Spezielle Kapitel des Informationsmanagements

Prof. Dr. Stefan Voß, Sommersemester 1998

Kryptographie

Andreas Fink

Inhaltsverzeichnis

1 Einleitung

Unter Electronic Commerce versteht man die elektronische Abwicklung von Geschäftsverkehr („elektronisches Handeln“, „elektronische Märkte“), d.h. die (teil-) automatisierte Kommunikation (Informationsaustausch) von Unternehmen mit externen Partnern zur (elektronischen) Abwicklung von Transaktionen unter Einsatz von Informations- und Kommunikationstechnik. Dabei werden alle Phasen von Markttransaktion unterstützt (Informations-, Vereinbarungs- und Abwicklungsphase).

Eine elektronische Unterstützung solcher Transaktionen läuft letztendlich auf eine unternehmensübergreifende Integration von Informations- und Kommunikationssystemen hinaus. Nur hierdurch können moderne Logistik- und Produktionskonzeptionen wie „Just-in-time“ sinnvoll verwirklicht werden. Der Zwang hierzu ergibt sich durch die Veränderungen der Wettbewerbsbedingungen, insbesondere im Zusammenhang mit der Globalisierung und einer weitergehenden Arbeitsteilung in allen Unternehmensprozessen mit einer Vervielfachung der Informationsprozesse. Voraussetzung für ein erfolgreiches Umsetzen von entsprechenden Potentialen ist ein ganzheitliches Prozeßdenken über Unternehmensgrenzen und eine entsprechende Unterstützung durch entsprechende Informations- und Kommunikationstechnik. Ansätze hierzu sind schon seit den 70er Jahren im Zusammenhang mit EDI-Konzeptionen (Electronic Data Interchange) vorhanden. EDI steht für eine zwischenbetriebliche, strukturierte Kommunikationsform für den Austausch von codierten Informationen mit spezifizierbarer Semantik. Einem weitgehenden Durchbruch stand bisher das Fehlen einer einfachen und effizienten Kommunikationsinfrastruktur sowie eine hohe Komplexität und Vielfalt bezüglich Formaten zum Datenaustausch entgegen. Als Vorteile sind u.a. zu nennen: Reduktion administrativen Aufwands durch Automatisierung kostenintensiver Arbeitsprozesse, Rationalisierung, erhöhte Daten- und Informationsqualität, Verbesserung des Informationsflusses (z.B. durch Synchronisation).

Auf der Absatzseite ergeben sich neue Potentiale durch den Durchbruch des Internets bzw. WWWs als neuem Vertriebsweg. Hierdurch ergibt sich mittelfristig ein verschärfter globaler Wettbewerb mit höherer Markttransparenz. Eine entsprechende Konzeption eines kundenorientierten Informationsmanagements ist die Voraussetzung für die erfolgreiche Etablierung entsprechender Systeme. Als etablierte Ansätze sind zur Zeit zu nennen: *Electronic Banking*, Software-Verteilung per WWW, erste *Elektronische Kaufhäuser* im WWW, u.ä.

Die oben beschriebenen Entwicklungen erbringen neue Rationalisierungs- und Erfolgspotentiale, aber gegebenenfalls zunächst auch eine hohe Komplexität im Zusammenhang mit Konzeption, Entwicklung und Einsatz neuer Informations- und Kommunikationssysteme. Allen Entwicklungen gemeinsam ist aber der Zwang zur Übertragung von Daten zwischen in der Regel nicht lokalen Informationssystemen; dies gilt sowohl für die „Business-to-Business“- als auch für die „Business-to-Customer“-Transaktionen. Es ergibt sich somit die Erfordernis einer Datenübertragung, die gewissen Bedingungen genügt – in dem hier betrachteten Kontext insbesondere der Geheimhaltung der Nachricht, aber auch Kriterien wie einer Garantie einer Nichtverfälschung der Nachricht oder der Nachprüfbarkeit des Absenders der Nachricht. Da in der Regel nicht davon ausgegangen werden kann, daß die Kommunikationsinfrastruktur entsprechende Funktionalitäten bietet, ergibt sich die Notwendigkeit zum Einsatz von Kryptographie. In der Regel geht man hierbei von einer Unsicherheit der Kommunikationsverbindungen aus und muß somit auf einer Ende-zu-Ende-Basis die notwendige Funktionalität sicherstellen.

Im weiteren werden nach einer Begriffsklärung zunächst Anforderungen an bzw. Einsatzmöglichkeiten von Kryptographie diskutiert. Daraufhin werden ausgewählte

kryptographische Verfahren kurz vorgestellt; als umfassende Referenz hierfür sei auf Schneier (1996) verwiesen. Letztendlich wird auf politische und rechtliche Rahmenbedingungen eingegangen sowie die aktuelle Situation (Internet/WWW als Medium für Electronic Commerce, Elektronischer Zahlungsverkehr) diskutiert.

Gegenstand der Kryptographie ist die Kommunikation in der Gegenwart von Gegnern. Kryptographie als Wissenschaft wird in der Regel als Teilgebiet der Mathematik bzw. Informatik angesehen, das sich primär mit Methoden zur Verschlüsselung von Nachrichten beschäftigt. Dabei kommen Krypto-Systeme zum Einsatz; hierunter versteht man Systeme bei Nutzung eines Kommunikationssystems in der Gegenwart von Gegnern mit dem Zweck der Abwehr von dessen Absichten. Bei der Kypto-Analyse besteht die Zielsetzung darin – aus der Sicht eines potentiellen Gegners – Krypto-Systeme zu brechen. Kryptologie kann mal als die Zusammenfassung von Kryptographie und Krypto-Analyse bezeichnen. (Oftmals werden diese Krypto...-begriffe aber auch synonym verwandt.)

Im folgenden seien einige potentielle Anwendungsmöglichkeiten von Kryptographie genannt:

- Schutz der Daten auf einer Festplatte (im Hinblick auf Geheimhaltung)
- Übertragung einer vertraulichen Nachricht per E-Mail
- Übertragung einer Kreditkartennummer im WWW
- Überprüfbarkeit des Absenders einer elektronischen Bestellung
- Nachweisbarkeit einer elektronischen Kommunikation
- Digitale Unterschriften (*digital signatures*)
- Digitales Geld (*cyber-cash, ecash,...*)
- Digitale Wahlen (*electronic voting*)

2 Historie

Kryptographische Verfahren werden seit Jahrtausenden im Rahmen der Diplomatie bzw. in Kriegen zur Übermittlung geheimer Nachrichten angewandt; vgl. Kahn (1996). Beispiele hierfür sind der Einsatz einfacher Buchstaben-Ersetzungsverfahren (wie Verschiebung um vier Stellen im Alphabet). Solche Verfahren sind allerdings sehr unsicher; beispielsweise ist durch Häufigkeitsuntersuchung einzelner Buchstaben oder durch einfaches Durchprobieren eine solchermaßen codierte Nachricht in der Regel leicht zu entschlüsseln.

