Einführung in die Kryptographie und Kryptoanalyse

Seminararbeit im Seminar

„Kryptographische Verfahren und ihre Anwendung“

VAK 03-794

Wintersemester 2000/01

Universität Bremen

Eilert Brinkmann

15. Februar 2001

Inhaltsverzeichnis

Vorwort

Diese Seminararbeit „Einführung in die Kryptographie und Kryptoanalyse“ ist die schriftliche Ausarbeitung des gleichnamigen Auftakt-Referats im Seminar „Kryptographische Verfahren und ihre Anwendung“ am 15. November 2000. Sie soll einen Überblick über dieses Themengebiet geben, um auf die nähere Beschäftigung mit einzelnen Verfahren und Anwendungen vorzubereiten, sowie einige allgemeine Aspekte rund um Kryptographie kurz beleuchten.

Dazu werden nach der Einführung von Grundbegriffen sowie einem kurzen Überblick über die historische Entwicklung und gegenwärtige Anwendungsfelder grundlegende kryptographische Konzepte und Klassen von Verfahren vorgestellt. Dies schließt auch einen Blick auf organisatorische Aspekte ein. Abschließend werden nach einem Einblick in das Gebiet der Kryptoanalyse noch einige gesellschaftliche Rahmenbedingungen angesprochen.

Es ist ausdrücklich nicht Ziel dieser Arbeit, detailliert auf konkrete kryptographische Verfahren einzugehen oder deren mathematische Grundlagen ausführlich zu beschreiben.

Die Hauptquellen, auf denen diese Arbeit basiert, sind [10] und [4]. Andere relevante Quellen werden jeweils an der Stelle ihrer Verwendung angegeben.

1 Überblick

1.1 Grundbegriffe

Wenn durch die Wahl des Transportwegs nicht von vornherein ausgeschlossen werden kann, daß geheime Nachrichten während ihres Transports vom Absender zum Empfänger in die Hände Dritter gelangen, so müssen diese Nachrichten während der Übermittlung irgendwie gegen unbefugte Zugriffe geschützt werden.

Eine Möglichkeit, vertrauliche Nachrichten dem Zugriff durch Unbefugte zu entziehen, besteht darin, bereits die bloße Existenz dieser Nachrichten zu verbergen. Dieses ist das Ziel der **Steganographie**, der Kunst, geheime Informationen so in anderen, unverfänglich wirkenden Nachrichten zu verbergen, daß sie nur für in das Verfahren eingeweihte Empfänger wiederzuentdecken sind. Solche Verfahren werden im folgenden jedoch nicht näher betrachtet.

Wird die Tatsache, daß eine geheime Nachrichtenübermittlung stattfindet, vor Dritten nicht verborgen, so läßt sich zumindest der Inhalt der Nachricht durch **Verschlüsselung** vor Kenntnisnahme durch Unbefugte schützen. Dabei wird die Nachricht zur Übertragung in einer Weise unleserlich gemacht, die die Rückumwandlung in den ursprünglichen Text nur Empfängern ermöglicht, die im Besitz eines bestimmten, geheimen Schlüssels sind. Eine Methode zur Verschlüsselung wird auch als **Chiffre** bezeichnet, die Vorgänge des Ver- und Entschlüsselns dementsprechend als Chiffrieren bzw. Dechiffrieren.

Die Kunst der Geheimhaltung von Nachrichten durch Verschlüsselung heißt **Kryptographie**. Neben der reinen Geheimhaltung widmet sich die Kryptographie noch weiteren Sicherheitsaspekten bei der Nachrichtenübermittlung (siehe Abschnitt 1.2). Das Gegenstück dazu, die Analyse von kryptographischen Verfahren und verschlüsselten Nachrichten mit dem Ziel, Verschlüsselungen zu brechen, ist Gegenstand der **Kryptoanalyse**. Der Begriff **Kryptologie** bezeichnet schließlich die Wissenschaft, die Kryptographie und Kryptoanalyse in sich vereint. Dieser Bereich soll Gegenstand der folgenden Kapitel sein.

1.2 Ziele kryptographischen Schutzes

Zwar lautet die Übersetzung des Wortes Kryptographie „Geheimschrift“, doch gehen die heute von der Kryptographie umfaßten Augaben über diese Bedeutung des Wortes hinaus. Dennoch ist die Geheimhaltung wohl nach wie vor die offensichtlichste und bekannteste Anwendung kryptographischer Verfahren. Dieses Ziel wird auch als **Vertraulichkeit** bezeichnet. Hier geht es darum, eine Nachricht vor unbefugter Einsichtnahme durch Dritte zu schützen.

Ein weiteres Ziel ist die Überprüfbarkeit der **Integrität** einer Nachricht, das heißt, es soll für den Empfänger nachprüfbar sein, daß er die Nachricht unversehrt

erhalten hat. Während die Erkennung von zufälligen Veränderungen, etwa durch technische Störungen, auch mit einfacheren Mitteln möglich ist, erfordert der Schutz gegen gezielte Manipulationen den Einsatz kryptographischer Verfahren.

Eng damit verbunden ist der Wunsch nach **Authentizität**: Die Identität des Absenders einer Nachricht soll für den Empfänger nachprüfbar sein. Gleiches trifft auf die **Gültigkeit** der Nachricht zu, denn selbst eine ursprünglich vom richtigen Absender stammende Nachricht kann den Empfänger bei späterer Zustellung zu einer falschen Reaktion veranlassen, wenn sie durch zwischenzeitliche Ereignisse ihre Bedeutung verloren hat. Eng damit verbunden ist auch der z. B. im Zusammenhang mit Vertragsabschlüssen auftretende Wunsch nach **Nichtabstreitbarkeit**, womit gemeint ist, daß der Absender einer Nachricht seine Urheberschaft später nicht verleugnen kann. Der wesentliche Unterschied liegt dabei darin, daß auch ein authentischer Absender als potentieller Gegner anzusehen ist.

1.3 Historische Entwicklung

Die Benutzung einfacher kryptographischer Verfahren ist bereits seit dem Altertum überliefert. Das älteste bekannte Verschlüsselungsverfahren ist die Skytala, die bereits um ca. 400 v. Chr. von den Griechen verwendet wurde. Dabei wird ein Papyrusstreifen spiralförmig um einen Stab festen Durchmessers gewickelt und in Stab-Längsrichtung zeilenweise ein Text darauf geschrieben. Nach dem Abrollen des Streifens ist der Text dann nicht mehr ohne weiteres lesbar. Um den Originaltext wieder erkennbar zu machen, muß der Streifen erneut um einen Stab des gleichen Durchmessers gewickelt werden. Der Stabdurchmesser stellt hier also den zur Entschlüsselung notwendigen geheimen Schlüssel dar.

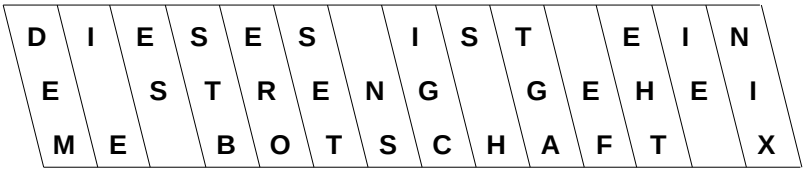

Abbildung 1: Beispiel zur Anwendung der Skytala

Das Beispiel in Abbildung 1 skizziert (auf die Ebene abgebildet) einen solchen aufgewickelten Streifen, der mit drei Zeilen beschriftet ist. Nach dem Abwickeln ist auf diesem Streifen dann nur noch die Zeichenfolge

```
DEMI EES STBEROSET NSIGCS HTGA EFEHTIE NIX
```

zu erkennen. Der Aufwand zum Brechen dieser Verschlüsselung beschränkt sich allerdings auf das Herausfinden des richtigen Stabdurchmessers, womit nur eine geringe Sicherheit geboten wird.

