreifbarkeit](#)
- [Schlusswort](#)
- [Quellenangabe](#)

## Vorwort

Die Bezahlung via Kreditkarte war im Internet bisher ein unsicheres Unterfangen, denn es gab keine Sicherheit gegen unbefugtes Kopieren der Kartennummer. Neue Verfahren sollen das Internet sicherer machen und damit das virtuelle Kaufhaus beziehungsweise Electronic Cash überhaupt erst ermöglichen.

## Einkaufen und Bezahlen per Electronic Cash

Das Internet entwickelt sich immer stärker zu einem internationalen Marktplatz, auf dem Dienstleistungen und Produkte rund um die Uhr und weltweit erreichbar angeboten werden. Banken und Kaufhäuser entdecken nun auch das Internet, Beispiele sind in den USA die Internet-Plaza, die Huntington Bancshares Inc. oder die Security First Network Bank. Ein großer deutscher Kaufhauskonzern will nun das erste virtuelle Kaufhaus eröffnen.

"Im Jahr 2000 werden im Internet und über Online-Dienste weltweit Finanztransaktionen mit einem Volumen von mehr als 500 Mrd. Dollar abgewickelt", meint Günter Bröcking, Geschäftsführer des auf Bankensoftware spezialisierten Softwareherstellers Management Data, eine Tochtergesellschaft der Österreichischen Creditanstalt. In

Deutschland werden bei der Bayerischen Vereinsbank rund 60.000 Konten bereits online geführt. Bisher konnten die Online-Konten nur über T-Online geführt werden, weil nur dieses Medium die hohen Sicherheitsanforderungen erfüllte. "Nun ist auch AOL soweit. Via PC können Vereinsbank-Kunden weltweit zum Ortstarif ihren Kontostand abfragen, die Umsätze der letzten 90 Tage ansehen oder Überweisungen tätigen", erläutert Vorstandsmitglied Dr. Stephan Schüller.

Im ersten Halbjahr 1997 sollen auch die notwendigen Sicherheitsstandards für die Abwicklung von Bankgeschäften im Internet verfügbar sein. "Schon heute bieten wir im Internet ein umfangreiches Angebot zu unseren Produkten und Dienstleistungen. Immobilien-Interessenten finden nicht nur eine Wohnung oder ein Haus nach ihren Vorstellungen. Sie können auch die Finanzierung gleich berechnen lassen. Geldanleger finden interessante Produkte mit aktuellen Konditionen und individuellen Renditeberechnungen. Börsen-Einsteiger macht unser Börsensimulator fit für den Aktienmarkt.

Man findet auch aktuelle Zahlen oder gar Stellenangebote unserer Bank", so Schüller. Allein im September verzeichnete die Bank 380.000 Zugriffe auf das Internet-Programm, im Juni waren es knapp 200.000. Die Tendenz ist weiterhin stark steigend.

Rushhour auf dem Vereinsbank-Server ist montags bis freitags zwischen 10 und 16 Uhr. Die meisten Zugriffe werden daher während der Arbeitszeit vom Büro aus getätigt. Das deutet zum einen darauf hin, daß die Durchdringung der privaten Haushalte mit Online-Anschlüssen noch nicht so hoch ist. Zum anderen beweist es, daß es sich nicht mehr nur nachtschwärmende Surfer im Internet handelt, sondern auch der Normalverbraucher immer mehr dieses Medium nutzt.

Allen diesen Anwendungen ist jedoch gemein, daß letztendlich Güter bewegt werden, deren Bestellung und Bezahlung gegen kriminellen Mißbrauch zu schützen ist. Und da das Internet per se offen und damit von sich aus keine sicheren Transaktionen garantiert, müssen entsprechende Sicherheitsmechanismen implementiert werden. Als einen Durchbruch für Internet und Online-Banking stuft Bröcking daher die Vereinbarung zwischen Master Card und Visa ein, einen gemeinsamen technischen Standard für die Sicherheit von Online-Finanztransaktionen zu forcieren. Der "Druck zur Einigung" sei im wesentlichen von Banken und Handelsketten in den USA ausgegangen, die die Unterstützung zweier konkurrierender Standards abgelehnt hätten. Der SET-Standard (Secure Electronic Transactions) basiert auf einer eigens dafür entwickelten Verschlüsselungstechnologie von RSA Data Security.

Der RSA-Verschlüsselungsalgorithmus wurde bereits 1978 beschrieben. Er beruht auf dem Problem der Faktorisierung großer Zahlen. Es ist zwar relativ einfach, zwei Primzahlen aus mehr als hundert Dezimalstellen zu finden, aber selbst Großrechner können in angemessener Zeit nicht aus dem Produkt der Primzahlen die entsprechenden Faktoren errechnen. Das Produkt großer Primzahlen läßt sich daher als öffentlicher Schlüssel verwenden und die dazugehörige Faktorisierung als geheimer Schlüssel.

Der Standard wird von führenden Softwareherstellern im Markt für Finanzsoftware unterstützt. "Das elektronische Kaufhaus ist kein Versandhandel im Internet, denn die Privatsphäre der Nutzer in Online-Diensten erfordere den höchstmöglichen Schutz durch Verschlüsselung", stellt RSA-Präsident Jim Bidzos fest.

Mitte Juli stellte Netscape in Zusammenarbeit mit RSA den ersten Verschlüsselungsalgorithmus mit 128 bit Länge vor. Dieses Verfahren ist auf grund amerikanischer Exportbestimmungen nur auf die USA beschränkt, internationale Versionen des Netscape-Internet-Navigators werden mit einer Schlüssellänge von "nur" 40 bit ausgeliefert. Je größer die Schlüssellänge, umso höher der Rechenaufwand zum "Knacken" des Codes. "Dieses höhere Sicherheitsniveau wird die Verbreitung des Internet als Medium für Online-Geschäfte sicher beschleunigen", erwartet der technische Leiter von Netscape, Marc Andreessen. Das Unternehmen will auch darauf hinwirken, daß die US-Regierung ihre bisherige restriktive Haltung aufgibt und Schlüssellängen oberhalb 40 bit auch für den Export freigibt.

"Das Interesse in 128 bit sowohl in den USA als auch international sollte die US-Regierung dazu veranlassen, im Interesse stärkerer weltweiter Konkurrenzfähigkeit amerikanischer Unternehmen sicherere Algorithmen in Produkten wie dem Netscape Navigator exportieren zu dürfen", fordert Marketingchef Mike Homer.

#### Mehr Sicherheit durch Verschlüsselung

Bei Bestellungen oder anderen Transaktionen im Internet kommt es darauf an, daß der Empfänger verifizieren kann, ob der Absender echt ist und die Informationen unterwegs nicht manipuliert wurden. Dies erreicht man mit Hilfe digitaler Unterschriften. Bevor er eine Nachricht über das Netz sendet, fügt der Absender eine kurze zusätzliche Datensequenz hinzu, die als digitale Unterschrift bezeichnet wird. Anschließend wird die Nachricht mit einem bestimmten Schlüssel chiffriert. Die so verschlüsselte Nachricht wird gemeinsam mit der unverschlüsselten Nachricht an den Adressaten übertragen, der die digitale Unterschrift mit seinem Schlüssel dechiffriert und beide

Versionen miteinander vergleicht.

Ergibt sich keine Übereinstimmung, so müssen die Daten als verdächtig angesehen und zurückgewiesen werden. Entweder wurden an der Datei Manipulationen vorgenommen, oder der echte Absender hat es versäumt, die Unterschrift zu erzeugen. Eine einwandfreie Unterschrift dagegen ist ein hinreichender Beleg dafür, daß die Daten nicht modifiziert wurden und von der richtigen Quelle stammen.

Es gibt zwei Hauptgruppen kryptographischer Funktionen. Eine verwendet einen einzigen Schlüssel für Ver- und Entschlüsselung (SecretKey-Kryptographie), während die andere zwei Schlüssel benutzt (PublicKey-Kryptographie). Bei der letzteren können Meldungen, die mit dem einen Schlüssel chiffriert wurden, nur mit dem jeweils anderen wieder entschlüsselt werden. Um die SecretKey-Kryptographie im Zusammenhang mit digitalen Unterschriften effizient einsetzen zu können müßte der Absender seinen privaten Schlüssel an jeden übergeben, mit dem er zu kommunizieren beabsichtigt. Nun versteht es sich aber von selbst, daß man einen privaten Schlüssel unmöglich an jeden Internet-Anbieter übergeben kann. Bei der PublicKey-Kryptographie kann der Absender seinen öffentlichen Schlüssel freizügig bekanntgeben und ihn sogar auf seiner Visitenkarte abdrucken. Nur mit diesem Schlüssel lassen sich Meldungen dechiffrieren, die zuvor mit dem privaten Schlüssel verschlüsselt wurden. Da aber dieser private Schlüssel sicher auf einem Datenträger (beispielsweise in der Smartcard) verwahrt und nicht einmal dem Eigentümer bekannt ist, läßt sich die Echtheit der digitalen Unterschrift und damit die des Absenders zweifelsfrei feststellen.