Ähnliche Verfahren erweisen sich jedoch sogar aus informationstheoretischer Sicht als sicher (d.h., in der codierten Nachricht allein sind keinerlei Informationen über die Ursprungsnachricht mehr enthalten, so daß ein Entschlüsseln der Nachricht für einen Gegner ohne weitere Information unmöglich ist). Hierbei handelt es sich beispielsweise um Verfahren, die Buchstabenersetzungen durchführen, aber dabei für jeden Buchstaben eine neue Ersetzungsvorschrift verwenden („One-Time-Pads“). Solche Verfahren wurden und werden beispielsweise von Geheimdiensten angewandt. Voraussetzung ist natürlich das Vorhandensein der Codierungsvorschriften auf beiden Seiten der Kommunikation. Hierbei können z.B. Kuriere verwandt werden; gelangen die Kuriere unversehrt zum Kommunikationspartner, können die entsprechenden Codierungsvorschriften durchgeführt werden (andernfalls schickt man einen weiteren Kurier ;-). Wichtig ist allein die Geheimhaltung der Codierungsvorschriften.

Als einfaches Beispiel für ein solches „perfektes“ Verfahren sei folgendes Protokoll angegeben. Man geht hierfür davon aus, daß die Nachricht im Bit-Format vorliegt: $m_1,m_2,m_3,...$ Nunmehr benötigt man einen geheimen Schlüssel, der ebenfalls als eine Folge von Bits vorliegen muß (in mindestens der gleichen Länge): $k_1,k_2,k_3,...$ Die Nachricht wird nun über folgende einfache Vorschrift in einen Geheimtext $c_1,c_2,c_3,...$ umgewandelt: $c_i = m_i+k_i \mod 2$. Die Entschlüsselung wird dann einfach durch die nochmalige Ausführung dieser Berechnung erreicht.

Im zwanzigsten Jahrhundert ergab sich durch das Entstehen neuer elektronischer Übertragungsmöglichkeiten (z.B. drahtlose Kommunikation) ein wachsender Bedarf für kryptographische Verfahren. Insbesondere durch den zweiten Weltkrieg ergab sich ein Boom. Beispielsweise wurden bei der Entschlüsselung des deutschen Enigma-Codes von einer britischen Gruppe unter Leitung von Alan Turing erstmals Computer eingesetzt. In der zweiten Hälfte des 20. Jahrhunderts entstand dann erstmals auch ein weitergehender ziviler Bedarf für den Einsatz kryptographischer Verfahren. Nunmehr beschäftigten sich auch Forschungsgruppen in der Industrie mit kryptographischen Verfahren (z.B. IBM: Lucifer, ca. 1969-1974). In den siebziger Jahren wurden symmetrische (s.u.) kryptographische Verfahren standardisiert. Primär ist hier der *Data Encryption Standard* (DES) zu nennen. Dabei ist aber der große Einfluß der *National Security Agency* (NSA), einer lange nicht offiziell bestätigten Teilorganisation des amerikanischen Verteidigungsministeriums (angeblich größter Arbeitgeber für Mathematiker, größter Nutzer von Super-Computern), zu nennen; vgl. Bamford (1982). Deren Anliegen ist zum einen Entwicklung und Einsatz sicherer Kommunikationsverfahren, beispielsweise zwischen US-amerikanischen militärischen oder Regierung-Stellen, zum anderen aber auch die Krypto-Analyse von Systemen „gegnerischer“ Stellen. Dementsprechend sind einige Kryptographie-Standards unter den Verdacht geraten, genau so sicher zu sein, daß ein Brechen des Krypto-Systems gerade nur mit den Ressourcen der NSA möglich ist. Unter dem raschen Fortschreiten der Informationstechnologie sind entsprechende Krypto-Systeme aber teilweise inzwischen mit „Standard-Ressourcen“ zu entschlüsseln, und damit praktisch für die meisten Zwecke nicht mehr brauchbar.

In der Mitte der siebziger Jahre ergab sich durch die Entwicklung von asymmetrischen Verfahren (s.u.) ein Durchbruch. Während bei symmetrischen Verfahren wie dem DES zunächst beide Kommunikationspartner im Besitz eines gemeinsamen geheimen Schlüssel sein müssen, der zuvor über einen sicheren Informationskanal übermittelt werden muß, ist dieses Erfordernis bei den asymmetrischen Verfahren nicht mehr gültig. Dies ist insbesondere bei wechselseitiger Kommunikation mit vielen Partnern (z.B. vielen Kunden oder Unternehmen) wichtig. So wären bei einer Kommunikation mittels symmetrischer Verfahren bei n Partnern $n(n-1)/2$ Schlüsselpaare notwendig; damit ergäben sich entsprechende Probleme bei Schlüsselverteilung und Verwaltung, insbesondere auch im Zusammenhang mit spontaner Kommunikation. 1976 wurden (von Diffie und Hellman sowie unabhängig davon von Merkle) Ideen und Methoden für Protokolle publiziert, bei denen ein Schlüsselpaar aus zwei korrespondierenden Schlüsseln zur Ver- bzw. Entschlüsselung verwendet wird, wovon einer öffentlich zugänglich ist, und dabei der Zwang einer der eigentlichen Kommunikation vorausgehenden geheimen Übermittlung eines gemeinsamen Schlüssels entfällt. Als Durchbruch für einen konkreten asymmetrischen Verschlüsselungsalgorithmus ist insbesondere das sogenannte RSA-Verfahren (s.u.) zu nennen, das 1977 von Rivest, Shamir und Adleman vorgestellt wurde. Heute gibt es eine große Anzahl von auf asymmetrischen Verfahren basierenden Krypto-Systemen, denen im Rahmen des durch das Internet ausgelösten Kommunikationsbooms wachsende Bedeutung zukommt. (Zur beschriebenen Entwicklung vgl. z.B. Garfinkel (1995).)

3 Anforderungen

Im weiteren werden zunächst die wesentlichen primären Anforderungen an Krypto-Systeme angegeben:

- Geheime Übertragung von Nachrichten
- Authentifikation/Authentikation/Authentifizierung
  (eindeutige Identifizierung des Kommunikationspartners)
- Digitale Unterschriften (eindeutige Identifizierung des Nachrichtenerstellers)
- Datenintegrität (Sicherstellung der unmodifizierten Übertragung von Nachrichten)

Neben solchen funktionalen Anforderungen sind aber auch zwei weitere Aspekte hervorzuheben: Zum einen sollen die Verfahren *sicher* sein, d.h. von einem Gegner in der Regel nicht zu brechen sein; zum anderen sollten die Verfahren einfach anzuwenden sein (im Idealfall transparent für den Nutzer).