Ein weiteres einfaches Verschlüsselungsverfahren geht auf den römischen Kaiser Cäsar zurück. Diese nach ihm benannte Cäsar-Chiffre verschlüsselt einen Text, indem sie jeden Buchstaben durch den Buchstaben ersetzt, der im Alphabet drei Positionen weiter hinten steht. Damit wird z. B. der Text

```
DIESE NACHRICHT IST GEHEIM
```

durch die Zeichenfolge

```
GLHVH QDFKULFKW LVW JHKHLP
```

ersetzt[1] — ebenfalls eine sehr einfache Chiffre, die keine hohe Sicherheit bietet.

Die klassische Anwendung von Kryptographie liegt vor allem im militärischen und nachrichtendienstlichen Bereich sowie beim Einsatz durch Diplomaten, wo es gilt, Nachrichten sicher durch feindliches Gebiet zu bringen: Gegner sollen daran gehindert werden, abgefangene Nachrichten zu lesen und daraus militärische oder politische Vorteile zu ziehen. Dies ist auch heute noch einer der Hauptanwendungsbereiche von Kryptographie.

Nachdem Kryptographie anfangs mit einfachen manuellen Verfahren praktiziert wurde, wurden die Methoden im Laufe der Zeit verfeinert und nahmen dabei an Komplexität zu. Die Entwicklung mechanischer Hilfsmittel ermöglichte aufwendigere Chiffren, die Angriffe weiter erschwerten. Ein Beispiel für eine Verschlüsselungsmaschine ist die *Enigma*, die vor allem aufgrund ihrer Verwendung durch die deutschen Streitkräfte während des zweiten Weltkriegs bekannt wurde. Trotz des für damalige Verhältnisse relativ aufwendigen Verfahrens gelang es den Briten, diese Verschlüsselung zu brechen — nicht zuletzt durch Schwächen in deren Implementierung und Nachlässigkeit bei der Benutzung. [5]

Die heutige Nutzung von Kryptographie erfolgt praktisch immer unter Verwendung von elektronischen Hilfsmitteln, da die inzwischen notwendigen, sehr aufwendigen Verfahren anders nicht realisierbar wären. Dabei gibt es sowohl Realisierungen von kryptographischen Funktionen in Hardware, die speziell für diese Aufgaben optimiert ist, als auch Implementierungen in Software, die auf gewöhnlichen Rechnern verwendet werden können und in vielen Anwendungen eingesetzt werden.

1.4 Heutige Anwendungsbereiche

Die Anwendung von Kryptographie ist heutzutage weit verbreitet. So kommt Verschlüsselung überall dort zum Einsatz, wo eine geschützte Speicherung oder Übertragung von vertraulichen Daten erforderlich ist. Dies kann beispielsweise

[1] Das Beispiel verwendet der Einfachheit halber unser heutiges Alphabet.

dem Schutz von Geschäftsgeheimnissen dienen, aber auch die sichere Durchführung elektronischer Transaktionen ist von zunehmendem Interesse. Daneben bestehen die gewohnten Anwendungen durch staatliche Stellen nach wie vor fort. Ein großes Anwendungsfeld hat sich ferner durch die Verbreitung des Mobilfunks ergeben, da Funkverbindungen ohne besondere Schutzmaßnahmen Angreifern durch den fehlenden physikalischen Zugangsschutz naturgemäß ein leichtes Ziel bieten.

Besondere Bedeutung hat Kryptographie dort, wo es die Kommunikation über öffentliche Netze zu schützen gilt. Dies gilt insbesondere für das durch seine offene Struktur kaum geschützte Internet, aber z. B. auch für herkömmliche Telefonnetze. Allerdings ist trotz der bestehenden Unsicherheiten die freiwillige Benutzung von Kryptographie bei der alltäglichen Kommunikation längst nicht die Regel. So werden etwa die durchaus bestehenden Möglichkeiten zur Verschlüsselung von E-Mails in vielen Bereichen noch wenig genutzt.

1.5 Bedrohungsszenarien und Lösungsansätze

Es sind vielfältige Angriffe auf übermittelte Nachrichten bzw. gegen deren Sender oder Empfänger denkbar, wenn unbefugte Eingriffe in die Kommunikation nicht von vornherein — etwa durch persönliche Überbringung — ausgeschlossen sind. Eine Gefahr besteht dabei darin, daß Dritte Kenntnis vom Inhalt einer vertraulichen Nachricht erhalten. Ein Schutz dagegen ist durch eine Verschlüsselung möglich, die nur dem rechtmäßigen Empfänger der Nachricht die Rückgewinnung des ursprünglichen Inhalts ermöglicht.

Kann ein Angreifer die Nachrichtenübertragung nicht nur beobachten, sondern auch aktiv beeinflussen, so besteht ein weiteres Risiko in unbefugten Veränderungen einer Nachricht während des Transports. Ebenso ist damit zu rechnen, daß ein Angreifer selbst erstellte Nachrichten mit gefälschter Absenderangabe verschickt. Beides kann den Empfänger zu irrigen Annahmen über die Absichten des (vermeintlichen) Absenders führen. Damit wäre es beispielsweise möglich, im Namen eines anderen Aufträge (z. B. Warenbestellungen, Überweisungsaufträge an eine Bank, etc.) zu erteilen, die dessen tatsächlichen Interessen zuwiderlaufen. Zum Schutz gegen solche Angriffe können kryptographische Verfahren zur Wahrung von Integrität und Authentizität zum Einsatz kommen, wie sie in Abschnitt 4 näher beschrieben werden.

Schließlich ist es auch denkbar, daß ein Angreifer mitgelesene Nachrichten zu einem späteren Zeitpunkt erneut sendet oder auch, entsprechenden Zugriff auf den Transportweg vorausgesetzt, Nachrichten verzögert oder ganz unterdrückt. Schäden könnten dabei etwa durch mehrfach, zu spät oder gar nicht ausgeführte Aufträge entstehen. Als Schutz können bei Bedarf geeignete Mechanismen eingesetzt werden, die zumindest die Erkennung solcher Manipulationen ermöglichen. Verzögerungen oder das Ausbleiben von Nachrichten zu verhindern ist dagegen kaum möglich.

1.6 Kanalmodell

Eine allgemeine Möglichkeit, den Ansatzpunkt kryptographischer Schutzverfahren im Kommunikationsablauf zu illustrieren, ist das Kanalmodell. In seiner Grundform ohne Schutzmaßnahmen ist dieses Modell in Abbildung 2 dargestellt.

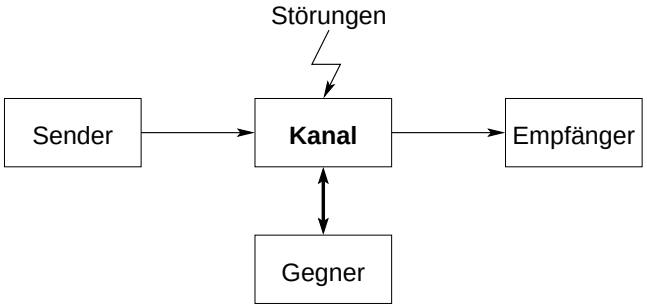

Abbildung 2: Allgemeines Kanalmodell

Der Weg, auf dem eine Nachricht vom Sender zum Empfänger gelangt, wird als Kanal bezeichnet. Um die universelle Verwendung des Modells zu ermöglichen, kann es sich bei dem Kanal neben einem Übertragungsmedium zur Überwindung einer räumlichen Distanz auch um ein Speichermedium handeln, auf dem die Nachricht quasi zur Überbrückung einer zeitlichen Distanz abgelegt wird. In diesem Fall ist es auch zulässig, daß der „Empfänger“ mit dem „Sender“ identisch ist. Somit läßt sich dieses Modell sowohl auf die Nachrichtenübermittlung als auch auf die Speicherung von Daten anwenden.

