B 19 Kryptografie

Wolfgang Semar

B 19.1 Grundlagen

Kryptografie ist die Lehre von der Verschlüsselung von Daten und den Techniken, die zur Realisierung derselben verwendet werden (Lit. 01, S. 5). Sie hat längst die Grauzone der Spionage und des Militärbereichs überschritten und ist als Schlüsseltechnik für die Absicherung weltweiter Computernetze von zentraler Bedeutung. Die Art und vor allem die Menge der Daten, die schützenswert sind, haben sich mit der Verbreitung elektronischer Datenverarbeitung deutlich gewandelt. Es werden nicht nur im Berufs-, sondern auch zunehmend im Privatleben Informationen vor unberechtigtem Zugriff und vor Manipulation geschützt. Verschlüsselungsverfahren kommen im Rahmen der Datenübertragung, besonders in offenen Netzen wie dem Internet, eine besondere Bedeutung zu. Die Kryptografie soll die Vertraulichkeit von Daten ermöglichen. Schließlich hat jede Person und jede Organisation ein legitimes Interesse an dem Schutz ihrer Daten vor Ausspähung. Neben dem offensichtlichen Zweck der Geheimhaltung muss die Kryptografie weitere, grundlegende Kriterien erfüllen wie die Integrität, die Authentizität und die Verbindlichkeit beim Austausch von empfindlichen Daten. Diese vier Kriterien müssen erfüllt sein, wenn eine optimale Datensicherheit gewährleistet sein soll. Für jedes Kriterium gibt es eigene Lösungsmöglichkeiten, die Kunst liegt darin, mit einem Verschlüsselungssystem möglichst alle vier Kriterien gleichzeitig zu erfüllen. Ein weiteres Ziel kann in manchen Situationen Anonymität sein, z. B. beim elektronischen Geld. Darunter wird die Vertraulichkeit nicht des Nachrichteninhalts, sondern sogar des vollständigen Kommunikationsvorgangs als solchem verstanden. Genau genommen muss zwischen der Kryptografie, die sich mit der Verschlüsselung von Daten beschäftigt, und der Kryptoanalyse, die sich mit derer Entschlüsselung beschäftigt, unterschieden werden. Der Oberbegriff für beide Disziplinen ist Kryptologie (Lit. 05, S. 1).

B 19.1.1 Vertraulichkeit

Das klassische Problem beim Austausch von Daten und Nachrichten ist die Vertraulichkeit (Privatheit bzw. Geheimhaltung). Der Inhalt soll nur autorisierten Personen zugänglich gemacht und vor anderen verborgen werden. Es stellt sich also die Frage: Wie kann Alice eine Mitteilung an Bob senden, ohne dass Mallory sie lesen kann? In diesem Fall kommt es nur darauf an, dass der Inhalt einer Nachricht vor Dritten geschützt ist. (In der Literatur werden fiktive Personen zum besseren Verständnis der Situation eingesetzt. Die beiden eigentlichen Partner werden als Alice und Bob bezeichnet. Mallory ist die Figur des Bösen, die den Schriftverkehr belauscht.) Dies lässt sich durch die Verfahren der Kryptografie realisieren. Ein Klartext wird in eine verschlüsselte Form, den Geheimtext, überführt, somit kann eine fremde Person den ursprünglichen Text nicht mehr erkennen. Der Verschlüsselungsvorgang wird als Chiffrieren, der Entschlüsselungsvorgang als Dechiffrieren bezeichnet (Lit. 06, S. 19).

B 19.1.2 Integrität

Unabhängig davon, ob eine Nachricht geheim bleiben soll oder nicht, haben normalerweise der Absender und der Empfänger ein großes Interesse daran, dass sie unverändert ankommt. Es stellt sich hier die Frage: Wie kann Bob eine Nachricht von Alice erhalten, so dass er sicher sein kann, dass sie nicht von Mallory verändert wurde? Ein weiterer Unsicherheitsfaktor ist also die Integrität (Unversehrtheit) der ausgetauschten Daten. Um dies sicherzustellen kann der Text mit einer Art elektronischem Fingerabdruck versehen werden (Lit. 06, S. 22).