Um den komplexen Algorithmus für eine elektronische Unterschrift nur auf möglichst wenige Daten anwenden zu müssen und somit Zeit zu sparen, wird auf die zu unterschreibenden Daten zunächst ein sogenannter Hash-Algorithmus angewendet, der die Daten im Umfang reduziert. Sie werden dann mit dem privaten Schlüssel des Absenders "signiert". Signatur und Daten werden zum Empfänger übertragen, dieser wendet auf die Daten den Hash-Algorithmus an und dekodiert die Signatur mit dem öffentlichen Schlüssel des Absenders. Sind die beiden so erhaltenen Werte gleich, ist die Authentizität und Integrität der Daten sichergestellt. Die Zertifizierung eines solchen öffentlichen Schlüssels, vergleichbar mit einem Ausweis, fördert in Deutschland der 1989 gegründete Verein Teletrust. Die Arbeitsgruppe Mailtrust will mit achtzehn Partnerfirmen und der Telekom AG eine entsprechende Infrastruktur aufbauen. Anlässlich der CeBIT '97 ist eine erste Vorführung geplant. "Im europäischen Rahmen läuft bereits ein Projekt zur Sicherung von Transaktionen im Internet. Eine oberste europäische Zertifizierungsinstanz wird mit unseren Techniken arbeiten", so Teletrust-Vorsitzender Prof. Dr. Helmut Reimer. Diese Aktivitäten dienen nicht zuletzt dem Zweck, die Abhängigkeit von amerikanischer Technologie zu verringern.

Die Geschwindigkeit ist bei der Kryptographie selbstverständlich wichtig, denn niemand möchte bei der Abwicklung seiner Transaktionen lange Wartezeiten in Kauf nehmen. Ohne einen hardwaremäßigen Krypto-Coprozessor könnte dieser Vorgang zehn Sekunden oder länger dauern. Netscape beispielsweise will hardwaregestützte Sicherheitsverfahren in die Browser integrieren. Dieser Meinung ist auch Robert Schneider, Chef der deutschen Chipkarten-Firma SCM Microsystems. "Cybercash und andere Software-gestützte Verfahren haben Sicherheitslücken, da eine Authentifizierung des Benutzers nicht vorgesehen ist. Besser sind Hardware-gestützte Verfahren auf PCMCIA-Basis (PC-Cards) oder Smartcards". Für PCMCIA (spezielle Schnittstelle für Zusatzkarten vorwiegend in Notebook-Rechnern) spreche der hohe Datentransfer.

Ein wesentlicher Vorteil des PC-Card-Formats ist die große Verbreitung von PCMCIA-Slots, die 1995 bereits in über 10 Millionen Systemen installiert waren. Die meisten Notebook-PCs verfügen über mindestens einen PCMCIA-Steckplatz vom Typ II. Zudem gehört diese Technologie bereits zur Standardausstattung in vielen neuen Desktop-PCs, und ältere PCs können problemlos mit einem Adapter-Kit aufgerüstet werden.

#### Smartcards mit Kryptoprozessor

Smartcards sind kreditkartengroße Plastikkarten, die einen Mikrocontroller zur Verwaltung und Speicherung der Daten enthalten. Nachteil gegenüber PC-Cards sind die relativ geringe Datenrate und Rechenleistung sowie das spezielle Lesegerät. Dennoch, diese intelligenten Chipkarten lassen sich mit PC-Cards kombinieren und haben sich bereits in puncto Datensicherheit gegenüber Kredit, Scheck und Bankkarten-Magnetstreifen bewährt. Statistiken der "Cartes Bancaires" zeigen, daß die französischen Banken beispielsweise den Betrugsanteil von 0,3 Prozent des gesamten Transaktionswertes auf 0,04 Prozent seit der weitgestreuten Einführung der Smartcard senkten.

Die Smartcard-Technologie wurde bereits Mitte der siebziger Jahre entwickelt, ihre große Verbreitung begann jedoch erst Mitte der Achtziger in den Bereichen Gesundheitswesen, Personentransport und elektronischer Geldverkehr. Verschiedene Faktoren sprechen laut Schneider für die schnelle Verbreitung der Smartcards in Europa: mehr Sicherheitsfunktionen bei zunehmender Anzahl von Ferntransaktionen, Mißbrauch durch mangelnde Sicherheit bei Magnetstreifenkarten sowie sinkende Herstellungskosten für Smartcards. In Europa werden bereits landesweite Programme, die auf der Smartcard-Technologie basieren, eingeführt. Ein Beispiel ist die Krankenversicherungskarte für alle 80 Millionen Versicherten in Deutschland. Ähnliche Überlegungen gibt es auch in anderen europäischen

Ländern.

Smartcards sind daher mit 37 Prozent jährlich das am stärksten wachsende Marktsegment für Mikrochips. Übereinstimmend erwarten die Chiphersteller Motorola und Siemens bis zur Jahrtausendwende ein Volumen von 1,5 Mrd. Mark weltweit. So will Motorola laut Allan Hughes, weltweitverantwortlich für dieses Geschäft, ab dem Jahr 2000 durchschnittlich 10 Millionen Smartcard-Mikrocontroller pro Woche überwiegend in Großbritannien produzieren.

"Smart Cards stellen ein ideales Medium zur Speicherung des öffentlichen/privaten Schlüssels für Sicherheitslösungen auf Basis von RSA dar", erläutert Schneider. Die derzeitige dynamische Entwicklung des Internet und der wachsende Bedarf an sicheren Transaktionen habe neue Einsatzbereiche geschaffen, insbesondere für die Vergabe von Zugriffsrechten und die Abrechnung. Die Smartcards könnten mit Merkmalen wie der elektronischen Unterschrift und Verschlüsselung dazu beitragen, die Transaktionen zwischen Verbrauchern und Banken, dem Einzelhandel und Dienstleistern sicherer zu gestalten.

Die im Oktober '96 vorgestellten sogenannten "FastCrypto"-Chips von Motorola sind in der Lage, komplexe Verschlüsselungsfunktionen bis zu 200 mal schneller auszuführen als konventionelle Smartcard-Chips. Laut Mike Inglis, Worldwide Smartcard Operations Manager bei Motorola, eignen sich die FastCrypto-Chips für den Einsatz in Smartcards, die sowohl eine hohe Verschlüsselungsgeschwindigkeit als auch ein hohes Maß an Datensicherheit verlangen. Anwendungen sind daher die "elektronische Geldbörse" sowie elektronische Handelskonzepte. Bei den Chips können "Public Key"-Kryptographietechniken angewandt werden, die als die sicherste Verschlüsselungsmethode anerkannt sind.

Als einer der führenden Anbieter von Smartcard-Lösungen hat die Firma Schlumberger die FastCrypto-Chips für die Smartcards der "Cryptoflex"-Reihe ausgewählt. In diesen Karten verarbeiten die FastCrypto-Chips den RSA-Algorithmus, der bei der "PublicKey"-Verschlüsselungsmethode den neuesten Stand der Technik darstellt. Jerome Traisnel, Marketing Director bei der Smartcard Division von Schlumberger, bezeichnet die Produkte der "Cryptoflex"-Reihe als die "sichersten Smartcards im heutigen Angebot". Nach seinen Worten sind sie für Applikationen geeignet, die eine sichere Informationsübertragung über Datennetzwerke erfordern, wie beim elektronischen Handel, elektronischen Banktransaktionen, EMail und Werksschutz.

Die beiden neuen FastCrypto-Chips SC49A und SC50 sind mit einem 8bit Mikrocontroller, einem modularen arithmetischen Coprozessor in 1024 Bit Technik, 20 KB ROM, 4 KB EEPROM und 896 Bytes RAM ausgestattet. Die modulare 1024 Bit-Verschlüsselungseinheit kann auch 512 und 786 Bit-Schlüssel effizient verarbeiten. Die neuen Chips ermöglichen darüber hinaus die Entwicklung von Multifunktions-Smartcards, da zum Beispiel der 8 KB große EEPROM-Speicher (Electrically Erasable Programmable Read Only Memory) beim SC50 für mehr als nur eine Applikation genutzt werden kann. So ist eine einzige Smartcard als Kredit und Guthabekarte, elektronische Geldbörse und Kundenkarte einsetzbar.

#### Elektronisches Geld auf der Chipkarte

Neben dem Internet als elektronischem Marktplatz gibt es bereits zahlreiche andere Beispiele für sogenannte ElectronicPurse-Systeme (elektronische Geldbörse) in Europa. Im Feldversuch "Electronic Purse" von Danmont in Dänemark wurde eine landesweit nutzbare PrepaidCard (Karte, auf der ein Guthaben gespeichert ist) eingesetzt, die von öffentlichen Telefonen, Verkaufsautomaten, Waschsalons und Parkuhren akzeptiert wird. Das Projekt war nach Startschwierigkeiten erfolgreich, obwohl es sich um ein hoch komplexes offenes System handelt, da die Karte eines Anbieters von jedem Reader-System bei anderen Anbietern akzeptiert werden muß.

