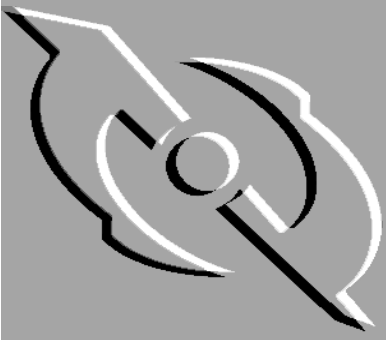

Einführung in die Kryptographie

COPYRIGHT

Gedruckt in der EU, PGP, Version 6.5.1 Int, 24-12-99.*

Network Associates International BV. +31(20)5866100
Gatwickstraat 25
NL-1043 GL Amsterdam
http://www.nai.com

info@nai.com

* wird gelegentlich anstelle von ® für die Kennzeichnung von eingetragenen Warenzeichen verwendet, um Warenzeichen, die eingetragen sind, zu schützen.

BESCHRÄNKTE GARANTIE

Beschränkte Garantie. Network Associates garantiert für einen Zeitraum von sechzig (60) Tagen ab Kaufdatum, daß das Medium, auf dem die Software gespeichert ist (z. B. Disketten), frei von Mängeln in bezug auf Material und Verarbeitung ist.

Ansprüche des Kunden. Die gesamte Haftung von Network Associates sowie von deren Anbietern und Ihr alleiniger Anspruch bestehen nach Wahl von Network Associates entweder (i) in der Rückerstattung des für die Lizenz bezahlten Preises, falls zutreffend, oder (ii) im Ersatz des fehlerhaften Mediums, auf dem die Software gespeichert ist, durch eine Kopie der Software auf einem fehlerfreien Medium. Das fehlerhafte Medium ist gemeinsam mit einer Kopie des Kaufbelegs an Network Associates zurückzugeben. Die Kosten dafür sind vom Kunden zu tragen. Diese beschränkte Garantie gilt nicht, wenn der Fehler auf einen Unfall, auf Mißbrauch oder auf fehlerhafte Anwendung zurückzuführen ist. Für Ersatzmedien wird nur für den Rest der ursprünglichen Garantiefrist eine Garantie übernommen. Außerhalb der Vereinigten Staaten von Amerika steht dieser Anspruch nicht zur Verfügung, sofern Network Associates den Beschränkungen entsprechend den Exportkontrollgesetzen und -bestimmungen der USA unterliegt.

Garantieausschluß. Soweit es das geltende Recht zuläßt, es sei denn, es ist in den Angaben zur beschränkten Garantie in diesem Dokument anders vorgesehen, WIRD DIE SOFTWARE „OHNE MÄNGELGEWÄHR“ GELIEFERT. OHNE EINSCHRÄNKUNG DER VORGENANNTEN BESTIMMUNGEN ÜBERNEHMEN SIE DIE VOLLE VERANTWORTUNG FÜR DIE AUSWAHL DER SOFTWARE, MIT DER SIE DIE GEWÜNSCHTEN ERGEBNISSE ERZIELEN MÖCHTEN, SOWIE FÜR DIE INSTALLATION UND VERWENDUNG DER SOFTWARE UND DIE DURCH DEN EINSATZ DER SOFTWARE ERZIELTEN ERGEBNISSE: OHNE EINSCHRÄNKUNG DER VORGENANNTEN BESTIMMUNGEN ÜBERNIMMT NETWORK ASSOCIATES KEINERLEI GARANTIE DAFÜR, DASS DIE SOFTWARE FREI VON FEHLERN UND UNTERBRECHUNGEN ODER ANDEREN AUSFÄLLEN IST UND DASS SIE IHREN ANFORDERUNGEN ENTSPRICHT. SOWEIT ES DAS GÜLTIGE RECHT ZULÄSST, SCHLIESST NETWORK ASSOCIATES JEGLICHE GARANTIEANSPRÜCHE, OB AUSDRÜCKLICH ODER STILLSCHWEIGEND, EINSCHLIESSLICH DER STILLSCHWEIGENDEN GEWÄHRLEISTUNG DER HANDELBARKEIT UND DER EIGNUNG FÜR EINEN BESONDEREN ZWECK, DES NICHTVERSTOSSES IN BEZUG AUF DIE SOFTWARE UND DIE DAZUGEHÖRIGE DOKUMENTATION, JEDOCH NICHT AUF DIESE BESCHRÄNKT, AUS. DA HAFTUNGSBESCHRÄNKUNGEN BEZÜGLICH STILLSCHWEIGENDER GEWÄHRLEISTUNGEN IN EINIGEN STAATEN UND RECHTSORDNUNGEN NICHT ZULÄSSIG SIND, TRIFFT DIE OBIGE BESCHRÄNKUNG AUF SIE MÖGLICHERWEISE NICHT ZU. Die vorgenannten Bestimmungen sind in dem im Rahmen des geltenden Rechts zulässigen Umfang einklagbar.