B 19.1.3 Authentizität

Die Authentifikation stellt sicher, dass eine Nachricht auch wirklich von dem Absender stammt, der vorgibt, der Absender zu sein. Die Frage: Wie kann Bob sicher sein, dass die Nachricht wirklich von Alice stammt und nicht etwa von Mallory frei erfunden wurde? ist somit die Frage nach der Authentizität, der Echtheit der Nachricht. Erst der sichere Beweis, dass eine Person auch wirklich die ist, die sie vorgibt zu sein, führt beispielsweise beim E-Commerce zu befriedigenden Geschäftsabschlüssen. Um dies sicherzustellen werden Verschlüsselungsverfahren als auch Fingerabdrucksverfahren mit Unterschriftsfunktion (siehe B 19.3.2)

verwendet (Lit. 06, S. 24). Die Wichtigkeit der Authentizität für den elektronischen Geschäftsverkehr zeigt sich im Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz, IuKDG) vom 22. Juli 1997 (http://www.iid.de/rahmen/iukdg.html), das in Art. 3 das Gesetz zur digitalen Signatur (Signaturgesetz, SigG) enthält. Dieses hat zum Zweck, „Rahmenbedingungen für digitale Signaturen zu schaffen, unter denen diese als sicher gelten und Fälschungen digitaler Signaturen oder Verfälschungen von signierten Daten zuverlässig festgestellt werden können" (§ 1 Abs. 1 SigG). Das SigG ist nach Art. 11 IuKDG am 1. August 1997 in Kraft getreten.

B 19.1.4 Verbindlichkeit

Sie soll sicherstellen, dass der Absender einer Nachricht später nicht leugnen kann, dass diese, zum Beispiel eine Bestellung, tatsächlich von ihm stammt. Es wäre durchaus denkbar, dass Alice (fälschlicherweise) nachträglich behauptet, die Nachricht stamme nicht von ihr (Lit. 06, S. 25). Bob hat somit ein Interesse daran sicherzustellen, dass Alice nicht leugnen kann diese Nachricht (so) gesendet zu haben. Die Verbindlichkeit stellt somit die Beweisbarkeit des Ursprungs einer Nachricht sicher. Dazu gehört neben der beschriebenen Authentifizierung auch die sorgfältige Schlüsselgenerierung, die gewährleistet, dass keine andere Person geheime Schlüssel kennen kann. Hinzu kommen Zertifikate, die eine vertrauenswürdige Stelle ausgestellt hat und die untrennbar mit der Identität des Besitzers verbunden sind (siehe B 19.4). Erst diese Verbindlichkeit sichert einen gelungenen Geschäftsabschluss.

B 19.2 Verfahren zur Gewährleistung von Vertraulichkeit

Mit Hilfe sogenannter Konzelationssysteme (lat. celare: verbergen, verheimlichen) lassen sich Nachrichten oder Daten vor unbekannten Mitlesern absichern. Die Auswahl geeigneter kryptografischer Verfahren hängt dabei von der Notwendigkeit ab, die Daten vor dem Zugriff Dritter zu schützen. Der Illusion, dass das verwendete Verschlüsselungsverfahren nicht knackbar ist, sollte man sich allerdings nicht hingeben. Aus der Tatsache, dass stets die Möglichkeit besteht, dass der verwendete Verschlüsselungsalgorithmus einem Dritten bekannt ist (Shannons Maxime), folgt eine weitere Grundregel der Kryptografie, die sogenannte Kerckhoffs Maxime. Die Sicherheit eines kryptografischen Verfahrens beruht nicht auf der Geheimhaltung des verwendeten Algorithmus sondern alleine auf der Geheimhaltung des Schlüssels, der zum Dechiffrieren benötigt wird (Lit. 05, S. 8). Aus ihr folgt, dass ohne Kenntnis des Schlüssels kein Rückschluss vom Geheimtext auf den Klartext möglich ist, selbst bei Bekanntsein des verwendeten Verschlüsselungsalgorithmus.