Teilweise ergeben sich aber aus verschiedenen Sichtweisen weitere, teilweise widersprüchliche Anforderungen. So mag der Staat die potentielle Möglichkeit der Entschlüsselung aller Nachrichten für erforderlich halten, während Bürgern vollkommen sichere Verfahren oder vollkommene Anonymität wichtig sein kann. Andererseits ist auch eine vollkommene Anonymität nicht unbedingt sinnvoll; z.B. ist es zweckmäßig, im Rahmen des Wirtschaftsverkehrs elektronische Transaktionen nachvollziehen zu können.

In diesem Zusammenhang ist zu diskutieren, was überhaupt „sicher“ heißt. Sicher im *informationstheoretischen* Sinn bedeutet, wie oben bereits angesprochen, daß das kryptographische Verfahren perfekt in dem Maße ist, daß durch eine Krypto-Analyse ohne weitere Informationen die Nachricht nicht entschlüsseln werden kann. Solche Verfahren sind aber in der Regel aus verschiedenen Gründen nicht praktikabel. Unter einem sicheren Verfahren versteht man deshalb in der Praxis zumeist ein solches, bei dem *voraussichtlich* der Aufwand zum Entschlüsseln der kodierten Nachricht zu groß ist. Beispielsweise kann man ein Verfahren, bei dem das Entschlüsseln von Nachrichten durch potentielle Gegner voraussichtlich 10^{10} Jahre dauert, als sicher bezeichnen. Problematisch ist allerdings die hierbei notwendige Abschätzung der Ressourcen (wie Zeit, Rechenkapazität), die benötigt werden, um das Verfahren zu brechen. In diesem Zusammenhang sind natürlich Abstufungen zu machen. So genügt ein Verfahren, das zur Zeit einen Rechenaufwand von 10 Jahren bei Nutzung der gesamten aktuell verfügbaren Computerkapazität auf der Erde zum Brechen eines Codes benötigt, wohl zumeist zum Übersenden einer privaten Nachricht, während z.B. an Krypto-Systeme im Zusammenhang mit der Einführung von Standards für *Elektronisches Geld* (s.u.) höhere Anforderungen zu stellen sind.

4 Symmetrische Verfahren

Symmetrische Verfahren besitzen die primäre Funktionalität der geheimen Übertragung von Nachrichten *M* zwischen Kommunikationspartnern, die im Besitz eines gemeinsamen geheimen (privaten) Schlüssels *K* sind (deswegen der Begriff *symmetrisch*); dieser muß zuvor über einen sicheren Kommunikationskanal übertragen werden (z.B. persönlich, oder per Telefon (?)). Bezeichnet man das Verschlüsselungsverfahren durch E sowie das Entschlüsselungsverfahren durch D (jeweils unter Verwendung des geheimen Schlüssels *K*) so kann man den grundsätzlichen Verfahrensablauf einer geheimen Übermittlung einer Nachricht *M* zwischen zwei Kommunikationspartnern wie folgt darstellen:

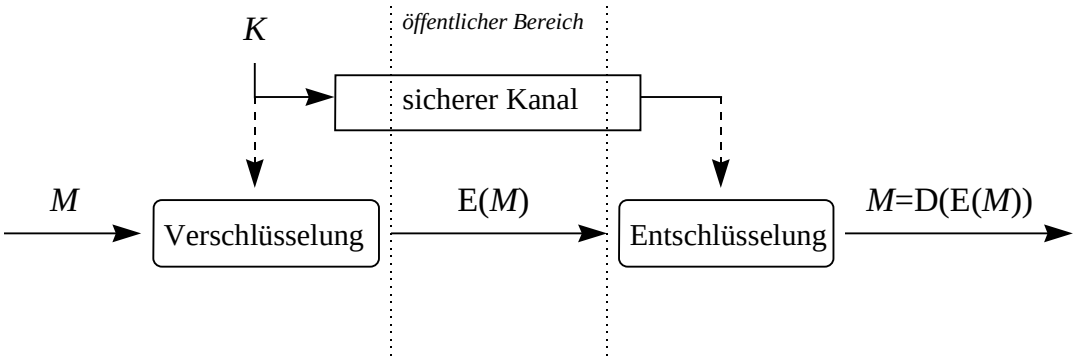

Abbildung 1: Symmetrische Verfahren

4.1 DES - Data Encryption Standard

Das bekannteste symmetrische kryptographische Verfahren ist die DES-Methode. Der grundsätzliche Ablauf bei der Kodierung bzw. Dekodierung von Nachrichten sei hier nur kurz angedeutet: Es werden, unter Verwendung eines Schlüssels der Länge 56 Bit, bei der Verschlüsselung jeweils 64-Bit-Datenblöcke durch eine iterative Kombination von einfachen Verschiebe-, Ersetzungs- und logischen XOR-Operationen durchgeführt (und umgekehrt bei der Entschlüsselung mit der gleichen Methode). Dementsprechend ist das DES-Verfahren einfach und effizient – gegebenenfalls auch in Hardware – zu implementieren (mit Verschlüsselungsraten von mehr als 100 Mbit/s). Die bei der ursprünglichen DES-Methode verwandte Schlüssellänge von 56-Bit wird inzwischen als nicht (mehr) sicher angesehen; z.B. gibt es eine Abschätzung aus dem Jahr 1994, daß das Brechen des Schlüssels in 50 Tagen auf einer Workstation zu bewerkstelligen ist. Heute kommen bei entsprechenden Anforderungen deshalb Erweiterungen (z.B. Triple-DES mit einer größeren Schlüssellänge) oder andere Verfahren zum Einsatz.

4.2 IDEA - International Data Encryption Algorithm

IDEA ist noch relativ neu (1990) und verwendet eine Schlüssellänge von 128-Bit. Die Verfahrensweise sei auch hier nur kurz angedeutet: Es werden jeweils 64 Bit Datenblöcke über eine iterative Kombination von insbesondere Additions-, Multiplikations- und XOR-Operationen transformiert. Das IDEA-Verfahren wird zur Zeit als eines der sichersten Verfahren angesehen. IDEA wird z.B. auch im PGP-Verfahren eingesetzt. Bei einer entsprechenden Implementierung sind Verschlüsselungsraten in der gleichen Größenordnung des DES-Verfahrens möglich. Nachteil des IDEA-Verfahrens ist die vorhandene Patentierung, die jedoch eine kostenlose Nutzung für nicht-kommerzielle Zwecke zuläßt.