MONDEX in Großbritannien ist das bisher wahrscheinlich erfolgreichste Electronic-Purse-System. Seit 1995 erhalten Verbraucher PrepaidCards, die als Bargeldersatz für Transaktionen jeder Höhe verwendet werden können. Die MONDEX Card wird im Einzelhandel und bei Dienstleistern akzeptiert und eignet sich auch für Transaktionen zwischen Privatpersonen. Das Guthaben auf der Karte kann mit Hilfe speziell angepaßter Geldautomaten, die mit dem MONDEX Symbol gekennzeichnet sind, wieder aufgefüllt werden (zu dem gibt es für diesen Zweck einen neu entwickelten Telefonautomaten). Das MONDEX System wurde für den internationalen Einsatz konzipiert und kann bis zu fünf verschiedene Währungen auf einer Karte speichern. Die Benutzerführung für Transaktionen erfolgt zudem mit Hilfe von Symbolen, so daß keine Probleme durch Sprachbarrieren entstehen.

Mastercard, VISA und Europay International entwickeln seit kurzem gemeinsam ein offenes System für den Einsatz von Smart Cards im elektronischen Handel. Im Rahmen ihrer Initiative EUROPAY planen Sie die Entwicklung eines kombinierten Electronic Purse/Kreditkartensystems, das Interoperabilität und Sicherheit im internationalen Einsatz ermöglicht. Der Sicherheitsaspekt steht im Vordergrund und wird von den meisten Unternehmen derzeit als größte Hürde für die Implementierung des elektronischen Handels angesehen. Die Zukunftspläne verschiedener Branchenexperten basieren jedoch auf den kryptographischen Möglichkeiten von Smart Cards.

Abgesehen von diesen Projekten erfreuen sich ElectronicPurse-Systeme seit ihrer Einführung wachsender Beliebtheit in Europa. Auch in den USA wird für das nächste Jahr ein rapider Anstieg der Nachfrage erwartet. "Für das Jahr 2000 liegt der geschätzte Anteil dieser Systeme an allen finanziellen Transaktionen bei 16 Prozent, das entspricht einem Volumen von 1,7 Milliarden Dollar", erläutert Robert Schneider von SCM. "Die Einführung von Multifunktionskarten für verschiedene Einsatzbereiche (verschiedene Anwendungen, die auf einer einzelnen Smart Card unter einem einheitlichen Betriebssystem laufen) werden die Nachfrage nach Smart Cards zusätzlich erhöhen".

#### Sicherheitspaket für das Internet

Das Internet wird sicherer, so sicher, daß Handel und Geldwirtschaft dieses effektive Kommunikationsnetz nutzen können, um Geschäfte und Transaktionen abzuwickeln. Diese Meinung vertritt die deutsche Tochter der israelischen Firma AR Algorithmic Research (Dietzenbach).

Das neue Gesamtpaket ARISF (AR Internet Security Framework) ist jetzt für alle gängigen Computersysteme verfügbar und enthält Sicherheits-Soft und Hardware, die Handelsunternehmen oder Banken ihren Kunden zur Verfügung stellen können. Unverfälschbare digitale Unterschrift, sichere Internet TCP/IP-Kommunikation und einfache Datenhandhabung, bei der ein Nutzer sich nicht weiter um die Verschlüsselung und Datensicherheit kümmern muß, sind wichtige Eigenschaften des Sicherheitspaketes. Hardwaremodule tragen dazu bei, das erforderliche hohe Sicherheitsniveau zu erreichen.

Die Anwendung beim Endkunden ist verfügbar auf allen gängigen Plattformen (einschließlich Windows 3.x). Eingesetzt werden kann das System ohne weitere Anpassungen mit jedem Standard-Internet-Browser oder anderen TCP/IP-Anwendungen des Internets.

Für den Serviceanbieter werden Filter und andere Funktionen bereitgestellt, wodurch sowohl Authentifizierung wie verschlüsselte Kommunikation mit dem System ermöglicht werden. Bestellformulare, Überweisungen o.ä. können digital unterschrieben werden. So entsteht die Möglichkeit, mit Hilfe von WWW Internet-Anwendungen sichere Dienstleistungen wie Home Banking bereitzustellen. Für den Anbieter enthält das Paket ein Managementsystem zum Aufbau einer Infrastruktur für das Public/PrivateKey-Verfahren und die Zertifizierung von elektronischen Schlüsseln nach dem X.509-Standard.

Kryptographische Server im Unternehmen sowie eine preisgünstige Lösung mit RSA-Chipkarten oder RSA-Standalone-Prozessoren beim Endanwender bilden den Hardwareteil des Sicherheitskonzeptes. Für das zentrale System, bei dem sowohl Sicherheit als auch Performance für den Einsatz entscheidend sind, wird ein kryptographischer Hochsicherheits-Server angeboten, der physikalisch und logisch abgesichert ist.

#### Sicherheit bei Electronic Cash

Das Transaktionsprotokoll muß zeigen, daß Sicherheit auf höchster Stufe erreicht wird, indem höchstentwickelte Verschlüsselungstechniken - z.B. die RSA-Verschlüsselung - zur Anwendung kommen.

Dem User muß versichert werden, daß seine elektronischen Token und sein Speichergerät nicht leicht gefälscht oder verändert werden können. Wenn kriminelle Aktivitäten erfolgen, so sollte es sofort zur Inspektion der Token oder der verwendeten Speichermedien kommen. Der Austausch elektronischer Token erfordert, daß der Empfänger (z.B. der Händler) ein Zertifikat über die Authentizität der Token bekommt. Die Authentifikation kann durch eine dritte Partei (Bank) oder wechselseitig durch die miteinander korrespondierenden Parteien nachgewiesen werden. Der User muß auch imstande sein, zu verifizieren, daß der Austausch zwischen den erwünschten Parteien tatsächlich erfolgt ist.

Die empfangene und bezahlte Information muß unwiderlegbar sein, unabhängig von jeglichen Komplikationen, die durch die Lieferung von Diensten über längere Zeitspannen entstehen, sei es durch Unterbrechungen des Dienstes oder durch momentane Differenzen aufgrund von unterschiedlichen Verrechnungsmethoden verschiedenster Firmen. Alle Sicherheitsanforderungen sollen für jede Partei garantiert sein, ohne daß eine Partei einer anderen vertrauen muß.

#### Zuverlässigkeit bei Electronic Cash

Die den Geldaustausch unterstützende Infrastruktur muß zuverlässig sein. Wann auch immer der User eine Transaktion durchführen will, muß das System verfügbar sein. Dem User muß garantiert werden, daß das System trotz Komponentenfehler oder Hochlast zuverlässig die geforderten Dienste erbringt.

Durch die zunehmende Häufigkeit der Abwicklung von Geschäften via Internet gerät die Wirtschaft in hohe Abhängigkeit von der Verfügbarkeit des Systems. Wiederum sei erwähnt, daß ein System fehlerhaft sein oder zur

Zielscheibe für Angriffe werden kann. Der Schaden, der durch einen Angriff, durch einen Design-Fehler, durch einen Implementierungsfehler, durch einen temporären Fehler etc. entstehen könnte, hätte katastrophale Auswirkungen für die Netzwerkinfrastruktur. Aus diesem Grund muß jene Infrastruktur ein hohes Maß an Verfügbarkeit repräsentieren und auftretende Fehler durch Fehlertoleranz transparent machen. Darunter versteht man z.B., daß bei einem Fehler an einem Server ein anderer Server seine Aufgabe übernimmt. Dem User wird aber dieser Fehler nicht präsentiert.

Das Sicherheitsproblem der Secret-Key-Systeme bei Smart-Cards

Secret-Key Bezahlungssysteme sind trivial. Da gibt es nur einen Schlüssel, den sogenannten Master-Schlüssel (master key), der über das gesamte System verteilt wird. Die Smart-Card des Käufers produziert eine Unterschrift auf die Transaktionsdaten durch Verwendung des Master-Schlüssels. Die Unterschrift wird vom Terminal des Händlers verifiziert, indem der Master-Schlüssel verwendet wird. Die Sicherheit baut vollständig auf der strengen Vertraulichkeit des Master-Schlüssels auf. Da der Schlüssel auf das gesamte System verteilt wird, ist es sehr schwierig, diesen geheimzuhalten. Somit sind jene Systeme nicht für große, offene, verteilte Systeme geeignet. Die Sicherheit von Secret-Key-Systemen kann durch unterschiedliche Schlüssel erreicht werden.