Die berühmteste Verschlüsselung überhaupt dürfte die von Gaius Julius Caesar sein. Er verschob jeden der 20 Buchstaben des lateinischen Alphabets um drei Stellen nach rechts. Da diese zyklische Vertauschung mathematisch wie eine Addition von 3 (mit den Sonderregeln 18+3=1, 19+3=2, 20+3=3) funktioniert, nennt man das Verfahren auch Caesar-Addition. Die heute älteste bekannte Verschlüsselung stellt jedoch die Skytale von Sparta (5. Jhdt. v. Chr.) dar. Ein Holzstab wurde mit einem schmalen Band aus Pergament spiralförmig umwickelt, der dann der Länge nach mit einer Nachricht beschrieben wurde. Den Text auf dem abgewickelten Pergamentstreifen sollten nur die Generäle lesen können, die über Stäbe vom gleichen Durchmesser verfügten (Lit. 02, S. 3). Im 16. Jhdt. entwickelte Blaise de Vigenère die Caesar-Methode weiter, indem er den Verschiebungsbetrag fortlaufend änderte, es wird somit eine Folge von Zahlen als Schlüssel, z.B. 12, 1, 19, 6, 2 auf den Klartext angewendet. Der erste Buchstabe wird um 12 Zeichen, der zweite um 1 Zeichen usw. verschoben. Nach dem Ende der Folge wird wieder von vorne angefangen. Man könnte sich den Schlüssel auch als Sequenz von Buchstaben (hier NBUGC; A wird um 12 Stellen auf N verschoben, usw.) vorstellen. Das Vigenère-Verfahren machen sich die sogenannten Rotormaschinen wie die Enigma zu Eigen. Sie bestehen aus mehreren hintereinander liegenden drehbaren Scheiben. Jede dieser Scheiben weist vorne und hinten 26 Kontaktflächen auf, für jeden Buchstaben des Alphabets eine. Die Scheiben sind fest verdrahtet. Dies führt zu einer Permutation des Alphabets und somit zu einer einfachen Ersetzung von Buchstaben. Bereits bei drei Rotoren sind Schlüsselwörter mit einer Periodenlänge von 263 = 17.576 Zeichen möglich. Der Schlüssel besteht in der Angabe, welcher Rotor in welcher Reihenfolge einzusetzen ist und wie ihre jeweilige Anfangsstellung aussieht. Die

Enigma bestand aus einer Kombination von bis zu acht austauschbaren Rotoren, die nach jedem Zeichen jeweils um einen anderen Betrag weitergeschaltet wurden. Zusätzlich besaß sie einen Reflektor, der dafür sorgte, dass jedes Zeichen zweimal in unterschiedlicher Richtung das Gerät durchlief, hinzu kam ein weiterer paarweiser Austausch von Zeichen, der je einmal am Anfang und am Ende der Operation durchgeführt wurde. Zum Schlüssel gehörte hier auch die Angabe, wie die Zeichenersetzung vorzunehmen war. Ist der Schlüssel genauso lang wie der zu chiffrierende Text, handelt es sich um das One-Time-Pad (Einmalblock)-Verfahren. Dies ist auch das einzige Verfahren, dessen Sicherheit bewiesen wurde. Natürlich muss bei diesem Verfahren jedes Mal ein neuer Schlüssel verwendet werden (Lit. 02, S. 51).

Die meisten aktuellen Verschlüsselungsverfahren arbeiten mit einem weiteren Trick. In jedem Verschlüsselungsschritt werden nicht Zeichen für Zeichen, sondern ein längerer Klartextblock verarbeitet und durch den Geheimtextblock ersetzt, wobei jedes Klartextzeichen eines Blocks das gesamte Ergebnis beeinflusst (Lit. 06, S. 42). Dadurch werden Regelmäßigkeiten im Klartext über mehrere Zeichen hinweg verteilt (Diffusion). Ein Chiffrierungsschritt muss dabei so beschaffen sein, dass zwei Klartextblöcke, die sich nur in einem Zeichen unterscheiden, zu völlig unterschiedlichen Geheimtextblöcken führen. Diese Verfahren werden Blockverschlüsselungen genannt. Heutzutage werden Methoden mit mindestens 8 Byte, also 64 Bit, verwendet. Bei vielen Verfahren wird der Eingabeblock zu Anfang einer jeden Runde in zwei Hälften (R und L) zerlegt. Die Operationen (Kombination von Addition, Multiplikation, exklusives oder (XOR) und Vertauschungen) werden nur auf den R-Teil angewendet, ihr Ergebnis wird durch XOR mit L verknüpft und bildet die rechte Hälfte des Rundenergebnisses, während die linke Hälfte von dem unveränderten R gebildet wird. So wird für eine Hälfte des Blocks mit der anderen Hälfte Konfusion erzeugt, während die andere Hälfte unverändert bleibt. Diese wird in der jeweils folgenden Runde dem Konfusionsverfahren unterworfen. In jede einzelne Runde gehen Teile des Schlüssels ein. Verfahren mit dieser Methode werden als Feistel-Netzwerke bezeichnet. Die Dechiffrierung gestaltet sich bei Kenntnis des Schlüssels einfach, denn sie läuft in umgekehrter Reihenfolge die Inversen der elementaren Operationen durch und liefert als Ergebnis den Klartext.