5 Asymmetrische Verfahren

Asymmetrische Verfahren bieten über die geheime Übertragung von Nachrichten hinaus weitere Möglichkeiten wie digitale Unterschriften und die Sicherstellung von Datenintegrität, die untenstehend ebenfalls dargestellt werden.

Bei den asymmetrischen Verfahren werden zwei Schlüssel für die Ver- bzw. Entschlüsselung verwendet. Hintergrund hierfür sind sogenannte one-way functions $f(M)$, die einfach berechenbar sind, während die inverse Funktion f^{-1} nicht bzw. nur mit einem erhöhtem Aufwand berechenbar ist (Beispiel: Multiplikation bzw. Faktorisierung). Als spezielle

Version solcher Funktionen besitzen die sogenannten *trapdoor functions* die zusätzliche Eigenschaft, daß eine geheime inverse Funktion f^{-1} existiert, die effizient berechenbar ist, sofern man eine entsprechende Zusatzinformation besitzt.

5.1 Asymmetrische Verschlüsselung

Der grundsätzliche Ablauf bei asymmetrischen Verfahren kann wie folgt dargestellt werden. Voraussetzung ist zunächst, daß jeder Kommunikationspartner ein Schlüsselpaar zur Ver- bzw. Entschlüsselung besitzt: der geheime/private Schlüssel *SK* (secret, private) und der öffentliche Schlüssel *PK* (public); *PK* wird veröffentlicht. Der Absender verschlüsselt die zu übertragende Nachricht *M* mittels des öffentlichen Schlüssels *PK* des Empfängers unter Anwendung eines Verfahrens E; der Empfänger kann diese verschlüsselte Nachricht dann mit seinem privaten Schlüssel *SK* entschlüsseln.

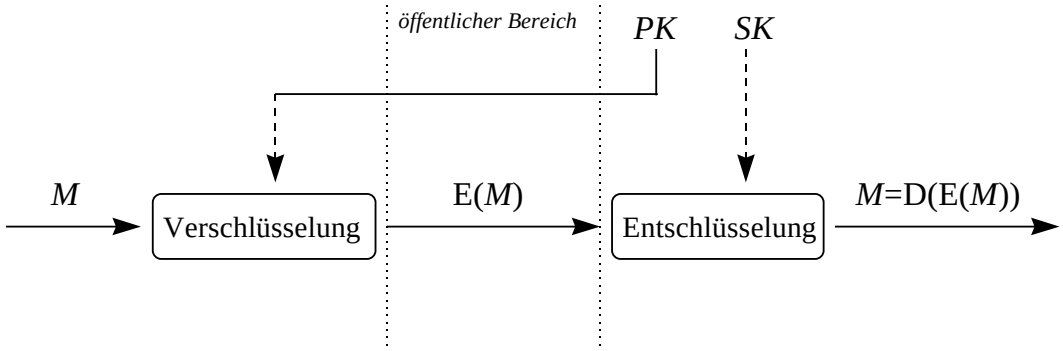

Abbildung 2: Asymmetrische Verfahren

Ein Nachteil der asymmetrischen Verfahren ist allerdings die Tatsache, daß ihre Anwendung deutlich langsamer als bei symmetrischen Verfahren ist (um einen Faktor von ca. 100). Deshalb modifiziert man ihre Anwendung in der Regel folgendermaßen: Bei jeder Kommunikation wird ein (pseudo-) zufälliger *session key K* generiert. Die Nachricht wird nun mittels eines symmetrischen Verfahrens mit dem Schlüssel *K* verschlüsselt; weiterhin wird *K* mittels eines asymmetrischen Verfahrens mit dem öffentlichen Schlüssel *PK* des Empfängers verschlüsselt. Nunmehr werden die verschlüsselte Nachricht und der verschlüsselte *session key* an den Empfänger übermittelt.

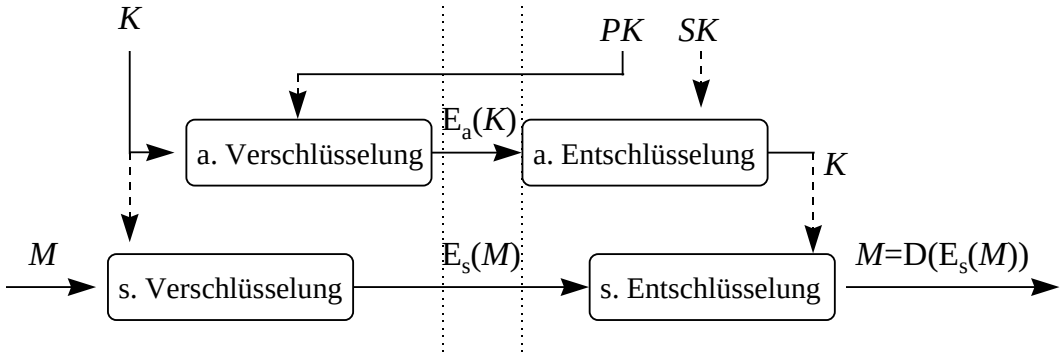

Abbildung 3: Kombination von asymmetrischer und symmetrischer Verschlüsselung

5.2 Digitale Unterschriften

Asymmetrische Verfahren bieten weiterhin die Funktionalität einer digitalen Unterschrift (Signatur), d.h. der Nachprüfbarkeit des Absenders einer Nachricht. Die Idee hierbei ist es, die Nachricht *M* mit dem eigenen privaten Schlüssel *SK* zu verschlüsseln; eine erfolgreiche Entschlüsselung mit dem entsprechenden öffentlichen Schlüssel *PK* stellt dann sicher, daß die Nachricht von dem angenommen Absender stammt. Aus Effizienzgründen wird auch hier das Verfahren wieder modifiziert: Lediglich eine „Zusammenfassung" (*message-digest, hash-value, checksum, fingerprint*) H*(M)* der Nachricht wird verschlüsselt (z.B. ein Hash-Wert der Länge 128 Bit). Der Empfänger entschlüsselt die verschlüsselte Zusammenfassung, berechnet selbst H(*M*) und überprüft auf Gleichheit.

Das Verfahren H sollte eine effizient berechenbare „One-Way Hash Function" darstellen, die aus einer beliebig langen Nachricht *M* einen Wert *h* fester Länge konstruiert; dabei müssen die folgenden beiden Eigenschaften erfüllt werden:

- Für einen gegebenen Wert *h* ist es praktisch unmöglich, eine Nachricht *M* zu konstruieren, so daß H(*M*)=*h*.
- Für eine gegebene Nachricht *M* ist es praktisch unmöglich, eine andere Nachricht *M'* zu konstruieren, so daß H(*M*)= H(*M'*).