In jenen Systemen wird der Master-Schlüssel durch eindeutige geheime Schlüssel in der SmartCard ersetzt, die mit Hilfe der eindeutigen Smart-Card-Identifikationsnummer aufgebaut werden. Zur Verifikation von Unterschriften, die durch einen geheimen, kartenspezifischen Schlüssel geschaffen wurden, braucht das Terminal des Händlers auf jeden Fall den Master-Schlüssel. Aus Effizienzgründen wird keine Liste von kartenspezifischen Schlüsseln gehalten, sondern das Terminal hält nur den Master-Schlüssel. Der Prozeß des Händlers nimmt den Master-Schlüssel und entwickelt den kartenspezifischen Schlüssel aus der Smart-Card-ID-Nummer des Users so wie der User es schon zuvor machte.

Dieses System ist etwas sicherer als das Basissystem, weil die geschaffenen Unterschriften über den kartenspezifischen Schlüssel entstanden sind. Wenn der Mißbrauch des Schlüssels erkannt wird, erfolgt ein Ausschluß (der User wird auf eine schwarze Liste gesetzt). Der Master-Schlüssel ist weniger weit über das System verbreitet. Doch das ganze System ist gefährdet, wenn der Master-Schlüssel gestohlen wird. Dann könnte etwa der User Geld selbst produzieren. Er hat den Master-Schlüssel der Bank und kann jetzt selbst unterschreiben. Seine Unterschrift ist von jener der Bank nicht mehr unterscheidbar. Und der Master-Schlüssel ist immer noch auf allen Terminals der Service-Provider vorhanden. Dieses Problem überwindet man durch Public-Key-Systeme. Hier hält jedes Terminal einen öffentlichen Verifikationsschlüssel, um die digitalen Unterschriften der Karte zu überprüfen. Mit dem öffentlichen Schlüssel können die Anwender aber keine Unterschrift leisten.

CyberCash

Die Firma CyberCash Inc. in Reston (Virginia) wurde im August 1994 von Bill Melton, Steve Crocker und Donald Eastlake gegründet und ermöglicht die kreditkartenbasierende Bezahlung am Internet (Beginn: 12 Dezember 1994).

Das sichere Internet Payment Service veranlaßt den Kunden zur Kontoeröffnung auf einem CyberCash-Server, von dem aus die Geldtransaktionen via Kreditkarte oder über das Bankkonto erfolgen. Es ist ein auf Windows basierendes System. Auch soll es Mac- bzw. Unix-Versionen geben. Konsumenten mit einem Personal-Computer, einem Internet-Browser und einen Netzanschluß sind in der Lage, sichere Bezahlungen durchzuführen. Es verwendet laut den Herausgebern zwei verschiedene Verschlüsselungssysteme (RSA: 768 BIT Schlüssellänge, DES: 56 BIT Schlüssellänge).

Die Transaktionen werden durch digitale Unterschriften (RSA) authentifiziert und durch den DES-Algorithmus verschlüsselt. CyberCash ist ebenfalls ein experimentelles Cash-System und zusätzlich noch ein kreditbasierendes System. Im E-Cash-System bauen die User ein Konto mit der Bank auf. Dann verwenden Sie eine Software, die von CyberCash gratis zur Verfügung gestellt wird. Am Ende des Tages wird CyberCash alle E-Cash Transaktionen einlösen. Die E-Cash-Kontostände werden in Dollar konvertiert. Das CyberCash-System operiert auf der Spitze jedes allgemeinen Sicherheitssystems (wie es etwa das sichere HTTP ist) und verwendet RSA und DES Sicherheitstandards für die Verschlüsselung.

Beim Kauf werden die Kreditkartendaten verschlüsselt und elektronisch unterschrieben zum Händler transferiert. Der Händler entschlüsselt die Daten nicht. Statt dessen fügt er weitere Informationen (u.a. Zahlungsbetrag) zur Datenstruktur hinzu und überträgt die Daten an den CyberCash-Server. Nach Überprüfung der Unterschrift wird die Kartenummer in das Kreditkarten-Netzwerk übertragen.

PGP, eine Übersicht

Pretty Good(tm) Privacy (PGP), von Philip Zimmermann's Pretty Good Software ist eine hochsichere

kryptografische Software für MSDOS, Unix, VAX/VMS und andere Computer. PGP erlaubt es, geheime Dateien oder Nachrichten bequem und mit Authentizität auszutauschen. Geheim bedeutet, nur die Personen, die eine Nachricht lesen sollen, können sie auch lesen. Authentizität bedeutet, wenn eine Nachricht von einer bestimmten Person zu kommen scheint, kann sie nur von dieser Person kommen. Bequem heißt, Sicherheit und Authentizität ohne die Schwierigkeiten wie z.B. der Schlüsselverwaltung herkömmlicher kryptografischer Programme. Es werden keine 'sicheren' Kanäle benötigt, um die Schlüssel auszutauschen, und dies macht PGP wesentlich einfacher in der Benutzung. Dies kommt daher, das PGP auf einer neuen Technologie basiert, die RSA-Verschlüsselung heißt. PGP kombiniert die Bequemlichkeit des Rivest-Shamir-Adleman (RSA) Kryptosystems mit der Geschwindigkeit herkömmlicher Verschlüsselungsmethoden, digitalen Unterschriften, Datenkompression vor der Verschlüsselung, gute Ergonomie und hervorragende Schlüsselverwaltung. Und PGP führt die RSA-Funktionen schneller durch als die meisten anderen Software-Lösungen. PGP ist RSA-Verschlüsselung für Jedermann. PGP stellt keine eingebauten Modem-Funktionen zur Verfügung. Sie müssen eine eigene Software dafür benutzen.

#### Wozu PGP

Es ist persönlich. Es ist privat. Und es geht niemanden außer Sie etwas an. Vielleicht planen Sie eine politische Kampagne, ihre Steuern oder eine unerlaubte Affäre. Oder vielleicht tun Sie etwas, von dem Sie denken das es nicht illegal sein sollte, aber es ist. Was auch immer es ist, Sie wollen nicht, das ihre private elektronische Post (E-mail) oder ihre vertraulichen Dokumente von irgend jemand anders gelesen werden. Es ist nichts falsch daran, Privatsphäre zu verlangen. Vielleicht denken Sie, ihre E-mail ist legitim genug um ohne Verschlüsselung auszukommen. Wenn Sie ein so gesetzestreuher Bürger sind, der nichts zu verstecken hat, warum schreiben Sie ihre Briefe nicht auf Postkarten ? Warum verweigern Sie einen Drogentest wenn er verlangt wird ? Warum verlangen Sie einen Durchsuchungsbefehl wenn die Polizei vor der Tür steht ? Versuchen Sie etwas zu verstecken ? Sie müssen ein Drogendealer sein, wenn Sie ihre Post in Umschlägen verstecken. Müssen gesetzestreue Bürger ihre E-mail verschlüsseln ?

Was, wenn jeder glauben würde, gesetzestreue Bürger müßten Postkarten für ihre Post benutzen ? Wenn irgendjemand seine Privatsphäre gelten machen und seine Post in Umschläge stecken würde, würde das sofort Verdacht erregen. Vielleicht würden die Behörden seine Umschläge öffnen um zu sehen was er versteckt. Glücklicherweise leben wir nicht in einer solchen Welt, weil jeder seine meiste Post mit Umschlägen schützt. So erregt niemand Verdacht, wenn er seine Privatsphäre mit Umschlägen geltend macht. Analog dazu wäre es schön, wenn jeder, unschuldig oder nicht, seine E-mail verschlüsseln würde, denn dann würde niemand Verdacht erregen, wenn er seine private E-mail mit (Verschlüsselungs-) Umschlägen schützt. Sehen Sie es als eine Form der Solidarität.

Wenn die Regierung heute die Privatsphäre von normalen Leuten verletzen will, muß sie eine ganze Menge Geld ausgeben und Aufwand treiben um die Post abzufangen, mit Dampf zu öffnen und zu lesen, oder um Telefongespräche mitzuhören oder aufzuzeichnen. Diese Art aufwandsintensive Beobachtung ist im großen Stile unpraktikabel. Sie wird nur in wichtigen Fällen betrieben, wenn es lohnend erscheint. Mehr und mehr unserer privaten Kommunikation geht durch elektronische Kanäle. E-mail ersetzt immer mehr die Briefpost. Aber E-mail-Nachrichten sind zu einfach abzufangen und nach interessanten Stichwörtern zu durchsuchen. Das kann im großen Stile sehr einfach, routinemäßig, automatisch und unerkennbar gemacht werden. Internationale Kabelnetze werden jetzt schon von der NSA (National Security Agency/USA- Behörde) im großen Stile gescannt.

Wir gehen auf eine Zukunft zu, in der die Welt überzogen sein wird von hochkapazitiven Fiber-optischen Netzwerken die unsere allgegenwärtigen Personalcomputer verbinden. E-mail wird die Norm sein, nicht die Neuigkeit, die sie heute ist. Die Regierung wird unsere E-mail mit Verschlüsselungsprotokollen sichern, die von der Regierung geschaffen wurden. Die meisten Menschen werden damit zufrieden sein. Aber vielleicht werden einige ihre eigenen Sicherheitsmaßstäbe setzen.