Inhalt

Vorwort

Wenn man an Kryptographie denkt, denkt man zuerst an Spionageromane und Action-Comics. Kinder schneiden aus Zeitschriften Buchstaben aus, um sich daraus geheime Botschaften zu basteln. Fast jeder hat schon mal eine Fernsehsendung oder einen Kinofilm gesehen, in dem ein Herr im dunklen Anzug vorkam, an dessen Handgelenk eine Aktentasche mit Handschellen gekettet war. Mit dem Wort „Spionage“ werden Vorstellungen von James-Bond-Filmen, Verfolgungsjagden und wilden Schießereien verbunden.

Und da sind Sie nun, wie Sie in Ihrem Büro sitzen und der im Vergleich dazu alltäglichen Aufgabe gegenüberstehen, einen Verkaufsbericht an einen Kollegen zu schicken, ohne daß jemand anders mitlesen kann. Sie wollen lediglich, daß Ihr Kollege der tatsächliche und auch der einzige Empfänger Ihrer E-Mail ist, und Sie wollen ihm auch zweifelsfrei versichern, daß Sie der Absender sind. Die nationale Sicherheit steht dabei nicht auf dem Spiel, aber wenn Ihre Konkurrenten Zugang zu dem Verkaufsbericht bekommen, könnte Sie das teuer zu stehen kommen. Wie können Sie das verhindern?

Verwenden Sie Kryptographie. Sie werden vielleicht feststellen, daß das nicht ganz so aufregend ist, wie in dunklen Gassen geflüsterte Losungen, aber das Ergebnis ist das gleiche: Informationen werden nur dem offenbart, für den sie bestimmt sind.

Zielgruppe dieses Handbuchs

Dieses Handbuch ist nützlich für alle, die sich für die Grundlagen von Kryptographie interessieren und eine Erklärung der Terminologie und Techniken suchen, die hinter PGP-Produkten stehen. Es empfiehlt sich, dieses Handbuch zu lesen, bevor Sie mit der Verwendung von Kryptographie beginnen.

Hinweise zum Umgang mit diesem Handbuch

In diesem Handbuch wird beschrieben, wie Sie die Nachrichten und gespeicherten Daten Ihres Unternehmens mit Hilfe von PGP sicher verwalten können.

Kapitel 1, „Einführung in die Kryptographie“ liefert Ihnen einen Überblick über die Terminologie und Begriffe, die Ihnen bei der Verwendung von PGP-Produkten begegnen.

Kapitel 2, „Phil Zimmermann über PGP“, verfaßt vom Entwickler von PGP, beschäftigt sich mit Fragen über Sicherheit, Geheimhaltung und Sicherheitsrisiken, die in jedem Sicherheitssystem, auch in PGP, vorhanden sind.

Weitere Informationen

Informationen zu technischem Kundendienst und Antworten auf eventuelle produktbezogene Fragen finden Sie in der mitgelieferten Datei „What's New".

Weitere Publikationen zum Thema

Weiterführende Informationen zur Kryptographie finden Sie u. a. in folgenden Veröffentlichungen:

Nicht-technische und technische Einführungsliteratur

- „*Cryptography for the Internet*" Philip R. Zimmermann. Scientific American, Oktober 1998. In diesem vom Entwickler von PGP verfaßten Artikel finden Sie Informationen zu verschiedenen kryptographischen Protokollen und Algorithmen, von denen viele auch in PGP angewendet werden.

- „*Privacy on the Line*", Whitfield Diffie und Susan Eva Landau. MIT Press; ISBN: 0262041677. In diesem Buch werden Geschichte und Entwicklung der Kryptographie und Kommunikationssicherheit beschrieben. Dieses Buch eignet sich hervorragend für Einsteiger und Benutzer mit geringem technischem Wissen. Es enthält daneben aber auch Informationen, die selbst vielen Experten unbekannt sein dürften.