B 19.2.1 Symmetrische Verschlüsselung

Symmetrische Kryptografie ist gleichsam die Grundform der Verschlüsselung. Sender und Empfänger haben sich dabei auf einen Schlüssel geeinigt (Secret Key) oder der Dechiffrierschlüssel lässt sich aus dem Chiffrierschlüssel berechnen und umgekehrt (Lit. 01, S. 154). Symmetrische Verschlüsselungsverfahren werden auch als Secret-Key-Verfahren bezeichnet.

B 19.2.1.1 DES und seine Varianten

Das bekannteste und am weitesten verbreitete symmetrische Verschlüsselungsverfahren ist der Data Encryption Standard (DES). Es wurde 1976 in den Vereinigten Staaten als Bundesstandard anerkannt, es benutzt eine Blocklänge von 64 sowie Schlüssellänge von 56 Bit und wird 16mal durchlaufen. Er wird unter anderem bei der Abwicklung von Bargeldauszahlungen mit einer eurocheque-Karte verwendet. DES ist auf Standardrechnern in Wochen bis Monaten zu knacken. Anfang 1999 war es möglich, durch die Nutzung der Leerlaufzeit vieler per Internet verbundener Computer, eine durch DES verschlüsselte Nachricht innerhalb von 23 Stunden zu dechiffrieren. Erreicht wurde dies einfach durch das Ausprobieren aller möglichen Schlüssel (Brute-Force-Attack). Spezialrechner brauchen für die gleiche Aufgabe nur einen Bruchteil dieser Zeit. Eine auch heute noch sichere Variante von DES ist Triple-DES, die dreimalige, hintereinander geschaltete Anwendung von DES. Die Schlüssellänge steigt dadurch auf 168 Bit (etwa 3,74x1050 mögliche Schlüssel). Derzeit läuft eine Ausschreibung des NIST (National Institute of Standards and Technology) für den Advanced Encryption Standard (AES), den Nachfolger von DES. Bei AES soll es sich um eine frei verfügbare symmetrische 128-Bit-Blockchiffre mit Schlüssellängen von 128, 192 und 256 Bit handeln, die schneller als Triple-DES arbeitet. Der IDEA (International Data Encryption Algorithm) wurde 1990 an der Eidgenössischen Technischen Hochschule in Zürich entwickelt, er hat eine Blocklänge von 64 Bit, eine Schlüssellänge von 128 Bit und wird 8 mal durchlaufen. IDEA ist besonders in Software effizient umzusetzen, da alle Rechenvorgänge in 16-Bit-Register durchgeführt werden. Ein weiterer Vorteil von IDEA ist, dass bei einer Schlüssellänge von 128 Bit Brute-Force-Attacken nicht mehr durchführbar sind (Lit. 06, S. 56). Als AES-Nach-

folger ist der Algorithmus allerdings nicht geeignet, zudem ist IDEA noch bis 2011 patentrechtlich geschützt. Einen guten Kompromiss zwischen Sicherheit und Verfügbarkeit stellt der Blowfish-Algorithmus von Bruce Schneier da. Die Blocklänge beträgt 64 Bit, die Schlüssellänge kann bis zu 448 Bit beliebig gewählt werden und der Algorithmus wird 16 mal durchlaufen.