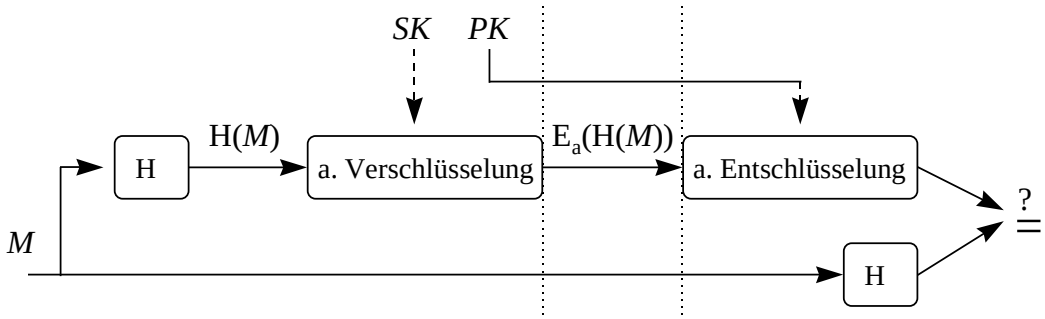

Abbildung 4: Digitale Signaturen über asymmetrische Verschlüsselung

Verschlüsselt man nun auch die Nachricht (s.o.), so erhält man eine geheime und authentifizierte Kommunikation. Bei Verwendung von Zusammenfassungen ist weiterhin die Integrität (Unverfälschtheit) der übertragenen Nachricht sichergestellt. D.h., man kann unter Verwendung asymmetrischer Methoden die wesentlichen Anforderungen an eine Datenübertragung erfüllen.

In den USA wurde vom *National Institute of Standards and Technology* (NIST) ein Standard für digitale Unterschriften definiert: Digital Signature Standard (DSS). In diesem Zusammenhang wurde auch eine One-Way Hash Function spezifiziert (Secure Hash Algorithm (SHA)), die Zusammenfassungen der Länge 160 Bit konstruiert.

5.3 RSA-Verfahren

Das RSA-Verfahren ist das aktuell am weitesten verbreitete praktikable asymmetrische Verfahren, das sich sowohl zur Verschlüsselung als auch für digitale Unterschriften eignet. Der größte Nachteil dieses Verfahrens ist die in den USA bis 2000 gültige Patentierung, die bei einer kommerziellen Nutzung in der Regel zu entsprechenden Kosten führt.

Im folgenden wird das RSA-Verfahren als grundlegendes asymmetrisches Verfahren kurz dargestellt. Man startet mit zwei sehr großen Primzahlen *p* und *q*, die nur anfangs nötig sind.

(Hierbei stellt sich zunächst das Problem, wie p und q zu bestimmen sind.) Nunmehr wählt man eine Zahl e, die relativ prim zu dem Produkt $(p\text{-}1)(q\text{-}1)$ sein muß (d.h. e und $(p\text{-}1)(q\text{-}1)$ dürfen keine gemeinsame Faktoren besitzen). Zusammen bilden dann $n=pq$ und e den öffentlichen Schlüssel. Der korrespondierende private Schlüssel (n,d) wird abgeleitet, indem man d als e^{-1} (mod $(p\text{-}1)(q\text{-}1)$) bestimmt. Hierbei ist die inverse Funktion im Sinne der Modulararithmetik definiert; d.h., d ergibt sich als eine Zahl, so daß das Produkt de gleich 1 (modulo $(p\text{-}1)(q\text{-}1)$) ist. Die Sicherheit des Verfahrens beruht darauf, daß sich n nicht effizient faktorisieren läßt. Diese Anforderung läßt sich komplexitätstheoretisch genauer spezifizieren, allerdings ohne daß ihre Gültigkeit nachgewiesen werden konnte. Zu den Einzelheiten und mathematischen Hintergründen wird auf Schneier (1996) verwiesen.

Die Ver- bzw. Entschlüsselung einer Nachricht M bzw. von Nachrichtenteilen m wird nun folgendermaßen durchgeführt:

Verschlüsselung E von m: $c = m^e \bmod n$

Entschlüsselung D von c: $m = c^d \bmod n$

Der Ablauf wird im folgenden anhand eines einfachen Beispiels verdeutlicht (in der Praxis verwandte Größenordnungen für n liegen zur Zeit bei 512-2048 Bit). Zunächst muß das Schlüsselpaar generiert werden:

$p = 47$ (zufällig gewählte Primzahl)

$q = 71$ (zufällig gewählte Primzahl)

$n = 47 \cdot 71 = 3337$

$(p\text{-}1)\cdot(q\text{-}1) = 3220$

$e = 79$ (e wird zufällig gewählt als relativ prim zu 3220)

$d = 79^{-1} \pmod{3220} = 1019$ (da $1019 \cdot 79 = 1 \pmod{3320}$)

$\rightarrow$ privater Schlüssel (3337, 1019), öffentlichen Schlüssel: (3337, 79)

Verschlüsselung:

$m = 688 \rightarrow E(m) = 688^{79} \bmod 3337 = 1570$

Entschlüsselung:

$E(m) = 1570 \rightarrow D(E(m)) = 1570^{1019} \bmod 3337 = 688 = m$

Angriffsmöglichkeiten

Eine Angriffsmöglichkeit zum Brechen des RSA-Kryptosystems ist zunächst der Zugriff auf p, q und d (wobei p und q nach Generierung der Schlüsselpaare auch gelöscht werden können). Somit muß insbesondere d geheimgehalten werden. Die zweite primäre Angriffsmöglichkeit ist der Versuch, n zu faktorisieren – beispielsweise über neue algebraische Techniken, deren Vorhandensein nicht ausgeschlossen werden kann, oder auch mittels bekannter ineffizienter Verfahren. In diesem Zusammenhang ist zu erwähnen, daß einer der Entwickler des RSA-Verfahrens bei einer Verfahrensbeschreibung (in Gardner's Kolumne in Scientific American 8/77) eine Herausforderung zum Brechen eines Codes gestellt hat. Hierbei wurde n als eine 129-stellige Dezimalzahl angegeben ($\cong$ 429-Bit Schlüssel); Zitat Rivest: „... sure, that I would never see the message ...". Die Nachricht wurde 1994 entschlüsselt (unter Nutzung von 1600 Workstations unter Koordination im Internet).