- „*The Codebreakers*", David Kahn. Scribner; ISBN: 0684831309. In diesem Buch wird die Geschichte der Codierung und der Entschlüsselung von Codes von der Zeit der Ägypter bis zum Ende des II. Weltkrieges beschrieben. Kahn hat das Buch in den sechziger Jahren geschrieben und 1996 eine überarbeitete Ausgabe herausgebracht. Das Buch enthält zwar keine Darstellungen von kryptographischen Verfahrensweisen, diente aber einer neuen Generation von Kryptographen als Anregung.

- „*Network Security: Private Communication in a Public World*", Charlie Kaufman, Radia Perlman und Mike Spencer. Prentice Hall; ISBN: 0-13-061466-1. In diesem Buch werden Netzwerk-Sicherheitssysteme und -protokolle, deren Funktionsweise sowie die jeweiligen Vor- und Nachteile beschrieben. Da dieses Buch bereits im Jahre 1995 erschienen ist, ist es nur bedingt auf dem neuesten technischen Stand. Es ist dennoch sehr empfehlenswert. Ferner ist die darin enthaltene Beschreibung der Funktionsweise von DES wohl eine der besten, die jemals in einem Buch veröffentlicht wurde.

Technische Literatur

- „*Applied Cryptography: Protocols, Algorithms, and Source Code in C*“, Bruce Schneier, John Wiley & Sons; ISBN: 0-471-12845-7. Ein geeignetes Werk für Anfänger über die Funktionsweise der Kryptographie. Wenn Sie ein Experte auf dem Gebiet der Kryptographie werden möchten, empfehlen wir die Lektüre dieses Standardwerks.

- „*Handbook of Applied Cryptography*“, Alfred J. Menezes, Paul C. van Oorschot und Scott Vanstone. CRC Press; ISBN: 0-8493-8523-7. Dieses Buch sollten Sie nach dem Werk von Schneier lesen. Es enthält viele komplizierte mathematische Zusammenhänge, eignet sich aber dennoch für Benutzer, denen Mathematik schwerfällt.

- „*Internet Cryptography*“, Richard E. Smith. Addison-Wesley Pub Co; ISBN: 0201924803. In diesem Buch wird die Funktionsweise vieler Internet-Sicherheitsprotokolle beschrieben. Es beschreibt in erster Linie Systeme, die hochentwickelt sind, jedoch durch unvorsichtige Verwendung fehlerhaft arbeiten. Der Schwerpunkt in diesem Buch liegt nicht auf mathematischen Darstellungen, sondern auf der Vermittlung von praktischem Wissen.

- „*Firewalls and Internet Security: Repelling the Wily Hacker*“, William R. Cheswick und Steven M. Bellovin. Addison-Wesley Pub Co; ISBN: 0201633574. Die Autoren dieses Buches sind zwei langjährige Forschungsspezialisten von AT&T Bell Labs. Sie berichten über ihre Erfahrungen bei der Wartung und Neugestaltung der Internet-Verbindung von AT&T. Dieses Buch ist sehr empfehlenswert.

Literatur für Fortgeschrittene

- „*A Course in Number Theory and Cryptography*“, Neal Koblitz. Springer-Verlag; ISBN: 0-387-94293-9. Ein hervorragendes Mathematikbuch zur Zahlentheorie und Kryptographie, das sich in erster Linie an Hochschulabsolventen richtet.

- „*Differential Cryptanalysis of the Data Encryption Standard*“, Eli Biham und Adi Shamir. Springer-Verlag; ISBN: 0-387-97930-1. In diesem Buch wird die Differentialkryptoanalyse auf DES angewandt erläutert. Das Buch eignet sich besonders zum Kennenlernen dieses Verfahrens.

Einführung in die Kryptographie 1

Julius Cäsar vertraute keinem der Boten, die Nachrichten an seine Generäle überbrachten. Er ersetzte deshalb in seinen Nachrichten jedes A durch ein D, jedes B durch ein E usw. So verfuhr er mit dem ganzen Alphabet. Nur jemand, der die Regel des Vertauschens durch den drittnächsten Buchstaben kannte, konnte die Nachrichten entschlüsseln.

Damit begann die Geschichte der Verschlüsselung.