Die US-Senatsverordnung 266 beinhaltet eine sehr störende Resolution. Wenn diese nicht bindende Erklärung Realität geworden wäre, wären Hersteller von sicheren Kommunikationsmitteln dazu verpflichtet gewesen, spezielle 'Falltüren' in ihre Produkte einzubauen, damit die Regierung jedermannes verschlüsselte Nachrichten lesen kann. Sie lautete: 'Es liegt im Sinne des Kongresses, das Anbieter von elektronischen Kommunikationservice und Hersteller von elektronischen Kommunikationsmitteln sicherstellen müssen, daß die Regierung unverschlüsselte Inhalte von Sprache, Daten und andere Kommunikationswegen erhalten kann, wenn das Gesetz es erfordert.' Diese Maßnahme wurde aber nach rigorosen Protesten von ziviler und industrieller Seite nicht Gesetz.

1992 wurde das 'FBI Digital Telephony wiretap proposal' im US-Kongreß vorgestellt. Alle Hersteller von Kommunikations-Equipment sollten spezielle 'Abhörports' in ihre Geräte einbauen, was es dem FBI möglich machen sollte, alle Formen elektronischer Kommunikation vom Büro aus abhören zu können. Obwohl es 1992 wegen Ablehnung durch die Bürger niemals Unterstützung fand, wurde es 1994 wieder vorgeschlagen. Das größte Alarmzeichen ist aber die neue Verschlüsselungs-Politik des Weißen Hauses, die schon seit dem Beginn der Bush-

Zeit von der NSA entwickelt und am 16. April 1993 bekannt wurde. Das Herzstück dieser Politik ist ein von der Regierung gebautes Verschlüsselungs-Gerät, der 'Clipper'-Chip, welcher einen neuen, von der NSA entwickelten geheimen Verschlüsselungsalgorithmus trägt. Die Regierung fordert die Privatindustrie auf, den Chip in ihre sicheren Kommunikationsgeräte einzubauen, wie verschlüsseltes Telefon, FAX, usw. AT&T baut den Clipper schon in seine 'secure voice'-Produkte ein. Das Problem: In der Produktion bekommt jeder Chip seinen einzigartigen Schlüssel und die Regierung erhält eine Kopie dieses Schlüssels. Keine Problem soweit, die Regierung verspricht, den Schlüssel nur zu benutzen um Ihre geheimen Nachrichten zu lesen, wenn sie durch das Gesetz dazu autorisiert wird. Aber natürlich, um Clipper erst effektiv zu machen wäre der nächste logische Schritt, alle anderen Formen der Kryptografie zu illegalisieren.

Wenn Privatsphäre illegal ist, werden nur illegale Privatsphäre haben. Geheimdienste haben Zugang zu guter kryptografischer Technologie. Waffenhändler und Drogendealer ebenfalls. Ölfirmen und andere große Konzerne ebenfalls. Nur die normalen Leute und kleine politische Organisationen hatten bis jetzt keinen Zugriff auf kryptografische Technologie mit 'militärischer Sicherheit'. Bis jetzt. PGP fordert die Menschen dazu auf, ihre Privatsphäre in die eigenen Hände zu nehmen. Dafür ist ein wachsender sozialer Bedarf vorhanden.

Die USA betrachten RSA-Verschlüsselungssysteme als Waffen (RSA-Systeme wurden für den militärischen Einsatz entwickelt) und erlauben deren Export nicht. Frankreich und Rußland verbieten den Einsatz solcher Systeme durch nichtmilitärische Einrichtungen. Zum Beispiel haben anonyme Systeme und unauffindbares digitales Cash einige offensichtliche Bedeutungen für das Arrangieren von "verschlüsselten" Mordverträgen und ähnliches. Militärische Anleitungen für Bombenbauer und für Waffen können anonym verschlüsselt werden und gegen Digitalgeld jenseits der Reichweite verschiedener Regierungen verkauft werden. Die Verbreitung massiver rassistischer und nationalsozialistischer Propaganda durch RSA-Krypto-Systeme ist ebenso denkbar.

Die Funktionsweise von PGP

Zuerst, einige elementare Terminologien. Nehmen wir an, ich will ihnen eine Nachricht schicken, aber ich will, das niemand außer ihnen Sie lesen kann. Ich kann die Nachricht 'verschlüsseln', was bedeutet, ich zerwürfle sie auf eine hoffnungslos komplizierte Art, sodaß niemand außer ihnen in der Lage ist, sie zu lesen. Ich benutze einen kryptografischen 'Schlüssel' um die Nachricht zu verschlüsseln und Sie müssen den selben Schlüssel verwenden um die Nachricht wieder zu entschlüsseln. So funktioniert es jedenfalls auf die herkömmliche Weise in 'Ein-Schlüssel'-Kryptosystemen.

In herkömmlichen Kryptosystemen, wie z.B. dem 'US Federal Data Encryption Standard (DES)' wird ein einzelner Schlüssel für Ver- und Entschlüsselung benutzt. Das bedeutet, der Schlüssel muß zuerst über sichere Kanäle übertragen werden, sodaß beide Seiten ihn kennen, bevor verschlüsselte Nachrichten über 'unsichere' Kanäle übertragen werden können. Das hört sich sinnlos an. Wenn ich einen sicheren Kanal habe, um den Schlüssel zu übertragen, wozu brauche ich dann Verschlüsselung ?

In RSA-Kryptosystemen hat jeder zwei Schlüssel, die zueinander komplementär sind, einen öffentlich bekannten und einen geheimen (Auch oft Privatschlüssel genannt). Jeder Schlüssel öffnet den Code, den der andere erzeugt. Den öffentlichen Schlüssel zu kennen hilft ihnen nicht, den zugehörigen geheimen zu erzeugen. Der öffentliche Schlüssel kann weit über ein Kommunikations-Netz verbreitet sein. Dieses Protokoll erzeugt Privatsphäre ohne die sicheren Kanäle zu brauchen, die für konventionelle Kryptosysteme benötigt werden.

Jeder kann den öffentlichen Schlüssel des Empfängers benutzen, um eine Nachricht für ihn zu verschlüsseln, und dieser benutzt seinen geheimen, um sie wieder zu entschlüsseln. Niemand außer ihm kann die Nachricht entschlüsseln, weil niemand außer ihm Zugriff auf den geheimen Schlüssel hat. Nicht einmal die Person welche die Nachricht verschlüsselt hat, kann sie entschlüsseln.

Authentifikation einer Nachricht ist auch möglich. Der geheime Schlüssel des Absenders kann benutzt werden, um eine Nachricht zu verschlüsseln, sie zu 'unterschreiben'. Das erzeugt eine digitale Unterschrift der Nachricht, welche der Empfänger (oder jeder andere) überprüfen kann, indem er den öffentlichen Schlüssel benutzt, um sie zu entschlüsseln. Dies beweist, das der Absender wirklich der wahre Erzeuger der Nachricht ist und das die Nachricht nicht von jemand anders verändert wurde, weil nur der Absender den geheimen Schlüssel besitzt, der die Unterschrift erzeugte. Eine Fälschung der Unterschrift ist unmöglich und der Absender kann seine Unterschrift später nicht leugnen.

Diese beiden Prozesse können kombiniert werden, um Geheimhaltung und Authentizität zu gewährleisten, indem Sie zuerst ihre Nachricht mit ihrem geheimen Schlüssel unterschreiben und dann mit dem öffentlichen Schlüssel des Empfängers verschlüsseln. Der Empfänger kehrt dieses Schema um, indem er zuerst die Nachricht mit seinem geheimen Schlüssel entschlüsselt und dann ihre Unterschrift mit ihrem öffentlichen Schlüssel prüft. Diese Schritte werden vom Programm automatisch ausgeführt.

Weil die RSA-Verschlüsselung wesentlich langsamer ist als konventionelle Methoden, ist es besser, ein schnelleres, hochsicheres konventionelles Verfahren zu verwenden, um den Text zu verschlüsseln. Dieser originale unverschlüsselte Text wird 'einfacher Text' genannt. In einem für den Benutzer unsichtbarem Prozess wird zuerst ein einmaliger Zufallschlüssel erzeugt, mit dem der Text dann auf konventionelle Weise verschlüsselt wird. Der Zufallschlüssel wird jeweils nur ein einziges Mal verwendet. Dann wird dieser Zufallschlüssel mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und mit der Nachricht zu ihm geschickt. Er entschlüsselt ihn mit seinem geheimen Schlüssel und benutzt ihn, um ihre Nachricht wieder mit den schnellen konventionellen Methoden zu entschlüsseln.