Der Kanal ist der Ort, an dem die Nachricht potentiell durch äußere Einflüsse gefährdet ist. Solche Einflüsse können zum einen technische Störungen der Übertragung sein. Die Erkennung und Korrektur solcher zufälligen Störungen erfordert allerdings keinen Einsatz von Kryptographie, sondern fällt in den Bereich von Codierungstheorie und Signalverarbeitung und wird im folgenden nicht weiter betrachtet.

Hier soll es vielmehr um die Gefährdung der Nachricht durch gezielte Angriffe gehen. Solange die Nachricht nicht besonders geschützt ist, hat ein Angreifer mit physikalischem Zugang zum Kanal freien Zugriff auf die Nachricht. Er kann also den Inhalt der Nachricht lesen und unter Umständen auch beliebig modifizieren, ohne daß dies für den Empfänger erkennbar wäre.

Dagegen kann eine Nachricht kryptographisch geschützt werden. Zum Schutz vor unbefugtem Mitlesen wird die Nachricht vom Sender unter Verwendung eines Schlüssels chiffriert und passiert den Kanal somit nur in verschlüsselter Form. Nur der berechtigte Empfänger kann die Nachricht unter Verwendung des richtigen Schlüssels wieder entschlüsseln und so auf ihren Inhalt zugreifen. Einem Gegner mit Zugriff auf den Kanal erschließt sich die Bedeutung der Nachricht dagegen

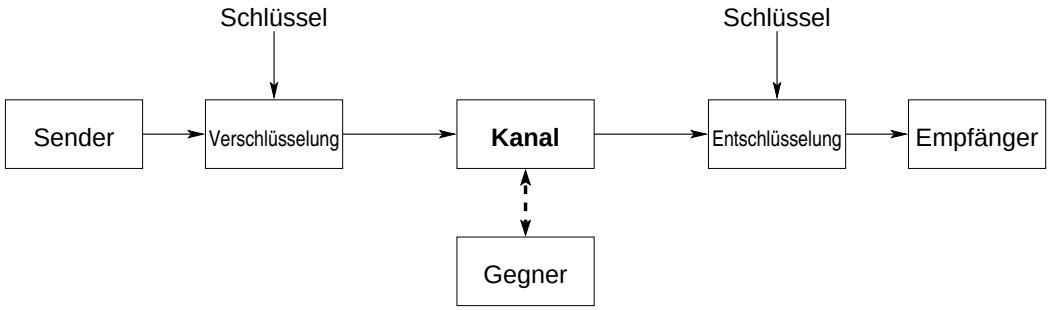

Abbildung 3: Der kryptographische Kanal

nicht. Dieser kryptographisch geschützte Kanal ist in Abbildung 3 dargestellt. In ähnlicher Weise können auch unbefugte Manipulationen an der Nachricht durch Einsatz krytographischer Mittel für den Empfänger erkennbar gemacht werden.

2 Chiffre-Arten

Abhängig davon, in welchen Einheiten Klar- bzw. Chiffretext verarbeitet werden und in welcher Weise der Klartext verändert wird, können mehrere Arten von Chiffren unterschieden werden.

2.1 Block- vs. Stromchiffre

Eine **Blockchiffre** operiert immer auf Klartextblöcken fester Länge. Dazu wird die zu verschlüsselnde Nachricht gegebenenfalls mit Füllzeichen auf ein Vielfaches der verwendeten Blockgröße aufgefüllt und in gleichgroße Blöcke aufgeteilt. Typischerweise werden alle Klartextblöcke mit dem gleichen Schlüssel und unabhängig von ihrer Position in der Nachricht verschlüsselt. Es gibt aber auch Varianten, die Verknüpfungen zwischen benachbarten Blöcken herstellen, um so etwa die Schwäche zu umgehen, daß sonst gleiche Klartextblöcke immer zum gleichen Chiffretextblock führen.

Dagegen wird bei einer **Stromchiffre** die zu verschlüsselnde Nachricht als Datenstrom aufgefaßt und zeichenweise mit einem Schlüsselstrom verknüpft. Bei diesem Schlüsselstrom handelt es sich um eine Pseudozufallsfolge, die nur mit Kenntnis eines geheimen Schlüssels, den sowohl Sender als auch Empfänger besitzen müssen, erzeugt werden kann. Eine Möglichkeit zur Erzeugung eines solchen Schlüsselstroms ist die Verwendung einer Blockchiffre in einer besonderen Betriebsart, in der sie nicht direkt zur Verschlüsselung des Klartextes eingesetzt wird, sondern durch Anwendung auf bekannte Ausgangswerte eine durch den geheimen Schlüssel bestimmte, pseudozufällige Zeichenfolge generiert. Im Gegensatz zu Blockchiffren ist die Verschlüsselung bei Stromchiffren positionsabhängig.

Ein beliebiger Abschnitt des Chiffretextes läßt sich also nicht entschlüsseln, ohne zuvor den gesamten vorhergehenden Teil der Nachricht zu entschlüsseln.

Wenn es erforderlich ist, direkt auf beliebige Teile des Chiffretextes zugreifen zu können, muß folglich eine Blockchiffre zum Einsatz kommen. Ein Beispiel für eine solche Anwendung ist die verschlüsselte Ablage einer Datenbank mit wahlfreiem Zugriff auf alle Datensätze. Eine Stromchiffre ermöglicht es wiederum, bei einem erst langsam entstehenden Klartext jedes Zeichen sofort zu verschlüsseln, ohne erst bis zum Erreichen einer vorgegebenen Blockgröße sammeln zu müssen. So finden Stromchiffren zum Beispiel Verwendung, wenn es darum geht, Eingaben von einem Terminal verschlüsselt zu einem Server zu übertragen, wobei jedes Zeichen sofort nach seiner Eingabe übermittelt werden soll.

2.2 Transpositions- und Substitutionschiffre

Je nach der Weise, auf die eine Chiffre auf den Klartext einwirkt, werden insbesondere zwei grundlegende Verfahren unterschieden. Eine **Transpositionschiffre** überführt Klartext in Chiffretext, indem sie die Anordnung der Zeichen verändert. Bei einer Blockchiffre läßt sich dies leicht so vorstellen, daß die Zeichen, aus denen ein Klartextblock besteht, in eine durch den Schlüssel bestimmte neue Reihenfolge gebracht werden. Ein Beispiel für eine reine Transpositionschiffre ist die in Abschnitt 1.3 vorgestellte Skytala.

Eine **Substitutionschiffre** ersetzt dagegen jedes Zeichen des Klartextes durch ein zugeordnetes Chiffretextzeichen, stellt also im einfachsten Fall eine Abbildung zwischen einem Klar- und einem Chiffretextalphabet dar. Die in Abschnitt 1.3 vorgestellte Caesar-Chiffre stellt eine sehr einfache Substitutionschiffre dar. Eine Chiffre, bei der einem Klartextzeichen immer das gleiche Chiffretextzeichen zugeordnet wird, ist allerdings sehr anfällig für Angriffe durch Analyse der Häufigkeiten der einzelnen Zeichen, weshalb solche monoalphabetischen Substitutionschiffren in der Praxis nicht mehr zum Einsatz kommen. Etwas sicherer sind polyalphabetische Chiffren, bei denen die Ersetzungsregel in Abhängigkeit vom Schlüssel mit jedem Zeichen wechselt.

Da einfache Transpositions- und Substitutionschiffren für sich genommen nicht sehr sicher sind, kommen in der Praxis typischerweise Varianten zum Einsatz, die schwerer zu analysierende Abbildungen erzeugen. Oft werden auch beide Chiffrearten miteinander zu sogenannten Produktchiffren kombiniert, um die Komplexität weiter zu steigern.