Um anzudeuten, wie schwer die zukünftige Sicherheit von Krypto-Systemen einzuschätzen ist, sei auf einen aktuellen ausgefallenen Forschungsansatz hingewiesen, der nicht primär im Hinblick auf Kryptographie durchgeführt wird, als „Abfallprodukt“ aber effiziente Faktorisierungsverfahren erbrächte, und damit entsprechende Krypto-Systeme brechen würde. Es gibt eine theoretische Konzeption für sogenannte Quanten-Computer, bei denen Berechnungen auf den Prinzipien der Quantenmechanik basierend ablaufen würden. Ein „Bau“ entsprechender Computer ist aber für die nahe Zukunft wohl nicht zu erwarten. In diesem Zusammenhang sei aber auch angemerkt, daß es andererseits auch Ansätze für Quanten-Krypto-Systeme gibt, bei denen im Zusammenhang mit dem Austausch eines geheimen Schlüssels die Tatsache ausgenutzt wird, daß die Messung an quantenmechanischen Systemen deren Zustand verändert.

5.4 ElGamal - Verfahren

Das Verfahren von ElGamal basiert im wesentlichen auf einer Idee von Diffie und Hellman. Da das entsprechende Patent 1997 abgelaufen ist, ist dieses – ebenfalls sowohl zur asymmetrischen Verschlüsselung als auch für digitale Unterschriften geeignete Verfahren – frei verwendbar. Die Sicherheit des Verfahrens basiert auf der Schwierigkeit, diskrete Logarithmen zu berechnen.

Im weiteren wird der Ablauf einer asymmetrischer Verschlüsselung kurz vorgestellt. Zunächst ist das Schlüsselpaar zu generieren. Hierzu wählt man eine Primzahl p, und daraufhin zufällig zwei Zahlen g und x jeweils kleiner als p. Daraus berechnet sich dann

$$y = g^x \bmod p\ .$$

Der öffentliche Schlüssel setzt sich nun zusammen aus (y, g, p); geheimgehalten wird x. Die Ver- bzw. Entschlüsselung einer Nachricht M bzw. von Nachrichtenteilen m wird nun folgendermaßen durchgeführt. Hierzu ist bei einer Verschlüsselung jeweils noch ein zufälliger Wert k zu wählen, der relativ prim zu p-1 sein muß.

Verschlüsselung von m: $\quad a = g^k \bmod p \qquad b = y^k\, m \bmod p$

Entschlüsselung von (a, b): $\quad m = b/a^x \bmod p$

D.h., die verschlüsselte Nachricht ist doppelt so lang wie die ursprüngliche Nachricht. Bei der Entschlüsselung bestimmt man m derart, daß $ma^x = b \bmod p$. Zur Veranschaulichung sei folgendes Beispiel betrachtet:

$p = 11$ (zufällig gewählte Primzahl)

$g = 5$

$x = 3$

$y = g^x \bmod p = 5^3 \bmod 11 = 125 \bmod 11 = 4$

$\rightarrow$ öffentlicher Schlüssel (y, g, p) = (4, 5, 11), geheim bleibt $x = 3$

Verschlüsselung einer Nachricht $m = 4$ ($k = 2$) :

$a = g^k \bmod p = 5^2 \bmod 11 = 25 \bmod 11 = 3$

$b = y^k\, m \bmod p = 4^2 \cdot 4 \bmod 11 = 64 \bmod 11 = 9$

Entschlüsselung:

$m = b/a^x \bmod p \quad$ *d.h.* $\quad a^x m = b \bmod p \quad 3^3 \cdot m = 9 \bmod 11 \ \Rightarrow \ m = 4$

5.5 PGP - Pretty Good Privacy

Als bekannteste Implementierung eines Krypto-Systems ist das PGP-System zu nennen. Diese Kryptosystem, entwickelt von Phil R. Zimmermann, ist mehr als ein „recht gutes“, mit Einschränkungen frei-verfügbares Verfahren, das in Implementierungen für verschiedene Plattformen vorliegt. PGP besitzt (ab Version 5) neben Funktionalität zur Schlüsselgenerierung und -Verwaltung inzwischen auch eine graphische Benutzerschnittstelle. Durch Exportbeschränkungen der USA liegt es in der Regel als US- und als internationale Version vor, die aber zueinander kompatibel sind.

PGP bietet verschiedene Verfahren zur Auswahl an. Zur symmetrischen Verschlüsselung können CAST, IDEA oder Triple-DES verwendet werden. Zur asymmetrischen Verschlüsselung können die Verfahren RSA oder ElGamal verwendet werden. Für digitale Unterschriften wird NIST DSS empfohlen (in Verbindung mit SHA als Hash-Funktion), während früher das RSA-Schlüsselpaar sowohl zur Verschlüsselung als auch für digitale Unterschriften verwendet wurde.

5.6 Schlüsselmanagement und -verteilung

Ein nicht zu unterschätzendes Problem im Zusammenhang mit der Anwendung kryptographischer Verfahren ist das Schlüsselmanagement. Dabei geht es zunächst um eine sichere Abspeicherung von geheimen Schlüsseln. Dies kann beispielsweise durch Paßwort geschützt auf einer Diskette oder (möglichst lokalen) Festplatte erfolgen. Hierzu können aber beispielsweise auch Chipkarten verwendet werden (gegebenenfalls auch im Zusammenhang mit einer Schlüsselerzeugung); es existieren auch sogenannte Krypto-SmartCards, die sogar die Durchführung der Verschlüsselung bzw. Entschlüsselung implementieren. Bei Verlust geheimer Schlüssel ergibt sich in der Regel die Situation, daß Nachrichten, die unter Verwendung des korrespondierenden öffentlichen Schlüssels verschlüsselt wurden, nicht mehr dekodiert werden können.

Ein weiteres Problemfeld ist die Verteilung von öffentlichen Schlüsseln. Hierbei muß sichergestellt werden, daß der erhaltene öffentliche Schlüssel von dem angenommen Kommunikationspartner stammt und nicht verfälscht wurde. Ansätze hierfür sind u.a. „Key-Server“ im WWW, Verteilung einer Zusammenfassung des öffentlichen Schlüssels (z.B. per Visitenkarte), Registrierung bei und Verbreitung durch eine vertrauenswürdige Institution. Die Integrität und Authentizität von öffentlichen Schlüsseln kann durch eine digitale Unterschrift einer vertrauenswürdigen Institution (Zertifizierungsstelle) garantiert werden; eine solche Institution garantiert dann damit, daß der öffentliche Schlüssel wirklich von dem angegebenen Urheber stammt.

6 Politische und rechtliche Rahmenbedingungen

Zunächst ist anzumerken, daß auf manche kryptographische Methoden (z.B. RSA in USA) Patente bestehen; in der Regel sind für eine kommerzielle Anwendung Gebühren zu zahlen.