Öffentliche Schlüssel werden in individuellen 'Schlüssel-Zertifikaten' aufbewahrt, welche die 'User ID' (der Name des Benutzers), die Entstehungszeit des Schlüssels und das eigentliche 'Schlüsselmaterial' enthalten. Öffentliche Schlüsselzertifikate enthalten öffentliche Schlüssel, während geheime Schlüsselzertifikate geheime Schlüssel enthalten. Jeder geheime Schlüssel ist nochmal mit einem Passwort verschlüsselt, um ihn zu schützen, sollte er gestohlen werden. Eine Schlüsseldatei, oder 'Schlüsselbund' enthält ein oder mehrere dieser Schlüsselzertifikate. Öffentliche und geheime Schlüssel werden in getrennten Schlüsselbunden aufbewahrt.

Die Schlüssel werden intern auch mit einer 'Key ID' referenziert, welche eine 'Abkürzung' (die untersten 64 Bit) des öffentlichen Schlüssels ist. Wenn diese Key ID angezeigt wird, sehen Sie aber nur 32 Bit, um noch weiter abzukürzen. Viele Schlüssel können die gleiche User ID haben, aber in der Praxis haben keine zwei Schlüssel die gleiche Key ID. PGP benutzt 'Nachrichten-Extrakte' um Unterschriften zu erzeugen. Ein Nachrichtenextrakt ist eine 128 Bit lange kryptografisch sehr starke Hash-Funktion. Es funktioniert etwa wie eine Checksumme oder CRC, indem es die Nachricht in kompakter Form 'repräsentiert' und dazu benutzt wird, um Veränderungen in der Nachricht zu entdecken. Aber im Gegensatz zu einer CRC ist es für einen Angreifer praktisch unmöglich, eine Nachricht zu erzeugen, aus der das gleiche Nachrichtenextrakt entsteht. Dieser Nachrichtenextrakt wird mit dem geheimen Schlüssel des Absenders verschlüsselt um eine digitale Unterschrift zu erzeugen.

Dokumente werden unterschrieben, indem ihnen ein Unterschriftszertifikat vorangestellt wird, welches die Key ID des Schlüssels enthält, mit welchem sie unterschrieben wurde, das verschlüsselte Nachrichtenextrakt und eine Zeitmarke, mit der festgestellt werden kann, wann die Unterschrift erzeugt wurde. Die Key ID wird vom Empfänger benutzt, um den zum Überprüfen nötigen öffentlichen Schlüssel zu finden. Das Programm des Empfängers sucht automatisch die zur Key ID passende User ID und den Schlüssel im öffentlichen Schlüsselbund.

Verschlüsselten Dateien wird die Key ID des öffentlichen Schlüssels vorangestellt, der benutzt wurde, um sie zu verschlüsseln. Das Programm des Empfängers sucht automatisch den zur Entschlüsselung nötigen Schlüssel im geheimen Schlüsselbund.

Diese zwei Schlüsselbunde sind die prinzipielle Methode, um öffentliche und geheime Schlüssel zu verwalten. Anstatt jeden einzelnen Schlüssel in einzelnen Datei zu verwalten, werden sie in Schlüsselbunden gesammelt, um ihr Auffinden durch User ID und Key ID möglich zu machen. Jeder Nutzer erhält sein eigenes Paar Schlüsselbunde. Erzeugte öffentliche Schlüssel werden temporär in einzelnen Dateien gehalten, damit Sie sie zu ihren Freunden senden können, die sie dann zu ihren öffentlichen Schlüsselbunden hinzufügen können.

Die Funktionsweise des RSA-Verfahrens

$\phi(x)$  sei die Eulersche Phi-Funktion, die die Anzahl der  $n$  aus  $N$  bezeichnet, die kleiner als  $x$  und mit  $x$  teilerfremd sind. Ist nicht weiter wichtig, interessant ist nur, daß für zwei Primzahlen  $p$  und  $q$  gilt:

$$\phi(p \cdot q) = (p-1) \cdot (q-1).$$

Es gilt

$$a^{\phi(z)} \equiv 1 \pmod{z} \quad [ = \text{bedeutet: ‚kongruent modulo‘} ]$$

also auch:

$$a^{\phi(z)+1} \equiv a \pmod{z} \quad (a < z)$$

Über die Umformung zu

$$a^x \equiv b \pmod{z}$$

$$b^y \equiv a \pmod{z}$$

Was haben wir nun davon? Nun, wenn es nicht gelingt, aus  $x$  und  $z$   $y$  zu berechnen, dann können wir das Zeichen  $a$

mit dieser Rechnung in das Zeichen  $b$  verschlüsseln, das nicht ohne weiteres zurückverwandelt werden kann. RSA verwendet für  $v$  das Produkt zweier möglichst großer Primzahlen, die Sicherheit des Ganzen liegt darin, daß noch kein schneller Algorithmus bekannt ist, um Primfaktorzerlegungen durchzuführen.

#### Zahlenbeispiel

Mit  $x^*y = (\phi(z)+1)$  kommen wir zur Verschlüsselung: Man nehme zwei Primzahlen (als Beispiel 13 und 11), deren Produkt (143) wird als  $z$  veröffentlicht (also nehmen wir besser größere Zahlen, daß  $143=13*11$  ist, läßt sich recht schnell herausfinden...), weiterhin berechnen wir  $(\phi(z)+1) = 121$ , einen Teiler hiervon (da kommt wohl nur die 11 in Frage...) veröffentlichen wir als  $x$ ,  $y$  (in diesem Fall auch 11) behalten wir geheim.

Nun nehmen wir das zu verschlüsselnde Zeichen (6) und berechnen  $b$ :

$$6^{11} = 362797056 = 50 \pmod{143}$$

Unser verschlüsseltes Zeichen ist also 50. Die verschicken wir nun, der Empfänger kann leicht ausrechnen:

$$50^{11} = 6 \pmod{143}$$

Normalerweise sind  $x$  und  $y$  natürlich voneinander verschieden, aber gute Zahlen zu finden wird erst bei größeren Zahlen leichter.

#### Das IDEA-Verfahren

IDEA ist ein ‚konventionelles‘ Verschlüsselungsverfahren, das sich als sicherer als das bekannte DES erwiesen hat. PGP benutzt eine Kombination von RSA und IDEA, weil eine komplette RSA-Verschlüsselung zu rechenaufwendig, sprich: langsam wäre. Also erzeugt PGP einen zufälligen Schlüssel, den ‚Session Key‘, mit dem die Information IDEA-codiert wird, und packt diesen RSA-codiert zu dem verschlüsselten Text dazu. Das hat außerdem den Vorteil, daß eine Nachricht mit wenig Aufwand für mehrere Empfänger verschlüsselt werden kann: PGP erweitert den verschlüsselten Text für jeden zusätzlichen Empfänger einfach um eine eigene RSA-codierte Kopie des ‚Session Key‘.

#### Der Schutz von öffentlichen Schlüsseln

In einem RSA-Kryptosystem müssen Sie die öffentlichen Schlüssel nicht vor dem Bekanntwerden schützen. Es ist sogar besser, wenn sie soweit wie möglich verbreitet sind. Aber es ist sehr wichtig, öffentliche Schlüssel vor Veränderungen zu schützen, um sicher zu gehen, daß ein Schlüssel wirklich dem gehört, dem er zu gehören scheint. Dies ist der verletzlichste Punkt eines RSA-Kryptosystems. Zuerst sehen wir uns eine mögliche Katastrophe an, und dann wie man sie mit PGP sicher verhindert.

Nehmen wir an, Sie wollen eine private Nachricht an Alice schicken. Sie laden sich Alice's öffentlichen Schlüssel aus einer Mailbox (oder BBS) herunter. Nachdem Sie die Nachricht mit diesem Schlüssel verschlüsselt haben, senden Sie diese über die E-mail Station der Mailbox an Alice. Unglücklicherweise, Ihnen und Alice unbekannt, hat ein anderer Benutzer namens Charlie die BBS infiltriert. Er hat ein neues Schlüsselpaar generiert und Alice's User ID benutzt. Er vertauscht seinen gefälschten Schlüssel mit Alice's echtem öffentlichem Schlüssel. Sie benutzen unwissentlich Charlie's Fälschung anstatt Alice's echten. Alles sieht normal aus, weil die Fälschung Alice's User ID hat. Jetzt kann Charlie die für Alice bestimmte Nachricht entschlüsseln, da er den passenden geheimen Schlüssel hat. Er könnte sogar die Nachricht wieder mit Alice's echtem öffentlichem Schlüssel verschlüsseln und an Alice senden, sodaß niemand irgendetwas bemerkt. Er kann sogar augenscheinlich echte Unterschriften von Alice erzeugen, da ja jeder den gefälschten Schlüssel benutzt, um die Unterschriften zu prüfen.