Verschlüsselung und Entschlüsselung

Daten, die ohne besondere Entschlüsselungsmethoden gelesen werden können, werden *Klartext* genannt. Das Verfahren zum Chiffrieren von Klartext, so daß dessen Inhalt unerkannt bleibt, wird *Verschlüsselung* genannt. Verschlüsseln von Klartext ergibt ein unleserliches Zeichengewirr, das dann *Verschlüsselungstext* genannt wird. Mit der Verschlüsselung bleiben Informationen unbefugten Personen verborgen, selbst wenn ihnen die Daten im verschlüsselten Zustand vorliegen. Das Verfahren des Zurückführens von chiffriertem Text in den ursprünglichen Klartext wird als *Entschlüsselung* bezeichnet.

Abbildung 1-1 zeigt das Verfahren des Verschlüsselns und Entschlüsselns.

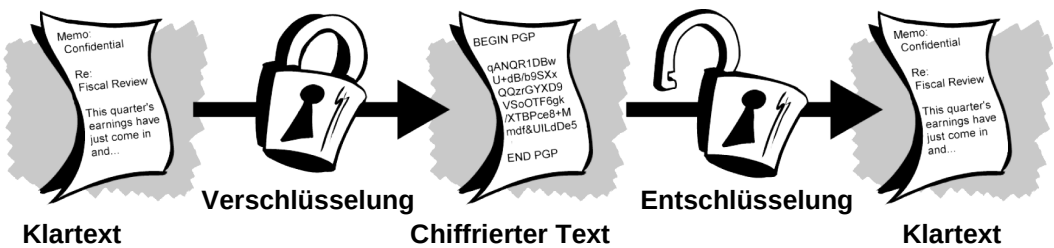

Abbildung 1-1. Verschlüsselung und Entschlüsselung

Was ist Kryptographie?

Kryptographie ist die Wissenschaft von der Ver- und Entschlüsselung von Daten mit Hilfe mathematischer Verfahren.

Dank der Kryptographie können vertrauliche Daten gespeichert oder über unsichere Netze (z. B. das Internet) übertragen werden, so daß diese nur vom eigentlichen Empfänger gelesen werden können.

Kryptographie ist also die Wissenschaft von der Datensicherung, dagegen ist die *Kryptoanalyse* die Wissenschaft von der Analyse und vom Entschlüsseln verschlüsselter Daten. Zur klassischen Kryptoanalyse gehören analytisches Denken, die Anwendung mathematischer Verfahren, das Auffinden von Strukturen, Geduld, Entschlossenheit und eine gehörige Portion Glück. Kryptoanalytiker werden auch *Hacker* genannt.

Kryptologie umfaßt sowohl die Kryptographie als auch die Kryptoanalyse.

Starke Verschlüsselung

„In der Praxis gibt es zwei Formen von Kryptographie: Mit der einen Form der Kryptographie können Sie Ihre Dateien vielleicht vor Ihrer kleinen Schwester schützen, mit der anderen Form vor dem Zugriff durch Organisationen der Regierung. In diesem Buch wird die letztere Form der Kryptographie behandelt.“

– Bruce Schneier, „Applied Cryptography: Protocols, Algorithms, and Source Code in C.“

PGP behandelt ebenfalls die letztere Form der Kryptographie.

Kryptographischer Code kann, wie im obengenannten Beispiel erklärt, *stark* oder *schwach* sein. Die Stärke des kryptographischen Codes wird anhand der Zeit und des Aufwands gemessen, dessen es zur Entschlüsselung bedarf. Mit einem *starken kryptographischen Code* entsteht ein chiffrierter Text, der ohne die Anwendung geeigneter Decodierungsverfahren kaum zu entschlüsseln ist. Wie schwierig ist es, einen solchen Text zu entschlüsseln? Selbst bei Einsatz aller zur Verfügung stehenden Computer und unter Nutzung der gesamten Zeitressourcen wäre es nicht möglich, den mit einem starken kryptographischen Code verschlüsselten Text in den nächsten Jahrtausenden zu entschlüsseln, selbst wenn eine Milliarde Computer pro Sekunde eine Milliarde Tests durchführen.