Größtes Hindernis für einen weitreichenden Durchbruch standardisierter Krypto-Systeme sind länderspezifische Rechtsvorschriften, die teilweise den Export oder auch den Einsatz bestimmter Krypto-Systeme verbieten. Beispielsweise besteht ein Exportverbot für „starke“ kryptographische Verfahren aus den USA (durch eine Klassifizierung als Waffen); deshalb ist im WWW z.B. das SSL-Protokoll (*Secure Socket Layer*) in der Regel mit kleinerer Schlüssellänge (40 statt 128) im Gebrauch, und damit nicht als sicher anzusehen.

In verschiedenen Ländern gibt es Bestrebungen, die Anwendung „starker“ Kryptographie einzuschränken (oder bereits entsprechende Vorschriften, vgl. die Situation in Frankreich). Die Situation in Deutschland ist (noch?) relativ unbeschränkt. Hier gibt es als zuständige Behörde das Bundesamt für Sicherheit in der Informationstechnik (BSI). Zur Zeit wird das Erfordernis einer gesetzlichen Regelung für den Einsatz von Verschlüsselungssystemen geprüft (z.B. Planung einer generellen Genehmigungspflicht aller Kryptoverfahren, Zulassung nur solcher Systeme, die eine Entschlüsselung durch entsprechende Behörden im Bedarfsfall ermöglichen). Andererseits gibt es Ansichten, daß ein Recht auf Anwendung von „starker“ Kryptographie aus dem Grundgesetz ableitbar ist.

In diesem Zusammenhang ist auf die Steganographie hinzuweisen, d.h. auf die „verdeckte“ Verschlüsselung. Durch einfache Verfahren kann man beispielsweise nicht nachweisbar verschlüsselte Nachrichten versteckt in anderen Daten (z.B. Bildern) kodieren. Damit ist eine Kontrolle der Anwendung von Kryptographie praktisch unmöglich. Mögliche Beschränkungen für den Einsatz von Krypto-Systemen sind damit als unverhältnismäßig, schädlich und unpraktikabel anzusehen (Kosten-Nutzen-Analyse!).

Schließlich ist noch auf das neue, relativ innovative Gesetz zur digitalen Signatur (Signaturgesetz - SigG) im Rahmen des Informations- und Kommunikationsdienste-Gesetzes (IuKDG) hinzuweisen. Zweck dieses Gesetzes ist es, Rahmenbedingungen für digitale Signaturen zu schaffen, unter denen diese als sicher gelten. Zitat: „Eine digitale Signatur im Sinne dieses Gesetzes ist ein mit einem privaten Signaturschlüssel erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Schlüssels, der mit einem Signaturschlüssel-Zertifikat einer Zertifizierungsstelle oder Behörde [...] versehen ist, den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen läßt.“

7 Internet / WWW als Medium für Electronic Commerce

Aktuell stellt sich die Frage, inwieweit das Internet bzw. das WWW als Medium für Electronic Commerce geeignet ist, bzw. wie man etwaige Defizite beheben kann. Zunächst sei hierzu auf einige diesbezügliche Eigenschaften der TCP/IP-Protokolle hingewiesen, auf denen das Internet basiert. Die Datenpakete im Internet werden offen über verschiedene, nicht unbedingt bekannte bzw. vertrauenswürdige Zwischenstationen übertragen. Damit ist zunächst das „Mitlesen“ aber auch ein Verfälschen von Nachrichten oder der Absenderadresse einfach möglich. Ein weiteres Problem in diesem Zusammenhang ist die Sicherstellung des „korrekten“ Kommunikationspartners; dies ist u.a. deshalb ein Problem, da in der Regel eine Transformation eines DNS-Namens zu einer IP-Adresse nötig ist. Das Nachfolgeprotokoll für TCP/IP ist in der Entwicklung (IPv6 bzw. IPnG); damit sollen dann Anforderungen wie authentische Adreßinformationen, nachprüfbare Zuordnung von DNS-Namen zu IP-Adressen, Routing nur über vertrauenswürdige Router/Gateways u.ä. teilweise erfüllt werden können.

Im Grunde muß aber auch dann immer noch davon ausgegangen werden, daß das Internet als Kommunikationsinfrastruktur unsicher ist. Hieraus ergibt sich direkt die Erfordernis für den Einsatz von Kryptographie auf Ende-zu-Ende-Basis. Hierfür wurden schon verschiedene Systeme entwickelt; beispielhaft ist hierbei das von Netscape entwickelte und inzwischen standardisierte SSL-Protokoll zu nennen, das HTTP um kryptographische Methoden erweitert, die eine sichere Kommunikation im WWW gewährleisten sollen. Im Zusammenhang mit Anwendungen wie der Abwicklung von Zahlungsverkehr über das Internet reichen solche Systeme aber in der Regel immer noch nicht aus.

8 Elektronischer Zahlungsverkehr

Zunächst seien die verschiedenen Parteien im Zusammenhang mit elektronischem Zahlungsverkehr klassifiziert:

- Nachfrager/Käufer
- Anbieter von Finanzdienstleistungen (z.B. Banken)
- Organisatoren des Zahlungssystems/Übertragungsmediums
- Anbieter/Verkäufer.

Mögliche Anforderungen an Systeme für einen elektronischen Zahlungsverkehr sind z.B.:

- Sicherstellung der Geheimhaltung und Integrität des Daten- und Zahlungsverkehrs
- Beweisbarkeit von Transaktionen
- Datenschutz (Vertraulichkeit, Anonymität)
- Rechtliche Anerkennung, gerechte Verteilung der Risiken
- Steuerliche Erfaßbarkeit, währungspolitische Kontrollierbarkeit
- Gesellschaftliche Akzeptanz, Benutzerfreundlichkeit, internationale Standards

Zur Zeit existiert noch kein diesen Anforderungen gerecht werdendes universelles System. Deshalb werden im weiteren verschiedene Formen des elektronischen Zahlungsverkehrs, die teilweise bereits im Einsatz, teilweise noch im Entstehen sind, angegeben. Bei allen im folgenden angegebenen Systemen sind Methoden der Kryptographie involviert. Da die Entwicklung auf diesem Gebiet zur Zeit sehr dynamisch verläuft, sei zu den jeweiligen Einzelheiten auf aktuelle Literatur bzw. das WWW verwiesen.