3 Kryptosysteme

3.1 Elemente eines Kryptosystems

Mathematisch gesehen besteht ein Kryptosystem aus dem Klartext (M), Chiffretext (C), Chiffrierabbildung (E) und -schlüssel (K) sowie Dechiffrierabbildung (D) und -schlüssel (K'). Dabei stehen diese Elemente derart zueinander in Beziehung, daß für beliebige M gilt:

$$C = E(K, M) \Leftrightarrow M = D(K', C)$$

Die Menge aller möglichen Schlüssel K wird als Schlüsselraum bezeichnet. Die Sicherheit eines Kryptosystems hängt zum einen von der Größe des Schlüsselraums, zum anderen aber auch von der Güte von E ab. Es ist offensichtlich, daß bei einem größeren Schlüsselraum der Aufwand zum Ausprobieren aller möglichen Schlüssel ebenfalls größer ist. Ein entsprechender Gewinn an Sicherheit setzt aber voraus, daß E so gewählt ist, daß es keinen kürzeren Weg zum Dechiffrieren der Nachricht gibt.

In einem symmetrischen Kryptosystem sind Chiffrier- und Dechiffrierschlüssel identisch oder stehen in einem einfachen Zusammenhang. Dagegen spricht man von einem asymmetrischen Kryptosystem, wenn die alleinige Kenntnis des Chiffrierschlüssels nicht ausreicht, um davon auf den Dechiffrierschlüssel zu schließen. Im folgenden wird auf die Eigenschaften beider Varianten näher eingegangen.

3.2 Symmetrische Kryptosysteme

Ein symmetrisches Kryptosystem zeichnet sich dadurch aus, daß der Chiffrierschlüssel K und der Dechiffrierschlüssel K' gleich sind oder zumindest in einem so einfachen Zusammenhang stehen, daß sich K' ohne nennenswerten Aufwand aus K herleiten läßt. Der Besitz beider Schlüssel ist also äquivalent, weshalb die folgenden Betrachtungen von nur einem Schlüssel ausgehen.

Dadurch, daß für die Verschlüsselung der gleiche Schlüssel wie bei der Entschlüsselung zum Einsatz kommt, ist es unbedingt erforderlich, daß dieser Schlüssel geheim bleibt. Das heißt, nur Sender und Empfänger dürfen im Besitz dieses Schlüssels sein. Daraus folgt, daß für jede einzelne Kommunikationsbeziehung ein eigener geheimer Schlüssel existieren muß. Dieser Schlüssel muß vorab über einen sicheren Kanal zwischen den Beteiligten vereinbart werden (siehe Abbildung 4).

Für ein einzelnes Sender-Empfänger-Paar ist ein solcher Schlüsselaustausch noch machbar, wenn die Beteiligten einander bekannt sind. Sollen jedoch beliebige Paare sicher Nachrichten austauschen können, so steigt die Anzahl der benötigten

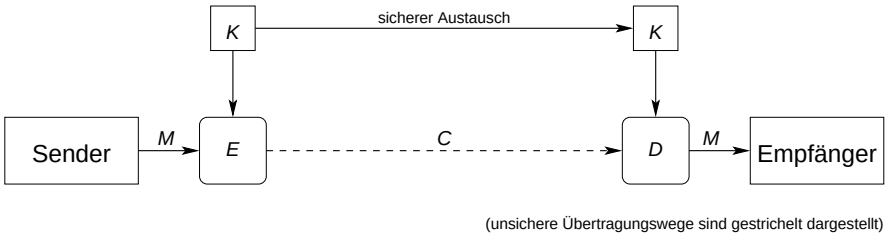

Abbildung 4: Symmetrisches Kryptosystem

geheimen Schlüssel exponentiell mit der Anzahl der Beteiligten an und deren sichere Verteilung wird schnell unpraktikabel. Dazu kommt, daß ein sicherer Kanal für den Schlüsselaustausch nicht immer ohne weiteres gegeben ist, insbesondere, wenn die Kommunikationspartner einander vorher nicht bekannt sind.

Einer der bekanntesten Vertreter symmetrischer Kryptosysteme ist der 1977 verabschiedete *Data Encryption Standard* (DES). Das darin verwendete Verfahren an sich ist zwar bisher nicht gebrochen worden, bietet aber einen für heutige Maßstäbe zu kleinen Schlüsselraum: Wer über die entsprechenden Mittel verfügt, kann eine DES-Verschlüsselung in kurzer Zeit durch Ausprobieren aller möglichen Schlüssel brechen. Dennoch ist DES noch immer weit verbreitet.

Offiziell abgelöst werden soll DES durch den *Advanced Encryption Standard* (AES). Als dessen Kernstück hat das amerikanische *National Institute of Standards and Technology* (NIST) im Oktober 2000 im Rahmen eines Wettbewerbs aus mehreren Bewerbungen einen Verschlüsselungsalgorithmus namens *Rijndael* ausgewählt. Dieses symmetrische Verfahren, das von den Belgiern Joan Daemen und Vincent Rijmen entwickelt wurde, unterstützt wesentlich größere Schlüsselräume als DES und bietet zudem die Möglichkeit, je nach Bedarf zwischen unterschiedlichen Schlüssellängen zu wählen. Damit bringt es gute Voraussetzungen mit, um diesen neuen, voraussichtlich im Frühjahr 2001 in Kraft tretenden Standard auf längere Sicht sicher zu machen. [8]

3.3 Asymmetrische Kryptosysteme (Public-Key-Systeme)

Bei einem asymmetrischen Kryptosystem sind die verwendeten Algorithmen so gewählt, daß zwischen dem Chiffrierschlüssel K und dem Dechiffrierschlüssel K' kein „einfacher“ Zusammenhang besteht. Das heißt, es ist ohne zusätzliches Wissen nicht möglich, aus K direkt auf K' zu schließen. Vielmehr ist der Aufwand, bei Kenntnis von K den zugehörigen Schlüssel K' zu finden, so hoch, daß ein Angriff auf diesem Weg nicht praktikabel ist. Es wird also nicht mit einem einzelnen Schlüssel, sondern immer mit einem geeignet gewählten Schlüsselpaar (K, K') gearbeitet.

Diese Eigenschaft asymmetrischer Kryptosysteme kann dahingehend genutzt werden, daß der Erzeuger eines Schlüsselpaares den Dechiffrierschlüssel als geheimen Schlüssel (*private key*) für sich behält, während er den Chiffrierschlüssel als öffentlichen Schlüssel (*public key*) bekannt gibt. Daher werden solche Systeme auch als Public-Key-Systeme bezeichnet. Damit ist jeder in der Lage, unter Verwendung des öffentlichen Schlüssels eine Nachricht zu chiffrieren, die dann nur von dem Besitzer des geheimen Schlüssel dechiffriert werden kann. So ermöglicht der Erzeuger des Schlüsselpaares durch die Verbreitung des öffentlichen Schlüssels allen Interessierten, ihm ohne vorherigen Austausch geheimer Schlüssel vertrauliche Nachrichten verschlüsselt zukommen zu lassen (siehe Abbildung 5).

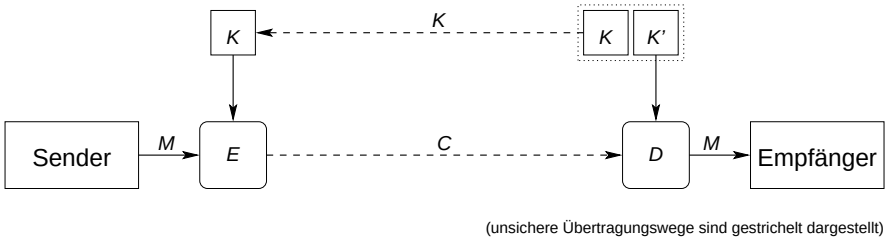

Abbildung 5: Asymmetrisches Kryptosystem

Damit ist bei einem asymmetrischen Kryptosystem das Problem der Schlüsselverteilung gegenüber einem symmetrischen System deutlich vereinfacht, da es nicht mehr erforderlich ist, zwischen allen Teilnehmern geheime Schlüssel auf sicheren Kanälen auszutauschen. Stattdessen kann die Schlüsselverteilung dadurch erfolgen, daß jeder Beteiligte seinen öffentlichen Schlüssel öffentlich bekannt gibt. Allerdings stellt sich durch die freie Verteilung der Schlüssel das neue Problem, daß Verfahren zur Sicherstellung der Authentizität der so erhaltenen Schlüssel benötigt werden (siehe Abschnitt 5.2).