Man könnte also annehmen, daß ein starker kryptographischer Code selbst für einen raffinierten Kryptoanalytiker nicht zu entschlüsseln ist. Doch das läßt sich nicht mit absoluter Sicherheit sagen. Selbst der stärkste verfügbare kryptographische Code kann vielleicht schon der Computertechnik von morgen nachgeben. Die von PGP verwendete starke Kryptographie ist aber das beste heute verfügbare Verfahren. Durch Wachsamkeit und Konservativismus werden Ihre Daten jedoch auch weiterhin sicherlich besser geschützt, als durch die Behauptung der Unentschlüsselbarkeit.

Funktionsweise der Kryptographie

Ein *Verschlüsselungsalgorithmus* oder Chiffriercode ist eine mathematische Funktion zur Ver- und Entschlüsselung. Dieser Algorithmus wirkt in Kombination mit einem *Schlüssel*, beispielsweise einem Wort, einer Zahl oder Wortgruppe zur Verschlüsselung des Klartexts. Derselbe Klartext kann durch Verschlüsselung mit unterschiedlichen Schlüsseln unterschiedlich chiffrierten Text ergeben. Die Sicherheit der verschlüsselten Daten ist von den folgenden zwei Größen abhängig: der Stärke des Verschlüsselungsalgorithmus' und der Geheimhaltung des Schlüssels.

Der Verschlüsselungsalgorithmus mit allen verfügbaren Schlüsseln und allen Protokollen, durch die er funktioniert, bilden ein *Verschlüsselungssystem*, beispielsweise das Verschlüsselungssystem PGP.

Konventionelle Verschlüsselung

Bei der konventionellen Verschlüsselung, auch Verschlüsselung mit *Geheimschlüsseln* oder *symmetrischen Schlüsseln* genannt, wird ein Schlüssel sowohl für die Ver- als auch die Entschlüsselung verwendet. Der Data Encryption Standard (DES) ist ein Beispiel für ein konventionelles Verschlüsselungssystem, das häufig auf Regierungsebene eingesetzt wird. In Abbildung 1-2 ist die konventionelle Verschlüsselung dargestellt.

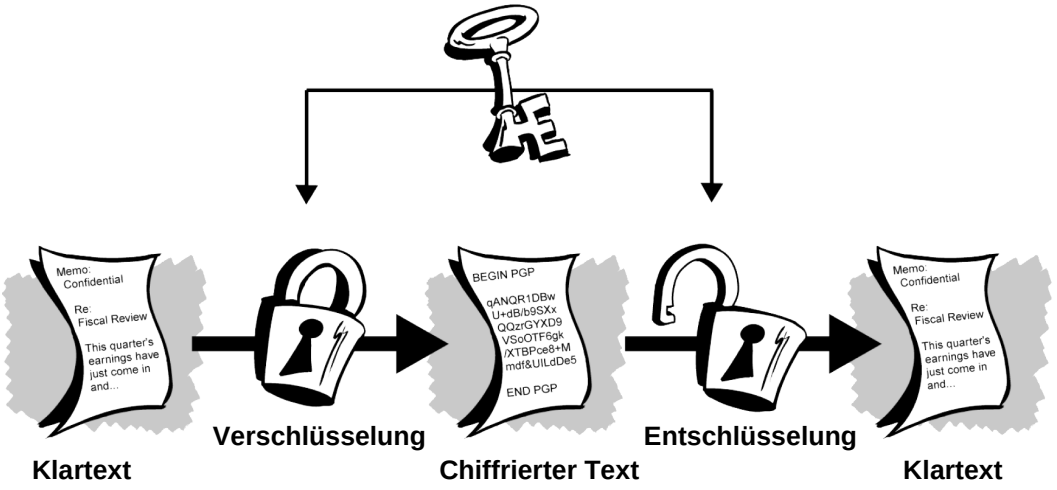

Abbildung 1-2. Konventionelle Verschlüsselung

Cäsars Verschlüsselungscode

Ein ganz einfaches Beispiel einer konventionellen Verschlüsselung ist ein Ersetzungschiffriercode. Dabei werden Informationsbestandteile gegeneinander ausgetauscht. Dies geschieht häufig durch Vertauschen einzelner Buchstaben im Alphabet. Zwei Beispiele dafür sind einfache Codes aus bekannten Kinderspielen oder auch Julius Cäsars Verschlüsselungscode. Dabei wird das Alphabet verschoben, wobei der Schlüssel die Anzahl der Zeichen ist, um die das Alphabet verschoben wurde.

Wenn wir beispielsweise das Wort „GEHEIM“ mit Cäsars Schlüsselwert 3 verschlüsseln, wird das Alphabet um drei Stellen nach hinten verschoben, so daß es mit dem Buchstaben D beginnt.