B 19.2.2 Asymmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung besteht immer die Notwendigkeit den zu verwendenden Schlüssel über einen sicheren Kanal auszutauschen. Mitte der Siebziger Jahre veröffentlichten Whitfield Difflie und Martin Hellman sowie unabhängig von ihnen Ralph Merkle ein Verfahren, das dieses Problem löst, indem zum Chiffrieren ein anderer Schlüssel als zum Dechiffrieren verwendet wird (asymmetrisches Verfahren). Zusätzlich sollte es nicht möglich sein aus der Kenntnis eines Schlüssels den anderen abzuleiten. Wer ein solches Verfahren nutzt, muss zunächst ein Paar zusammengehörender Schlüssel generieren. Einen der beiden Schlüssel hält er geheim (Private Key), den anderen gibt er der Öffentlichkeit bekannt (Public Key). Diese Verfahren werden auch Public-Key-Verfahren genannt. Jeder, der nun eine verschlüsselte Nachricht an eine Person schicken will, besorgt sich deren öffentlichen Schlüssel, verschlüsselt seine Nachricht damit und verschickt den Geheimtext. Dieser so chiffrierte Text kann nur vom Empfänger mit seinem privaten Schlüssel dechiffriert werden (Lit. 02, S. 94). Von zentraler Bedeutung ist dabei, dass der Empfänger der Nachricht den Schlüssel vorgibt, nicht etwa der Sender.

B 19.2.2.1 RSA

RSA, benannt nach den Entwicklern Ronald L. Rivest, Adi Shamir und Leonard M. Adleman, ist das bekannteste Public-Key-Verfahren und ein Quasi-Standard im Internet. Das Prinzip beruht darauf, dass es kein Problem darstellt, zwei große Primzahlen miteinander zu multiplizieren, es aber praktisch unmöglich ist, aus dem Produkt wieder die beiden Faktoren zu ermitteln. Dabei ist zu beachten, dass die beiden Faktoren sich in ihrer Länge deutlich unterscheiden. In praktischen Anwendungen variiert das Produkt zwischen 512 Bits (geringe Sicherheit) und 2048 Bits (sehr hohe Sicherheit) (Lit. 01, S. 207). Es wird allgemein angenommen, dass der Aufwand zur Wiederherstellung des Klartextes aus dem Chiffretext und dem öffentlichen Schlüssel äquivalent zur Faktorisierung des Produktes der beiden Primzahlen ist, allerdings gibt es dafür keinen Beweis. RSA ist um den Faktor 100 bis 1000 langsamer als DES. Dies mag als ein Nachteil von RSA erscheinen, ist aber tatsächlich eher von Vorteil. Denn für die Ver- und Entschlüsselung von normalen Mitteilungen fällt diese Zeit praktisch nicht ins Gewicht. Wer aber RSA mittels einer Brute-Force-Attacke brechen möchte, tut sich umso schwerer, je langsamer der Algorithmus ist.

B 19.2.2.2 ElGamal

Das Prinzip des 1985 von Taher ElGamal entwickelten Algorithmus beruht auf dem Problem des „diskreten Logarithmus“ (Lit. 03, S. 127). In praktischen Anwendungen variiert die Schlüssellänge zwischen 512 Bits (geringe Sicherheit) und 1024 Bits (sehr hohe Sicherheit). Eine Variante des ElGamal-Verfahrens ist der 1991 entwickelte Digital Signature Algorithm (DSA), der 1994 vom NIST zum Digital Signature Standard (DSS) erklärt wurde (Lit. 05, S. 555).

B 19.2.3 Hybride Verschlüsselung

Da asymmetrische Verschlüsselungssysteme in der Regel sehr viel langsamer arbeiten als symmetrische Algorithmen, werden bei den im Internet gebräuchlichen Verschlüsselungsprogrammen häufig beide Verfahren eingesetzt. Bei einem Verbindungsaufbau erzeugt der Sender einen zufälligen Sitzungsschlüssel (Session Key), mit dem er die Nachricht verschlüsselt. Der Session Key wird mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und zusammen mit der verschlüsselten Nachricht verschickt. Der Empfänger kann dann mit seinem privaten Schlüssel den asymmetrisch chiffrierten Schlüssel dechiffrieren und so die symmetrisch chiffrierte Nachricht dechiffrieren. Durch diese Kombination (hybride Verschlüsselung) vereinigt man einen gesicherten, aber langsamen Schlüsseltausch mit einer schnellen, aber weniger sicheren Verschlüsselung.