Eines der bekanntesten Public-Key-Verfahren ist der nach seinen Erfindern Rivest, Shamir und Adleman benannte RSA-Algorithmus, der in vielen Krypto-Produkten zum Einsatz kommt. Seine Sicherheit beruht darauf, daß bisher kein Verfahren bekannt ist, um innerhalb vertretbarer Zeit die Primfaktorenzerlegung einer sehr großen Zahl zu finden.

3.4 Hybride Kryptosysteme

Ein erheblicher Nachteil asymmetrischer Kryptosysteme liegt darin, daß die zugrundeliegenden mathematischen Verfahren sehr aufwendig sind, wodurch deren Anwendung verglichen mit symmetrischen Verfahren um ein Vielfaches langsamer ist. Daher werden in der Praxis oft sogenannte hybride Systeme eingesetzt, die die Anwendung von symmetrischen und asymmetrischen Verfahren kombinieren.

Dabei wird zunächst ein asymmetrisches Verfahren verwendet, um auf sicherem Wege einen zufällig generierten, nur einmal verwendeten Sitzungsschlüssel zwischen Sender und Empfänger auszutauschen. Dann zur Verschlüsselung der eigentlichen Nutzdaten mit diesem Sitzungsschlüssel ein symmetrisches Verfahren benutzt. So können die Vorteile eines asymmetrisches Kryptosystems bei der Schlüsselverteilung genutzt werden, während für die Verschlüsselung großer Datenmengen effizientere symmetrische Algorithmen verwendet werden.

4 Integrität und Authentizität

Für viele Anwendungen ist es wichtig, sicherzustellen, daß übermittelte Nachrichten den Empfänger unverfälscht erreichen (Integrität) und tatsächlich vom vorgeblichen Absender stammen (Authentizität). Mittel, um diese Ziele zu erreichen, sind Hash-Funktionen und Digitale Signaturen, deren Grundlagen im folgenden beschrieben werden.

4.1 Hash-Funktionen

Eine Hash-Funktion ist eine Einwegfunktion h, die eine Nachricht M mit beliebiger Länge auf einen Funktionswert $h(M)$ (Hash-Wert) fester Länge abbildet. Verfälschungen einer Nachricht sollen dadurch erkannt werden, daß sowohl Sender als auch Empfänger den Hash-Wert der Nachricht berechnen und ihre Ergebnisse auf einem geeigneten Weg miteinander vergleichen: Wurde die Nachricht während des Transports verfälscht, so muß sich dies in einem geänderten Hash-Wert äußern.

Anders als gängige Prüfsummenverfahren, die z. B. zur Erkennung von Übertragungsfehlern eingesetzt werden, müssen dabei aber nicht nur zufällig auftretende Fehler, sondern auch vorsätzliche Manipulationen sicher erkannt werden. Daraus ergeben sich für kryptographische Hash-Funktionen die folgenden Anforderungen:

1. $h(M)$ ist „einfach“ zu berechnen.
2. Finden von M mit $h(M) = X$ zu gegebenem X ist praktisch unmöglich.

   Mit dieser Anforderung soll ausgeschlossen werden, daß ein Angreifer zum Hash-Wert einer Nachricht gezielt eine andere Nachricht mit dem gleichen Hash-Wert finden kann, da es damit möglich wäre, eine Originalnachricht unerkannt durch eine Fälschung auszutauschen.
3. (M, M') mit $h(M) = h(M')$ ist praktisch nicht zu finden.

   Diese Anforderung soll gewährleisten, daß es nicht gelingt, gezielt zwei Nachrichten mit gleichen Hash-Werten zu generieren. Anderenfalls wäre es denkbar, zwei Personen unterschiedliche Nachrichten zukommen zu lassen, sie aber annehmen zu lassen, daß es sich um die gleiche Nachricht handelt.

Hash-Funktionen, die alle diese Anforderungen erfüllen, werden als starke Hash-Funktionen bezeichnet. Wird nur die dritte Anforderung nicht erfüllt, so spricht man dagegen von einer schwachen Hash-Funktion. Aufgrund der festen Länge des Hash-Wertes bei beliebiger Nachrichtenlänge ist es theoretisch immer möglich, Kollisionen, wie sie durch die Anforderungen 2. und 3. ausgeschlossen werden sollen, herbeizuführen, da jeweils eine unendliche Anzahl verschiedener Nachrichten auf den gleichen Hash-Wert abgebildet würde. Durch ausreichend lange Hash-Werte und einen geeignet gewählten Algorithmus läßt sich aber ausschließen, daß solche Kollisionen mit praktikablen Aufwand gezielt herbeigeführt werden können.

Ein weit verbreitetes Hashing-Verfahren ist der *MD5 Message-Digest Algorithm* [9]. Ein weiteres bekanntes Beispiel ist der *Secure Hashing Algorithm 1* (SHA-1), der längere Hash-Werte erzeugt und im Design einige Verbesserungen aufweist, durch die vermutete Schwächen von MD5 umgangen werden sollen.

4.2 Digitale Signaturen

Der im vorigen Abschnitt beschriebene Vergleich von Hash-Werten einer Nachricht geht davon aus, daß sich Empfänger und Sender auf einem manipulationssicheren Weg über den Hash-Wert verständigen. Dies kann prinzipiell auf einem geeigneten eigenen Kanal abseits der eigentlichen Nachrichtenübertragung erfolgen, etwa durch einen telefonischen Abgleich der Hash-Werte wenn die Beteiligten einander bekannt sind und sich anhand ihrer Stimme sicher erkennen können. Allerdings sind die Voraussetzungen dafür nicht immer gegeben und selbst dann ist ein solches Vorgehen mitunter zu umständlich um praktikabel zu sein. Es ist also wünschenswert, die Integrität und Authentizität einer Nachricht anhand von Informationen prüfen zu können, die direkt dieser Nachricht beigefügt werden.

Fügt der Sender einer Nachricht jedoch einfach nur einen Hash-Wert über die Nachricht bei, so kann der Empfänger daran zwar erkennen, ob die Nachricht seit der Berechnung des Hash-Wertes verändert wurde. Ob der erhaltene Hash-Wert aber tatsächlich von dem vorgeblichen Absender berechnet wurde, die Nachricht also authentisch ist, läßt sich daran jedoch nicht erkennen, denn auch ein Angreifer hätte die Nachricht fälschen und den passenden Hash-Wert beifügen können.

Gelöst wird dieses Problem durch das Anbringen einer digitalen Signatur an der Nachricht. Dabei kommt ein asymmetrisches Kryptoverfahren zum Einsatz, allerdings werden die Rollen von öffentlichem und privatem Schlüssel gegenüber der Anwendung zur verschlüsselten Nachrichtenübermittlung vertauscht: Der Sender verwendet einen geheimen Schlüssel zum Signieren der Nachricht, während der Empfänger mit dem zugehörigen öffentlichen Schlüssel die Authentizität der Signatur überprüfen kann. Unter anderem zur Begrenzung des Aufwands wird das asymmetrische Verfahren dabei in der Praxis nicht auf die gesamte Nachricht, sondern nur auf einen Hash-Wert der Nachricht angewendet.