Die einzige Möglichkeit, diese Katastrophe abzuwenden ist, jeden davon abzuhalten, die öffentlichen Schlüssel zu verändern. Wenn Sie Alice's Schlüssel direkt von Alice haben, ist das kein Problem. Aber das könnte schwierig sein, denn vielleicht lebt Alice tausend Kilometer entfernt oder ist zur Zeit nicht erreichbar. Vielleicht können Sie Alice's Schlüssel von einem vertrauenswürdigen Freund, David, bekommen. David weiß, er hat den echten öffentlichen Schlüssel von Alice. David könnte Alice's Schlüssel unterschreiben, um dessen Integrität zu bestätigen. David würde diese Unterschrift mit seinem eigenen geheimen Schlüssel erzeugen.

Das würde ein unterschriebenes öffentliches Schlüsselzertifikat erzeugen und zeigen, daß Alice's Schlüssel nicht verändert wurde. Dazu müssen Sie einen echten öffentlichen Schlüssel von David haben, um die Unterschrift zu prüfen. Vielleicht könnte David Alice ein beglaubigtes Zertifikat ihres Schlüssels übergeben. David wirkt also als ein ‚Vorsteller‘ zwischen Ihnen und Alice.

Der beglaubigte Schlüssel von Alice könnte von David oder Alice auf eine BBS geladen werden, von der Sie ihn

später wieder herunterladen können. Sie können David's Unterschrift mit seinem öffentlichen Schlüssel überprüfen. Niemand wird Sie dazu bringen, seinen gefälschten Schlüssel als Alice's zu akzeptieren, weil niemand David's Beglaubigung fälschen kann.

Eine vertrauenswürdige Person kann sich sogar darauf spezialisieren, neue Benutzer 'bekanntzumachen', indem er deren Schlüsselzertifikate beglaubigt. Diese Person könnte als 'Schlüsselverwalter' oder 'Beglaubiger' agieren. Von jedem von ihm beglaubigten Schlüsselzertifikat kann mit Sicherheit gesagt werden, das es wirklich demjenigen gehört, dem es zu gehören scheint. Alle Benutzer, die an diesem Service teilnehmen wollen brauchen nur eine bekannt echte Kopie des öffentlichen Schlüssels vom 'Schlüsselverwalter', um dessen Unterschriften prüfen zu können.

Ein vertrauenswürdiger Schlüsselverwalter oder Beglaubiger ist besonders für große unpersonale zentral kontrollierte Firmen oder Regierungsbehörden zu empfehlen. Einige Institutionen verwenden Hierarchien von Beglaubigern. In kleineren Umgebungen würde es besser funktionieren, wenn man allen Nutzern erlaubt, als 'Bekanntmacher' für ihre Freunde zu fungieren. PGP geht diesen 'organischen' nicht-institutionellen Weg. Er spiegelt besser die Art wieder, wie Menschen sonst miteinander umgehen, und erlaubt den Menschen die Wahl, wem Sie das Schlüsselmanagement anvertrauen.

Die Notwendigkeit öffentliche Schlüssel vor unerlaubter Veränderung zu schützen ist das schwierigste Problem in praktischen RSA-Applikationen. Es ist die Achillesferse der RSA-Kryptografie und ein großer Teil der Software-Komplexität wird nur gebraucht, um dieses eine Problem zu lösen.

Sie sollten einen öffentlichen Schlüssel nur dann benutzen, wenn Sie sichergestellt haben, das er wirklich dem gehört, von dem er es behauptet. Sie können sich dessen sicher sein, wenn Sie ihn direkt vom Besitzer haben oder wenn er eine Unterschrift von jemandem trägt, von dem Sie schon wissen, das Sie seinen echten öffentlichen Schlüssel haben. Auch sollte die User ID den vollen Namen des Besitzers enthalten, nicht nur den Vornamen.

Wie verlockt Sie auch immer sein mögen - und Sie werden verlockt sein-- trauen Sie niemals, NIEMALS einem öffentlichen Schlüssel, den Sie von einer BBS heruntergeladen haben, wenn er nicht von jemandem, dem Sie trauen unterschrieben ist. Ein nicht beglaubigter Schlüssel kann von jedem verändert worden sein, sogar vom SysOp der Mailbox.

Wenn Sie gebeten werden, einen öffentlichen Schlüssel zu beglaubigen, stellen Sie sicher, das er wirklich der Person gehört, die in der User ID angegeben ist, weil ihre Unterschrift auf diesem Schlüssel Ihr Versprechen ist, das dieser Schlüssel wirklich Ihr gehört. Andere Leute werden diesem öffentlichem Schlüssel vertrauen, weil Sie ihrer Unterschrift darauf vertrauen. Es wäre falsch, Hörensagen zu glauben - unterschreiben Sie nur, wenn Sie aus erster Hand wissen, das er wirklich Ihr gehört. Vorzugsweise sollten Sie einen Schlüssel nur dann unterschreiben, wenn Sie ihn direkt von der Person haben.

Um einen Schlüssel zu unterschreiben, müssen Sie sich über den Eigentümer viel sicherer sein, als wenn die nur mit diesem Schlüssel verschlüsseln. Um sicher zu sein, das ein Schlüssel zur Benutzung gut genug ist, sollten die Unterschriften einiger Bekanntmacher ausreichen. Aber um ihn selbst zu unterschreiben müssen Sie aus erster Hand wissen, wem er gehört. Vielleicht können Sie den Eigentümer anrufen und die Schlüsseldatei mit ihm überprüfen und festzustellen, das Sie wirklich ihren Schlüssel haben - und stellen Sie sicher, das Sie mit der richtigen Person reden.

Halten Sie sich vor Augen, das ihre Unterschrift auf dem öffentlichen Schlüssel nicht die Integrität dieser Person garantiert, sondern nur für die Integrität (das Eigentum) des Schlüssels bürgt. Sie werden nicht ihre Reputation verlieren weil Sie den Schlüssel eines Psychopaten beglaubigt haben, nur weil Sie absolut sicher waren, das dieser Schlüssel wirklich ihm gehört. Andere Leute werden dem Schlüssel vertrauen, weil Sie ihrer Unterschrift vertrauen (angenommen Sie vertrauen Ihnen), aber Sie müssen nicht dem Besitzer des Schlüssels vertrauen. Einem Schlüssel zu vertrauen bedeutet nicht, dem Schlüsselbesitzer zu vertrauen.

Vertrauen ist nicht unbedingt übertragbar; Ich habe einen Freund, von dem ich glaube, das er nicht lügt. Er ist ein leichtgläubiger Mensch, der glaubt, der Präsident lügt nicht. Das bedeutet nicht, das ich glauben muß, der Präsident lügt nicht. Das ist ganz einfach. Wenn ich Alice's Beglaubigung traue, und Alice traut Charlie's Beglaubigung, heißt das nicht, das ich Charlie's Beglaubigung trauen muß.

Es wäre eine gute Idee, ihren eigenen Schlüssel mit einer Sammlung von Unterschriften einiger Beglaubiger zu haben, in der Hoffnung, die meisten Leute werden wenigstens einem der Bekanntmacher genug trauen, für ihren Schlüssel zu bürgen. Sie können ihren beglaubigten Schlüssel in einigen Mailboxen ablegen. Wenn Sie jemandes Schlüssel beglaubigen, senden Sie ihm eine Kopie, damit er ihre Unterschrift in seine Schlüsseldatei aufnehmen kann.

Achten Sie darauf, das niemand ihren eigenen öffentlichen Schlüsselbund verändern kann. Das Überprüfen neuer Schlüssel ist unbedingt von der Integrität der Schlüssel ihres Schlüsselbundes abhängig. Behalten Sie physikalische Kontrolle über ihren geheimen Schlüsselbund, bevorzugterweise auf ihrem eigenen PC, nicht auf einem entfernten (z.B. Netzwerkservers), genauso wie Sie es mit ihrem geheimen Schlüsselbund machen. Dies, um die Schlüssel vor Veränderung zu schützen, nicht um sie geheimzuhalten. Behalten Sie immer Sicherheitskopien ihrer Schlüsselbunde auf schreibgeschützten Medien.

Weil Ihr eigener öffentlicher Schlüssel als 'oberste Autorität' zum direkten oder indirekten Beglaubigen aller anderen Schlüssel benutzt wird, ist er der wichtigste zu schützende Schlüssel. Um unerwünschte Veränderungen zu erkennen, können Sie PGP anweisen, ihren Schlüssel mit einer Sicherheitskopie auf einem schreibgeschützten Medium gegenzutesten.

PGP nimmt generell an, das Sie physische Sicherheit über Ihr System, ihre Schlüsselbunde und natürlich PGP selbst haben. Wenn ein Angreifer PGP selbst verändern kann, kann er eventuell die Sicherheitsmaßnahmen ausschalten, die PGP hat, ihre Schlüssel zu schützen. Ein etwas komplizierter Weg, ihren Schlüsselbund zu schützen wäre, wenn Sie die gesamte Schlüsseldatei mit ihrem geheimen Schlüssel unterschreiben. Sie können eine separate Unterschriftsdatei mit dem Befehl '-sb' erzeugen. Unglücklicherweise brauchen Sie immer noch eine Sicherheitskopie ihres öffentlichen Schlüssels, um die Integrität der Beglaubigung zu überprüfen. Benutzen Sie dazu nicht den Schlüssel aus der beglaubigten Unterschriftsdatei, denn diesen wollen Sie ja gerade überprüfen.