- **Home-Banking über Online-Dienste oder das Internet.** Diesbezügliche Systeme sind in der Regel nur als Ersatz für den Zahlungsverkehr Kunde-Bank zu verstehen und bieten zunächst keine erweiterte Funktionalität im Hinblick auf die Unterstützung von Electronic-Commerce-Anwendungen. Beim Home-Banking per Internet sind verschiedene Sicherheitskonzepte im Einsatz. Bei der Deutschen Bank beispielsweise wird folgende Verfahrenskombination angewandt:
  - Secure Socket Layer (SSL) - Protokoll (Schlüssel nur 40-stellig)
  - plattformunabhängige Java-Benutzeroberfläche
  - Verschlüsselung über Java-Programm mit IDEA-Verfahren (128-stellige Schlüssel, RSA, MD5)
  - Übertragung von Daten mit elektronischen Signaturen
  - Kontozugang über 5-stellige PIN und 6-stellige TANs
  - Firewall zur Sicherung der Informations- und Kommunikations-Infrastruktur der Bank

  Hierbei wird ein mehrstufiges Sicherheitskonzept verfolgt, das durch zwei Prüfungsgesellschaften zertifiziert wurde und als relativ sicher anzusehen ist. Vorteil ist dabei, daß der Kunde keine spezielle Software oder sonstige besondere Funktionalität auf seinem Rechner benötigt, da eine Java-Anwendung verwendet wird. Gleiches kann man aus einer anderen Sichtweise aber auch als Nachteil ansehen, da zum einen die Konsistenz dieser Anwendung sicherzustellen ist, zum anderen aber auch Möglichkeiten wie die

Identifizierung per Chipkarte oder gar Ausführung eines sicheren Krypto-Systems auf einer Chipkarte („Krypto-SmartCard“) auf Kundenseite nicht genutzt werden.

- **Elektronische Bezahlung per Kreditkarte.** Hierbei ergibt sich zum einen die Problemstellung einer geheimen Übertragung der Kreditkartennummer, aus Anbietersicht die Erfordernis einer Nachprüfbarkeit entsprechender Transaktionen, sowie aus Nachfragersicht insbesondere auch die Notwendigkeit der Überprüfung der Authentizität des Anbieters (um Scheinanbieter auszuschließen).

  In diesem Zusammenhang ist insbesondere die SET-Spezifikation (*Secure Electronic Transaction*, Beteiligte: Microsoft, Netscape, IBM, Visa, MasterCard, ...) zu nennen, wodurch eine sichere „Nachbildung“ des Kreditkarten-Zahlungssystems für das Internet ermöglicht werden soll. Die Kreditkarteninformationen des Nachfragers werden dabei verschlüsselt gespeichert und übertragen; weiterhin werden über Authentifizierungs-Server die Identitäten der beteiligten Geschäftspartner überprüft. Ein Problem ist auch hier die private Schlüsselverwahrung. Eine breite Nutzung des SET-Verfahrens wird ab 1998 erwartet, da erst dann entsprechende integrierte Implementierungen bzw. Infrastruktur zur Verfügung stehen werden.

- **Elektronisches Bargeld.** Die originäre Zielsetzung hierbei ist es, die Funktionalität von Geld elektronisch in dem Sinne nachzubilden, daß eine Bezahlung ohne Vermittlerinstanz möglich ist („privat an privat“, „peer to peer payment“, „wie Bargeld“). Dies würde dann auch die effiziente Bezahlung kleinster Geldbeträge im Internet ermöglichen; ein Beispiel hierfür wäre der Zugriff auf einzelne elektronische „Zeitungsartikel“ für Pfennigbeträge, was zum einen für den Nachfrager relativ günstig wäre, zum anderen aber trotzdem dem Anbieter – über die Masse – bei entsprechender Qualität seines Angebots Gewinne ermöglichen würde.

  Führendes System auf diesem Gebiet ist ecash der Firma DigiCash; dieses System, das wesentlich auf asymmetrischer Kryptographie basiert, wird bereits in Pilotversuchen getestet. Die Idee hierbei ist es, „Münzen“ als Byte-Sequenzen darzustellen, die über „Seriennummern“ identifiziert werden. Die Authentizität von Münzen wird per digitaler Unterschrift der ausgebenden Bank sichergestellt. Allerdings ist auch hier immer noch ein Online-Clearing der Gegenstelle beim Zahlungsvorgang notwendig, um Kopien zu verhindern. Andererseits ist in diesem System Anonymität verwirklicht – wie beim Einsatz von Bargeld kann die Bank den Weg der Münzen nicht zurückverfolgen.

  Weitere (notwendige) Funktionalität solcher Systeme ist die Möglichkeit der Wiederherstellung verlorengegangener ecash-Münzen (z.B. durch Festplattendefekt) über einen Recovery-Mechanismus, sowie das Verhindern des Kopierens von ecash-Münzen (beispielsweise über die Aufbewahrung auf Chipkarten oder in entsprechenden Bank-Depots). Neben dem Akzeptanzproblem ergibt sich für solche Systeme das Problem der Standardisierung bzw. Durchsetzbarkeit in der Praxis.

- **Speicherung von Geldbeträgen auf Chipkarten/Smartcards.** Spezifikation des zentralen Kredit-Ausschusses (ZKA): ec-Karte mit Chip, u.a.: vorausbezahlte Geldbörse (bis zu 400,- DM).

9 Literaturverzeichnis

9.1 Bücher

Bamford, J. (1982) The Puzzle Palace: A Report on America's Most Secret Agency. Houghton Mifflin.

Denning, D.E. (1982) Cryptography and Data Security. Addison-Wesley.

Garfinkel, S. (1995) PGP: Pretty Good Privacy. O'Reilly. *[auch in deutscher Übersetzung]*

Kahn, D. (1996) The Codebreakers. Macmillan Company. *[Geschichte der Kryptographie, Stand von ca. 1970]*

Schneier, B. (1996) Applied Cryptography: protocols, algorithms and source code in C. 2nd ed., Wiley. *[Standardwerk zur Kryptographie, auch in deutscher Übersetzung]*

Zimmermann, P.R. (1995) The Official PGP User's Guide. MIT-Press.

9.2 Artikel in Zeitschriften

Byte (1996) E-Cash. Titelthema 6/96.

Communications of the ACM (1996) Special Section Electronic Commerce. 6/96, 22-58.

Diffie, W. (1988) The first ten years of public-key cryptography. Proceeedings of the IEEE 76, 560-577.

Gardner, M. (1977) A New Kind of Cipher That Would Take a Millions of Years to Break, Scientific American 237 (8), 120-124.

Köhntopp, M. (1996) Sag's durch die Blume - Steganographie als Verschlüsselungstechnik. iX 4/96, 92-96.

Rivest, R., A. Shamir und L. Adleman (1977) A Method for Obtaining Digital Signatures and Public Key Cryptosystems. Communications of the ACM 21.

9.3 Internet, WWW

... unzählige Seiten, leicht aufzufinden über Suchmaschinen ...

ecash. http://www.digicash.com/ecash/ecash-home.html

SET Secure Electronic Transaction - Specification. http://www.mastercard.com/set/set.html

news:sci.crypt