Eine Signatur S wird dabei erzeugt, indem der Sender den Hash-Wert der Nachricht M mit seinem privaten Schlüssel K verschlüsselt:

$$S = E(K, h(M))$$

Diese Signatur wird dann zusammen mit der Nachricht an den Empfänger übermittelt, der nun seinerseits den Hash-Wert über die erhaltene Nachricht berechnen kann. Außerdem kann er, falls die Nachricht tatsächlich durch den vermeintlichen Absender signiert wurde, mit dessen öffentlichem Schlüssel die Signatur S entschlüsseln und muß dabei wieder den ursprünglichen Hash-Wert erhalten. Das heißt, wenn die Bedingung

$$D(K', S) = h(M)$$

erfüllt ist, kann der Empfänger davon ausgehen, daß die empfangene Nachricht authentisch ist, denn nur der Absender selbst konnte mit dem ihm allein bekannten privaten Schlüssel die Signatur erzeugen. Trifft diese Bedingung dagegen nicht zu, muß er annehmen, daß die Integrität der Nachricht verletzt wurde (Hash-Wert hat sich geändert) oder die Absenderangabe gefälscht ist, also ein anderer als der zum öffentlichen Schlüssel des angeblichen Absenders gehörende private Schlüssel zum Erzeugen der Signatur verwendet wurde.

Damit ist das Problem der Authentifizierung — wie auch schon bei der Nachrichtenverschlüsselung mit asymmetrischen Verfahren — weitgehend darauf reduziert worden, daß Nachrichtenempfänger auf zuverlässige Weise die öffentlichen Schlüssel ihrer Kommunikationspartner erhalten müssen.

Ferner sind mittels digitaler Signaturen auch Anwendungen denkbar, die über das bloße Prüfen der Authentizität hinausgehen. Muß z. B. eine Möglichkeit gegeben sein, die Existenz einer Nachricht zu einem bestimmten Zeitpunkt nachzuweisen, so läßt sich dies etwa durch Hinzuziehung einer unabhängigen, von allen Beteiligten als vertrauenswürdig angesehenen dritten Instanz („Notar“) realisieren. Dieser Notar kann eine Nachricht mit einem aktuellen Zeitstempel kombinieren und das Resultat mit seinem privaten Schlüssel signieren und an den Einreicher zurückgeben. Er bestätigt dabei mit seiner digitalen Signatur, daß ihm diese Nachricht zum angegebenen Zeitpunkt vorgelegen hat.

5 Schlüsselverwaltung und -verteilung

5.1 Schlüsselmanagement

Die besten Kryptoverfahren nützen wenig, wenn die verwendeten Schlüssel angreifbar sind. Dies zu verhindern ist Aufgabe des Schlüsselmanagements.

Die Sicherheit beginnt bei der Schlüsselerzeugung: Gute Schlüssel dürfen nicht vorhersehbar sein. So wären etwa fortlaufend vergebene Nummern denkbar ungeeignete Schlüssel, aber auch statistische Eigenschaften beispielsweise von Pseudozufallszahlen können Angriffspunkte bieten bzw. die Wahrscheinlichkeit für das Erraten des Schlüssels erhöhen. Schlüssel sollten daher im Idealfall absolut zufällig aus dem zur Verfügung stehenden Schlüsselraum gewählt werden. Dazu kommt, daß bei manchen Kryptoverfahren nicht alle Schlüssel gleich gut geeignet sind. In diesen Fällen ist darauf zu achten, keine „schwachen“ Schlüssel zu wählen, mit denen das Verfahren nur eine eingeschränkte Sicherheit bietet.

Als nächstes ist zu gewährleisten, daß geheime Schlüssel sicher aufbewahrt werden, also nur den zur Benutzung befugten Personen zugänglich sind. Sofern die Übermittlung eines geheimen Schlüssels nötig ist, muß auch sichergestellt sein, daß er nicht während des Transports in die falschen Hände fallen kann. In diesem Bereich ergeben sich in der Praxis wahrscheinlich die größten Risiken, da es hier nicht zuletzt auf sicherheitsbewußten Umgang mit Schlüsseln im Alltag ankommt. Die Erfahrung zeigt, daß Menschen aus Bequemlichkeit dazu neigen, selbst offensichtliche Sicherheitsregeln zu mißachten. Ein Schutz gegen solche Risiken ist durch organisatorische Maßnahmen, strikte Regeln im Umgang mit geheimen Schlüsseln und entsprechende Schulungen nur in begrenztem Umfang möglich.

Weiterhin gehört es zu den Aufgaben des Schlüsselmanagements, Möglichkeiten zum Widerruf bzw. zum Auswechseln von Schlüsseln vorzusehen. Dies kann planmäßig nach einer bestimmten Zeit geschehen, aber auch anlaßbezogen, etwa wenn Grund zu der Annahme besteht, daß ein Schlüssel kompromittiert wurde. In diesem Zusammenhang ist auch auf das sichere Löschen nicht mehr benötigter geheimer Schlüssel zu achten, um auszuschließen, daß sie womöglich nachträglich in fremde Hände fallen und beispielsweise zum Entschlüsseln mitgeschnittener verschlüsselter Nachrichten verwendet werden. Dies bedingt insbesondere auch Vorsichtsmaßnahmen bei der Entsorgung gebrauchter Datenträger, die sensitives Material enthalten.

Je nach Anwendungsbereich kann es auch notwendig sein, über Möglichkeiten zur Rekonstruktion von Schlüsseln (*Key Recovery*) ohne Mithilfe durch deren eigentlichen Besitzer zu verfügen. Beispielsweise kann ein Unternehmen ein berechtigtes Interesse daran haben, bei Ausfall eines Mitarbeiters auf dessen dienstliche Kommunikation zugreifen zu können. Dazu muß es berechtigten Stellen möglich sein, die dazu nötigen Schlüssel dieses Mitarbeiters zu erhalten, was im einfachsten Fall z. B. durch die Hinterlegung von Kopien dieser Schlüssel an einem sicheren Ort realisierbar ist. Allerdings ist bei der Schaffung solcher Möglichkeiten große Vorsicht geboten, um etwaigem Mißbrauch vorzubeugen.

5.2 Public Key Infrastructure (PKI)

Wie in Abschnitt 3.3 bereits erwähnt, bieten asymmetrische Kryptosysteme den Vorteil, daß Schlüssel über öffentliche Kanäle ausgetauscht werden können, was

aber das neue Problem der Gewährleistung der Authentizität von öffentlichen Schlüsseln mit sich bringt. Ein Weg, den Schlüsselaustausch zwischen beliebigen Kommunikationspartnern so zu organisieren, daß diese Anforderung erfüllt wird, ist eine *Public Key Infrastructure* (PKI).

Eine solche Struktur besteht zunächst einmal aus einem Verzeichnisdienst, über den die öffentlichen Schlüssel aller Teilnehmer abrufbar sind. Zur Lösung des Authentizitäts-Problems wird dabei zusätzlich eine Zertifizierungsstelle eingeführt, die mit dem Betreiber des Verzeichnisses identisch sein kann. Dabei handelt es sich um eine von allen Beteiligten akzeptierte unabhängige Instanz, die auf Antrag Zertifikate über öffentliche Schlüssel ausstellt.

Ein Zertifikat ist im wesentlichen ein Datensatz, der einen öffentlichen Schlüssel, Angaben zur Identität dessen Inhabers, also des Besitzers des zugehörigen privaten Schlüssels, sowie Informationen zur Gültigkeit des Schlüssels, insbesondere meist ein Ablaufdatum, enthält. Diese Daten werden von der Zertifizierungsstelle mit ihrem eigenen privaten Signaturschlüssel digital signiert. Diese Signatur wird Bestandteil des Zertifikats, daß dann in dem Verzeichnis veröffentlicht wird. Dieses Zertifikat ist damit allen Interessierten zugänglich und kann mittels des öffentlichen Schlüssels der Zertifizierungsstelle auf seine Echtheit (d. h., es wurde tatsächlich von der Zertifizierungsstelle ausgestellt) geprüft werden.

Die Zertifizierungsstelle bürgt also mit ihrer Signatur für die Authentizität der veröffentlichten Schlüssel. Diese Aufgabe bedeutet eine große Verantwortung und stellt hohe Anforderungen an die Vertrauenswürdigkeit der Zertifizierungsstelle. So muß sie insbesondere garantieren, daß sie die Identität der Inhaber der zertifizierten Schlüssel geprüft hat. Zusätzlich muß sie durch technische und organisatorische Maßnahmen in besonderem Maße gegen Angriffe geschützt sein. Insbesondere muß der private Signaturschlüssel der Zertifizierungsstelle unter allen Umständen geheim bleiben, da anderenfalls alle ausgestellten Zertifikate wertlos würden.