B 19.3 Verfahren zur Gewährleistung der Integrität und der Authentizität

Moderne kryptografische Verfahren lassen sich aber nicht nur einsetzen um Vertraulichkeit sondern auch die anderen drei Ziele (Integrität, Authentizität und Verbindlichkeit) zu erreichen. Man spricht dabei von Authentifikationssystemen. Um dies zu erreichen sind sogenannte Hashfunktionen notwendig. Hashfunktionen sind mathematische Methoden, die aus einem beliebigen Klartext nach einem bestimmten Verfahren einen Fingerabdruck (Hashwert, Message Digest – MD) der Nachricht generieren. Die Funktion verwandelt einen Klartext so in einen MD, dass auch die kleinste Veränderung des ursprünglichen Texts zu einem gänzlich anderen MD führt. Es gehört zu den Forderungen, dass aus dem einmal erzeugten MD der ursprüngliche Text nicht wieder rekonstruiert werden kann. Hashfunktionen sind nicht umkehrbar und gelten somit als Einwegfunktionen. Anders als beim Chiffrieren ist eine Wiederherstellung des Klartextes nicht möglich. Der Vorteil dieses Verfahrens liegt in der Tatsache, dass anstatt des gesamten Textes lediglich ein kurzer MD besonders geschützt werden muss. Die zur Zeit bekanntesten Hashfunktionen sind u.a. SHA-1 (Secure Hash Algorithm One), er wurde von der NSA (National Security Agency) entwickelt und als US-Standard angenommen. Der Hashwert hat eine Länge von 160 Bit. MD5, wurde von Rivest entwickelt und im Zusammenhang mit dem PEM-Standard (Privacy Enhanced Mail) vorgestellt. Der Algorithmus erzeugt einen MD von 128 Bit Länge. RIPEMD (RIPE-Message Digest) wurde im Rahmen des EU-Projektes RIPE (RACE Integrity Primitives Evaluation, 1988-1992) von Dobbertin, Bosselaers und Preneel entwickelt. Der MD ist entweder 128 Bit (RIPEMD-128) oder 160 Bit (RIPEMD-160) lang. Generell bieten Hashfunktionen mit längeren Prüfziffern höhere Sicherheit. RIPEMD-160 scheint sich in Europa und SHA-1 in den USA als de facto-Standard durchzusetzen.

B 19.3.1 Symmetrische Authentifikationssysteme

Der Sender verschlüsselt den MD einer Nachricht und sie selbst mit dem Secret Key und sendet beide an den Empfänger. Der Empfänger dechiffriert den MD und die Nachricht. Durch erneute Anwendung der Hashfunktion auf die Nachricht und Vergleich des Ergebnisses mit dem entschlüsselten MD kann er feststellen, ob die Nachricht während der Übertragung verändert wurde (Lit. 02, S. 69). Ein solches System hat einige Nachteile. Zum einen kann nur eine Person, die den geheimen Schlüssel kennt, eine solche Überprüfung vornehmen; wünschenswert wäre aber in vielen Situationen, dass jeder Beliebige die Echtheit einer Nachricht überprüfen kann. Zum anderen kann jeder, der über den zur Überprüfung nötigen Schlüssel verfügt, auch authentifizierte Nachrichten erstellen. Das bedeutet, dass das System in Gruppen von mehr als zwei Teilnehmern dem Empfänger keine Auskunft mehr darüber gibt, von wem eine bestimmte Nachricht eigentlich stammt, und dass es auch bei nur zwei Teilnehmern stets möglich ist, das Erstellen einer bestimmten Nachricht abzustreiten. Den MD könnte genauso gut der Kommunikationspartner verschlüsselt haben, denn auch er hat den Schlüssel (Lit. 04, S. 108). Integrität und Authentizität einer Nachricht werden also nur gegen Angriffe von außen stehenden Personen gesichert, Verbindlichkeit dagegen wird überhaupt nicht erreicht.