#### Der Schutz von geheimen Schlüsseln

Schützen Sie ihren geheimen Schlüssel und seinen Sicherheitssatz gut. Wirklich, wirklich gut. Wenn Ihr geheimer Schlüssel je bekannt wird, teilen Sie das besser jeder interessierten Partei mit (viel Glück), bevor irgendjemand ihn benutzt, um in ihrem Namen Unterschriften zu machen. Er könnte zum Beispiel benutzt werden, um gefälschte Schlüsselzertifikate zu beglaubigen, was vielen Leuten Probleme bereiten könnte, speziell wenn Sie großes Vertrauen genießen. Und natürlich, ein Bekanntwerden Ihres geheimen Schlüssel gefährdet auch alle Nachrichten, die an Sie geschickt werden.

Um ihren geheimen Schlüssel zu schützen, fangen Sie am besten damit an, immer physische Kontrolle über ihn zu behalten. Es ist OK, ihn auf ihrem Heimcomputer zu speichern, oder Sie können ihn auf ihrem Notebook halten, das Sie mit sich herumtragen können. Wenn Sie einen Bürocomputer benutzen müssen, über den Sie nicht immer die Kontrolle haben, behalten Sie den Schlüssel auf einer schreibgeschützten Diskette, die Sie nicht im Büro zurücklassen sollten, wenn Sie gehen. Es ist keine gute Idee, ihren Schlüssel auf einem Fern-PC, wie einem remote dail-in Unix-System, zu haben. Jemand könnte ihre Modem-Leitung abhören, ihren Sicherheitssatz herausfinden und dann den Schlüssel vom Fern-PC holen. Benutzen Sie ihren Schlüssel nur auf einem PC, den Sie kontrollieren können.

Speichern Sie ihren Sicherheitssatz nicht auf dem gleichen Computer wie ihre geheime Schlüsseldatei. Das wäre ungefähr so gefährlich, wie ihre Geheimzahl in der Geldbörse mit ihrer Scheckkarte aufzubewahren. Niemand anders sollte die Diskette mit der geheimen Schlüsseldatei in die Hände bekommen. Am besten wäre es, Sie merken sich den Sicherheitssatz gut und schreiben ihn nirgends auf. Wenn Sie ihn sich aufschreiben müssen, schützen Sie ihn gut, vielleicht sogar besser als ihre geheime Schlüsseldatei.

Behalten Sie Sicherungsdateien ihrer geheimen Schlüsseldatei -- denken Sie daran, daß nur Sie die geheimen Schlüssel besitzen. Wenn Sie diese verlieren werden alle von ihnen verteilten öffentlichen Schlüssel nutzlos.

Das dezentralisierte Schlüsselmanagement hat seine Vorteile, aber das bedeutet auch, das wir uns nicht auf eine zentrale Liste ungültig gemachter Schlüssel verlassen können. Das macht es ein wenig schwieriger, den Schaden gering zu halten, wenn der geheime Schlüssel bekannt wird. Sie müssen einfach in den Wald rufen und hoffen, das jeder es hört.

Wenn der schlimmste Fall eintritt-- Ihr geheimer Schlüssel und Ihr Sicherheitssatz fallen in falsche Hände (hoffentlich finden Sie das irgendwie heraus) -- müssen Sie ein 'Schlüssel bekannt geworden'- Zertifikat ausgeben. Dieses Zertifikat warnt andere Leute vor der Benutzung ihres öffentlichen Schlüssels. PGP kann mit dem Befehl '-kd' ein solches Zertifikat für Sie erstellen. Sie müssen es dann irgendwie zu jedem auf diesem Planeten schicken, oder wenigstens zu ihren Freunden und deren Freunden, usw. Deren PGP wird dieses Zertifikat in die öffentlichen Schlüsselringe einbauen und Sie automatisch davon abhalten, ihren öffentlichen Schlüssel zu benutzen. Sie können jetzt ein neues Schlüsselpaar erzeugen und den neuen öffentlichen Schlüssel mit dem Ungültigkeitszertifikat absenden.

#### Angreifbarkeit

Kein Datensicherheitssystem ist unangreifbar. PGP kann auf verschiedenen Wegen hintergangen werden. Mögliche Angreifbarkeiten schließen ein: Bekanntwerden ihres geheimen Schlüssels oder des Satzes, Veränderung öffentlicher Schlüssel, gelöschte Dateien, die immer noch auf ihrer Festplatte sind, Viren und Trojanische Pferde, Lücken in der physikalischen Sicherheit, elektromagnetische Emissionen, ungeschützte multi-user Systeme, Datenverkehrsanalyse oder sogar direkte Kryptoanalyse.

Manchmal benutzen kommerzielle Produkte den 'Federal Data Encryption Standard' (DES), einen ziemlich guten Algorithmus, der von der US-Regierung für kommerzielle Anwendung empfohlen wird (allerdings nicht für geheime Regierungsdaten, naja...). Es gibt mehrere Arbeitsmodi, die DES benutzen kann, wovon einige besser als andere sind. Die US-Regierung empfiehlt, nicht den schwächsten Modus für Nachrichten zu verwenden, den 'Elektronisches Codebuch' (ECB) Modus. Aber Sie empfehlen die stärkeren und komplexeren Modi 'Chiffatrückführung' (Chiper-Feedback - CFB) oder Chiffratblockverkettung (Chiperblock-Chaining - CBC).

Sogar die wirklich guten Softwarepakete, die DES in korrekter Weise verwenden, haben immer noch Probleme. Das Standard-DES benutzt einen 56-bit Schlüssel, der für heutige Anforderungen zu klein ist, und jetzt auch leicht mit simplem 'Durchprobieren' aller Schlüssel auf Hochgeschwindigkeitsmaschinen knackbar ist. DES ist am Ende seines nützlichen Lebens angelangt, und somit auch alle Software, die es benutzen.

Es gibt eine Firma, genannt AccessData (87 East 600 South, Orem, Utah 84058, Telefon 1-800-658-5199) welche ein Softwarepaket für \$185 verkauft, das die eingebauten Verschlüsselungen von Lotus 1-2-3, MS Excel, Symphony, Quattro Pro, Paradox, und MS Word 2.0 knackt. Es rät nicht einfach Passwörter -- es macht echte Kryptoanalyse. Einige Leute kaufen es, wenn Sie die Passwörter zu ihren eigenen Dateien vergessen haben. Behörden kaufen es auch, damit sie die Dateien lesen können, die sie beschlagnahmen. Eric Thompson sagt, sein Programm braucht nur Bruchteile einer Sekunde, um sie zu knacken, aber er hat ein paar Warteschleifen eingebaut, damit es für den Käufer nicht zu einfach aussieht. Er sagte mir auch, das die Passwort- Option von PKZIP auch oft einfach geknackt werden kann, und seine behördlichen Kunden haben diesen Service schon von einem anderen Anbieter.

#### Schlusswort

Israelische Forscher haben eine Methode entwickelt, die so gut wie jedes Verschlüsselungssystem knackt, auch das bei sensiblen Daten von Banken meistverwendete, DES. Es gilt als sicher, weil es mit Primzahlen arbeitet und "Einbrecher" mit extrem langen, schwer zu findenden Zahlen abwehrt. Gegen die Israelis hilft die Strategie nichts, sie finden Primzahlen jeder Länge, indem sie wie Verhaltensforscher die Chips beobachten, denen die Verschlüsselung einprogrammiert ist. Ähnliches ist schon bei "public keys" gelungen, bei denen alle Sender einen gemeinsamen Schlüssel und nur der Empfänger noch einen zweiten hat. Anstatt wie herkömmliche Datendiebe diesen Schlüssel zu stehlen, haben US-Forscher über die Beobachtung der Länge seiner Entzifferung durch den Empfänger die Codes geknackt. Nun wurde der härtere DES - ein "secret key", bei dem die Parteien den Schlüssel austauschen - überlistet. Die Forscher holen sich das Verschlüsselungsprogramm aus der "black box" - dem versiegelten, unzugänglichen Chip -, indem sie mehrere Male dieselbe Botschaft durch den Chip schicken und ihn zwischen jedem Durchgang mit Mikrowellen bestrahlen. Dadurch richten sie kleine Schäden im Programm an, das dann immer ein wenig anders verschlüsselt. Aus diesen Abweichungen schließlich kann man mit einem speziellen Verfahren - Differential-Fehler-Analyse - den Schlüssel selbst rekonstruieren.

#### Quellenangabe

- Diplomarbeit "Electronic Cash in verteilten Systemen" von Manhard Schlifni
- PGP Dokumentation Version 2.6.3
- [Standard 11/96](#)
- [Computerwelt 46/96](#)
- <http://web.mit.edu/network/pgp.html>