Es verbleibt die Frage, wie der zur Überprüfung von Zertifikaten erforderliche öffentliche Schlüssel der Zertifizierungsinstanz so verbreitet werden kann, daß die Verwender sich dessen Authentizität sicher sein können. Diese ist aber, da es sich nur um einzelne Schlüssel bekannter Instanzen handelt, relativ einfach zu lösen. Ein häufig gewählter Weg besteht darin, daß Hersteller kryptographischer Software ihren Produkten die öffentlichen Schlüssel einiger Zertifizierungsstellen beilegen. Auch die Veröffentlichung des Schlüssels bzw. eines Hash-Wertes dieses Schlüssels in einer schwer zu fälschenden Publikation, etwa einer Zeitschrift, ist ein brauchbarer Ansatz. Schließlich gibt es auch die Möglichkeit, daß sich mehrere Zertifizierungsstellen ihre Schlüssel gegenseitig oder in einer hierarchischen Struktur untereinander zertifizieren. So genügt dann die zuverlässige Kenntnis des Schlüssels einer dieser Stellen, um die Authentizität der Schlüssel der übrigen Stellen zu verifizieren und somit auch die von ihnen ausgestellten Zertifikate prüfen zu können.

6 Kryptoanalyse

Wie bereits an einigen Stellen angedeutet, ist mit diversen kryptoanalytischen Angriffen zu rechnen, die darauf abzielen, Chiffren zu brechen oder einen kryptographischen Schutz anderweitig unbrauchbar zu machen. Dabei sind vielfältige Ansätze für solche Angriffe denkbar.

6.1 Mögliche Angriffspunkte

Ein erfolgreicher kryptoanalytischer Angriff setzt immer voraus, daß gewisse Anhaltspunkte für die Analyse einer Chiffre vorhanden sind. Dies kann beispielsweise Wissen über Eigenschaften des zu einer verschlüsselten Nachricht gehörenden Klartextes, etwa über bekannte Textteile sein. Auch kann z. B. die Kenntnis der verwendeten Sprache Informationen über statistische Eigenschaften wie Häufigkeitsverteilungen von Zeichen und auftretende Redundanzen liefern.

Auch können Schwächen in kryptographischen Algorithmen unter Umständen dazu führen, daß die erzeugten Chiffretexte Eigenschaften aufweisen, die sich bei der Kryptoanalyse ausnutzen lassen. Ziel des Designs von Kryptosystemen muß es also sein, alle Eigenschaften zu vermeiden, die einem Angreifer Anhaltspunkte für eine Analyse bieten und ihm so das Dechiffrieren von Nachrichten oder gar Rückschlüsse auf geheime Schlüssel ermöglichen könnten. Diese Aufgabe ist nicht einfach und setzt umfangreiches theoretisches Wissen und Erfahrung voraus.

6.2 Klassen von Angriffen

Stehen einem Angreifer zur Analyse einer Verschlüsselung[2] als Ausgangsmaterial nur Chiffretexte zur Verfügung (*Ciphertext-only Attack*), so muß er versuchen, aus diesen auf die zugehörigen Klartexte zu schließen und möglichst auch den benutzten Schlüssel zu bestimmen. Verfügt er zusätzlich auch über die zu einigen Nachrichten gehörenden Klartexte (*Known-Plaintext Attack*), so kann dies die Aufgabe, den geheimen Schlüssel zu ermitteln, vereinfachen.

Ein weiteres Beispiel ist ein Angriff mit gewähltem Klartext (*Chosen-Plaintext Attack*), bei dem der Angreifer die Verschlüsselung verschiedener, von ihm gezielt gewählter Klartexte veranlaßt. Hier kann es durch Analyse der entstehenden Chiffretexte in Relation zu den Klartexten gelingen, Rückschlüsse auf den verwendeten Schlüssel zu ziehen. Solche Angriffe können verhindert werden, wenn dem Angreifer durch geeignete Gestaltung von Abläufen die Möglichkeit zu einer solchen Vorgehensweise genommen wird.

Ein neuerer und relativ komplizierter Ansatz ist die differentielle Kryptoanalyse. Dabei werden Paare von Chiffretexten miteinander verglichen, um durch Analyse

[2] Hier wird davon ausgegangen, daß der verwendete Verschlüsselungsalgorithmus bekannt ist.

der Unterschiede — bestimmte Eigenschaften der zugehörigen Klartexte vorausgesetzt — auf den verwendeten Schlüssel schließen zu können. Mit dieser Methode wurden einige Erfolge gegen das schwer zu analysierende DES erzielt, wenngleich dieses Verfahren damit nicht vollständig gebrochen wurde. [3]

7 Politischer und rechtlicher Rahmen

7.1 Einschränkungen kryptographischer Anwendungen

7.1.1 Beschränkungen von Verbreitung und Nutzung

Die Tatsache, daß Kryptographie Anwendung im militärischen und nachrichtendienstlichen Bereich findet, hat dazu geführt, daß kryptographische Produkte in einigen Ländern als „Waffe“ eingestuft wurden und damit z. B. entsprechenden Exportbeschränkungen unterliegen. So war es in den USA bis vor kurzem verboten, Produkte, die starke Kryptographie enthalten, zu exportieren, um zu verhindern, daß feindliche Staaten in den Besitz solcher Produkte kommen.

Diese Regelung hatte zur Folge, daß aus den USA ausgeführte Produkte nur Implementierungen von Verschlüsselungsverfahren enthielten, die — etwa durch verminderte Schlüssellängen — geschwächt waren. So sollte den US-Geheimdiensten die Möglichkeit offengehalten werden, damit verschlüsselte Nachrichten innerhalb kurzer Zeit zu dechiffrieren. Ob der vorgebliche Zweck der Regelung erfüllt werden konnte, kann als fraglich gelten, da die Herstellung kryptographischer Produkte nicht auf die USA beschränkt ist. Als Resultat waren in anderen Ländern hergestellte Produkte bei Anwendungen mit höherem Sicherheitsbedarf im internationalen Wettbewerb klar im Vorteil. Daher wurde Regelung schließlich im Oktober 2000 von der US-Regierung auf Druck der Wirtschaft soweit entschärft, daß das Exportverbot für Verschlüsselungsprodukte gegenüber den meisten Ländern faktisch aufgehoben ist. [1]

Ein anderes häufiges Argument gegen die freie Verbreitung und Verwendung von Kryptographie, ist die Tatsache, daß Verschlüsselung auch von kriminellen Vereinigungen genutzt werden kann, um eine Überwachung durch die Strafverfolgungsbehörden zu vereiteln. Aus diesem Grund beschränken einige Staaten auch die Zulässigkeit der Verwendung von Kryptographie im Inland. So war die Benutzung starker Verschlüsselung ohne besondere Genehmigung oder Erfüllung von Auflagen (Schlüsselhinterlegung) z. B. in Frankreich lange Zeit verboten. Erst im Frühjahr 1999 wurden die sehr strengen Regelungen dort gelockert. [7]

7.1.2 Schlüsselhinterlegung bei staatlichen Stellen

Auch, wenn die Nutzung von Kryptographie nicht grundsätzlich beschränkt wird, wird oft vorgebracht, daß es ein berechtigtes staatliches Interesse an der Möglich-

keit zur Überwachung von Kommunikation gäbe. Analog zu den unter bestimmten Umständen zulässigen Eingriffen in das durch Art. 10 GG geschützte Brief-, Post- und Fernmeldegeheimnis, müsse auch die Möglichkeit zu staatlicher Einsichtnahme in verschlüsselte Nachrichten gegeben sein. So läßt etwa §100a StPO unter bestimmten Voraussetzungen die Überwachung und Aufzeichnung der Telekommunikation bei der Strafverfolgung zur Aufklärung schwerer Verbrechen zu, und die Forderung, dies auch auf verschlüsselte Telekommunikation anwenden zu können, erscheint zumindest naheliegend.