B 19.3.2 Asymmetrische Authentifikationssysteme

Erst die Kombination aus asymmetrischer Verschlüsselung und Hashwert bietet die Möglichkeit, ein Analogon zur menschlichen Unterschrift zu erzeugen, in diesem Zusammenhang wird von digitalen Signaturen gesprochen (Lit. 02, S. 115). Will jemand eine Nachricht als von ihm erstellt ausweisen (quasi unterzeichnen), wendet er eine Hashfunktion auf diese Nachricht an, den MD verschlüsselt er mit seinem Private Key und hängt das Ergebnis als digitale Signatur der zu übertragenden unverschlüsselten Nachricht an. Jeder, der im Besitz des zugehörigen Public Key ist, kann die Echtheit der Nachricht überprüfen, indem er den MD dechiffriert und diesen vergleicht mit dem von ihm neu berechneten MD, der sich aus der unverschlüsselten Nachricht ergibt (gleiche Hashfunktion). Sind diese Werte identisch, wurde die Nachricht unterwegs nicht verändert. Signieren kann die Nachricht nur der Besitzer des Private Keys, so dass Integrität, Authentizität und Verbindlichkeit realisiert werden können. Allerdings kann bei diesem Verfahren jeder den Klartext lesen. Will man noch Vertraulichkeit sicher stellen, muss das Verfahren erweitert werden (elektronischer Umschlag). Der mit dem Private Key des Senders chiffrierte MD

wird der Nachricht angehängt. Die auf diese Weise verlängerte Nachricht wird mit dem Public Key des Empfängers chiffriert und übermittelt. Der Empfänger dechiffriert die verlängerte Nachricht mit seinem Private Key und trennt den immer noch chiffrierten MD von der nun dechiffrierten Nachricht ab, den er mit dem Public Key des Senders dechiffriert. Er berechnet selbst den MD der Nachricht und vergleicht diesen mit dem vom Sender übermittelten MD. Stimmen sie überein, kann er sicher sein, dass die Nachricht vom Sender stammt, unterwegs nicht verändert und von keinem Dritten belauscht wurde (Lit. 06, S. 114).

B 19.4 Zertifizierungsinstanzen

Noch bleibt das Problem zu lösen, dass kein nachvollziehbarer Zusammenhang zwischen einem Private Key und der vorgeblich zu ihm gehörenden Person besteht. Jemand kann sich als eine andere Person ausgeben, indem er unter deren Namen einen selbst erzeugten Private Key in Umlauf bringt. Dieses Problem wird durch das Einschalten eines vertrauenswürdigen Dritten gelöst, der sich für die Identität einer Person verbürgt. Dies kann über Vertrauensnetzwerke (Web of Trust) oder offizielle Zertifizierungsinstanzen (Certification Authority – CA, Trustcenter – TC) geschehen. CAs liefern mit digitalen Zertifikaten und Schlüsseln die Grundausstattung zur Teilnahme am rechtsverbindlichen und vertraulichen elektronischen Geschäftsverkehr. Sie überprüfen zunächst die Identität des Nutzers und generieren einen elektronischen Ausweis, das Zertifikat, das bestätigt, dass der Public Key wirklich der beantragenden Person gehört (Lit. 03, S. 208). An dieses CA kann sich der Empfänger wenden und den Public Key des Senders abrufen. Das Format solcher Zertifikate lässt sich standardisieren, so dass sie automatisch auswertbar sind.

Literatur

01 Bauer, Friedrich L.: Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie. 3., überarb. Aufl. Berlin, Heidelberg, New York: Springer-Verlag, 2000, 503 S.

02 Beutelspacher, Albrecht: Kryptologie. Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen; ohne alle Geheimniskrämerei, aber nicht ohne hinterlistigen Schalk, dargestellt zum Nutzen und Ergötzen des allgemeinen Publikums. 6., überarb. Aufl. Braunschweig; Wiesbaden: Vieweg, 2002, 152 S.

03 Buchmann, Johannes: Einführung in die Kryptographie. Berlin, Heidelberg: Springer, 1999, 229 S.

04 Grimm, Rüdiger: Kryptoverfahren und Zertifizierungsinstanzen. In: Datenschutz und Datensicherheit (DuD), 1996, S. 27-36

05 Schneier, Bruce: Angewandte Kryptographie. Protokolle, Algorithmen und Sourcecode in C. 1., korr. Nachdr. Bonn: Addison-Wesley, 1996, 844 S.

06 Selke, Gisbert: Kryptographie. Verfahren, Ziele Einsatzmöglichkeiten. 1. Aufl. Köln: O'Reilly, 2000, 225 S.