Realisierbar ist eine solche Überwachungsmöglichkeit für stark verschlüsselte Nachrichten nur, wenn die betreffenden Behörden über die zur Entschlüsselung nötigen geheimen Schlüssel verfügen. Dazu wäre die Verpflichtung zur Hinterlegung von Kopien dieser Schlüssel bei einer staatlichen Stelle (*key-escrow*) denkbar, allerdings ergäbe sich daraus ein hohes Mißbrauchsrisiko während sich die Einhaltung der Verpflichtung kaum kontrollieren ließe. Trotzdem wurden z. B. von Politikern in den USA und Deutschland Vorstöße in diese Richtung unternommen, die jedoch nicht erfolgreich waren. [11] [6]

7.1.3 Nutzen und Risiken von Beschränkungen

Der Nutzen solcher Beschränkungen ist als gering anzusehen. Kryptographisches Wissen einschließlich der genauen Beschreibung konkreter Verschlüsselungsverfahren ist heute weitgehend frei verfügbar. Damit ist es grundsätzlich möglich, unter Verwendung von bekannten und als sicher geltenden Verfahren eigene Kryptosysteme zu implementieren, um so etwa trotz durch Exportbeschränkungen anderer Länder fehlender Importmöglichkeiten an kryptographische Produkte zu kommen. Dazu kommt, daß mittlerweile ohnehin reichlich Software, die starke kryptographische Verfahren implementiert, international frei verfügbar ist.

Auch das Umgehen gesetzlich vorgeschriebener Einschränkungen beim Einsatz von Kryptographie wäre durch Verwendung nicht zugelassener Software möglich. Eine generelle Kontrolle der Einhaltung solcher Vorschriften ist dagegen kaum praktikabel oder mit rechtsstaatlichen Grundsätzen vereinbar, so daß ihre Mißachtung erst bei der tatsächlichen Durchführung einer Überwachungsmaßnahme feststellbar wäre. Schließlich ist auch kaum anzunehmen, daß ausgerechnet für den verbotenen Einsatz von Kryptographie angedrohte strafrechtliche Sanktionen auf Schwerkriminelle, gegen die sich solche Regelungen in erster Linie richten sollen, die nötige abschreckende Wirkung haben.

Dagegen bedeuten Beschränkungen von Kryptographie für alle Anwender mit einem berechtigten Interesse an deren Einsatz eine Verminderung der Sicherheit. So wäre etwa bei einer Begrenzung der Schlüssellängen die Vertraulichkeit der Kommunikation nicht mehr gewährleistet, was insbesondere im geschäftlichen Verkehr im Hinblick auf die Gefahr von Industriespionage u. ä. nicht akzeptabel ist. Auch Regelungen zur Hinterlegung von Schlüsseln sind problematisch, da nur ein begrenztes Vertrauen gegenüber den zuständigen staatlichen Stellen

angenommen werden kann. Gerade bei der zunehmenden Abwicklung von vertraulicher Kommunikation über öffentliche Datennetze und vor dem Hintergrund der Forderung nach von sicheren elektronischen Transaktionen im Zusammenhang mit E-Commerce sind gesetzliche Beschränkungen von Kryptographie angesichts der damit verbundenen Risiken nicht sinnvoll, zumal der zu erwartende Nutzen nur gering ist.

7.2 Rechtliche Fragen des Einsatzes

Neben der grundsätzlichen Zulässigkeit der Nutzung von Kryptographie sind bei ihrem Einsatz noch weitere rechtliche Aspekte zu berücksichtigen. So muß beispielsweise geklärt werden, welche rechtliche Stellung elektronisch übermittelten Dokumenten, die kryptographisch gesichert sind, zukommt.

Von entscheidender Bedeutung ist dabei die Bewertung digitaler Signaturen. Insbesondere wird die Frage aufgeworfen, welche Beweiskraft einem digital signierten Dokument zukommt und welche Formerfordernisse es erfüllen kann. Die Voraussetzungen, die digitale Signaturen erfüllen müssen, um die handschriftliche Unterschrift ersetzen können, regelt in Deutschland das Signaturgesetz. In seiner ursprünglichen, 1997 verabschiedeten Fassung stellt es extrem hohe Anforderungen an die Fälschungssicherheit und damit an die verwendeten technischen Verfahren und die Schutzvorkehrungen von Zertifizierungsstellen, was der Verbreitung eher hinderlich ist. Im Zuge der Anpassung an eine europäische Richtline wird dieses Gesetz jedoch überarbeitet und wird zukünftig auch eine Klasse von Signaturen zulassen, an die geringere Anforderungen gestellt werden. [2]

8 Fazit

Kryptographie ist ein nicht mehr wegzudenkendes Hilfsmittel, um eine sichere Kommunikation zu ermöglichen. Durch die zunehmende Kommunikation über offene Netze, Gefahren durch Wirtschaftsspionage und den Bedarf nach einem sicheren elektronischen Handel kommt ihr heute vor allem eine große wirtschaftliche Bedeutung zu, was sich auch in der Ausbildung entsprechender Rechtsnormen niederschlägt.

Es gibt diverse Arten kryptographischer Verfahren, die durch ihre unterschiedlichen Eigenschaften für verschiedene Zwecke geeignet sind und oft auch kombiniert eingesetzt werden. Die Entwicklung des für eine Anwendung geeignetsten Kryptosystems und insbesondere das Design guter Chiffren erfordert ein hohes Maß an Sachkenntnis und Erfahrung. Daher empfiehlt es sich meist, auf etablierte und vielfach geprüfte Verfahren zurückzugreifen. Neben technischen Fragen dürfen beim Einsatz von Kryptographie aber auch organisatorische Maßnahmen nicht vernachlässigt werden, da viele Unsicherheiten vor allem durch falsche Handhabung entstehen.

Literaturverzeichnis

[1] *Gelockerte US-Exportbestimmungen zur Kryptographie in Kraft.* Heise News-Ticker, Oktober 2000.
http://www.heise.de/newsticker/data/chr-20.10.00-001/.

[2] *Kabinett beschließt Entwurf des neuen Signaturgesetzes.* Heise News-Ticker, August 2000.
http://www.heise.de/newsticker/data/hob-16.08.00-002/default.shtml.

[3] Biham, Edi und Adi Shamir: *Differential Cryptanalysis of the Data Encryption Standard.* Springer-Verlag, 1993.

[4] Fumy, Walter und Hans Peter Riess: *Kryptographie: Entwurf, Einsatz und Analyse symmetrischer Kryptoverfahren.* Oldenbourg, 2. Auflage, 1994.

[5] Hess, Andreas: *Kryptographie: Grundlagen, Geschichte und derzeitige politische Diskussion*, 1998.
http://www.uni-mainz.de/~hessan00/krypto/KryptoInhalt.html.

[6] Hingst, Wolf-Christian: *Die deutsche Krypto-Kontroverse.* Telepolis, März 1998.
http://www.heise.de/tp/deutsch/inhalt/te/1416/1.html.

[7] Madsen, Wayne und David Banisar: *Cryptography and Liberty 2000 — An International Survey of Encryption Policy.* Electronic Privacy Information Center, 2000.
http://www2.epic.org/reports/crypto2000/.

[8] National Institute of Standards and Technology: *Advanced Encryption Standard (AES) Development Effort*, 2000.
http://csrc.nist.gov/encryption/aes.

[9] Rivest, Ronald L.: *The MD5 Message-Digest Algorithm.* rfc 1321, IETF, April 1992.

[10] Schneier, Bruce: *Applied Cryptography: protocols, algorithms, and source code in C.* John Wiley & Sons, 2. Auflage, 1996.

[11] Schulzki-Haddouti, Christiane: *Kanther fordert Key Escrow.* Telepolis, April 1997.
http://www.heise.de/tp/deutsch/inhalt/te/1185/1.html.