Ausgehend von

ABCDEFGHIJKLMNOPQRSTUVWXYZ

werden alle Buchstaben um drei Stellen verschoben. Dadurch erhält man folgendes Alphabet:

DEFGHIJKLMNOPQRSTUVWXYZABC

wobei D=A, E=B, F=C ist usw.

Mit diesem Schema wird der Klartext „GEHEIM“ als „JHKHLP“ verschlüsselt. Wenn eine andere Person den chiffrierten Text lesen soll, müssen Sie ihr mitteilen, daß der Schlüssel 3 ist.

Hierbei handelt es sich natürlich gemessen an den heutigen Standards um einen sehr einfachen Verschlüsselungscode. Der in Cäsars Zeiten wirksame Code soll hier auch nur als Beispiel für die Wirkungsweise konventioneller Verschlüsselung dienen.

Schlüsselverwaltung und konventionelle Verschlüsselung

Die konventionelle Verschlüsselung hat bestimmte Vorteile: Sie ist sehr schnell und besonders sinnvoll, wenn Daten verschlüsselt werden, die nicht *übertragen* werden. Dennoch ist die konventionelle Verschlüsselung, wenn sie als einziges Mittel der Übermittlung geschützter Daten verwendet wird, aufgrund der sich schwierig gestaltenden Schlüsselverteilung sehr kostenaufwendig.

Denken Sie an einen Darsteller aus einem bekannten Spionagefilm, beispielsweise jemanden, der einen Aktenkoffer zum sicheren Transport mit Handschellen an seinem Handgelenk befestigt hat. In diesem Aktenkoffer befindet sich in der Regel nicht der Code zum Bombenabwurf, die Biotoxinformel oder der Invasionsplan selbst. Meistens befindet sich darin der *Schlüssel*, mit dem die geheimen Daten entschlüsselt werden können.

Wenn die Kommunikation zwischen Absender und Empfänger anhand konventioneller Verschlüsselung geheim bleiben soll, müssen sie sich auf einen Schlüssel einigen und streng auf dessen Geheimhaltung achten. Wenn sich Absender und Empfänger an unterschiedlichen Orten aufhalten, müssen sie einem Kurier, einem Krisentelefon oder einem anderen sicheren Kommunikationsmedium vertrauen, um zu verhindern, daß der geheime Schlüssel während der Übertragung in die Hände von Unbefugten gerät. Wenn der Schlüssel bei der Übertragung abgefangen oder entdeckt wird, können die verschlüsselten Daten später gelesen, geändert, verfälscht oder mit dem Schlüssel beglaubigt werden. Das vorherrschende Problem bei der konventionellen Verschlüsselung besteht also in der *Schlüsselverteilung*: Wie gelangt der Schlüssel sicher zum Empfänger?

Kryptographie mit öffentlichen Schlüsseln

Das Problem der Schlüsselverteilung kann mit der *Kryptographie mit öffentlichen Schlüsseln* gelöst werden. Dieses Konzept wurde 1975 von Whitfield Diffie und Martin Hellman eingeführt. (Es existieren Beweise dafür, daß der britische Geheimdienst den Schlüssel bereits einige Jahre vor Diffie und Hellman entwickelte, diesen aber als militärisches Geheimnis ungenutzt ließ.)[1]

Kryptographie mit öffentlichen Schlüsseln ist ein asymmetrisches Schema, bei dem zur Verschlüsselung ein *Schlüsselpaar* verwendet wird: Mit einem *öffentlichen Schlüssel* werden Daten verschlüsselt, und mit dem zugehörigen *privaten* oder *geheimen Schlüssel* werden Daten entschlüsselt. Der öffentliche Schlüssel ist allen bekannt, der private Schlüssel dagegen bleibt geheim. Selbst Ihnen völlig fremde Personen mit einer Kopie Ihres öffentlichen Schlüssels können somit Daten verschlüsseln, die aber nur von Ihnen gelesen werden können.

Rein rechnerisch ist es unmöglich, den privaten Schlüssel aus dem öffentlichen Schlüssel abzuleiten. Jeder mit einem öffentlichen Schlüssel kann Daten zwar verschlüsseln, aber nicht entschlüsseln.
Nur die Person mit dem entsprechenden privaten Schlüssel kann die Daten entschlüsseln.

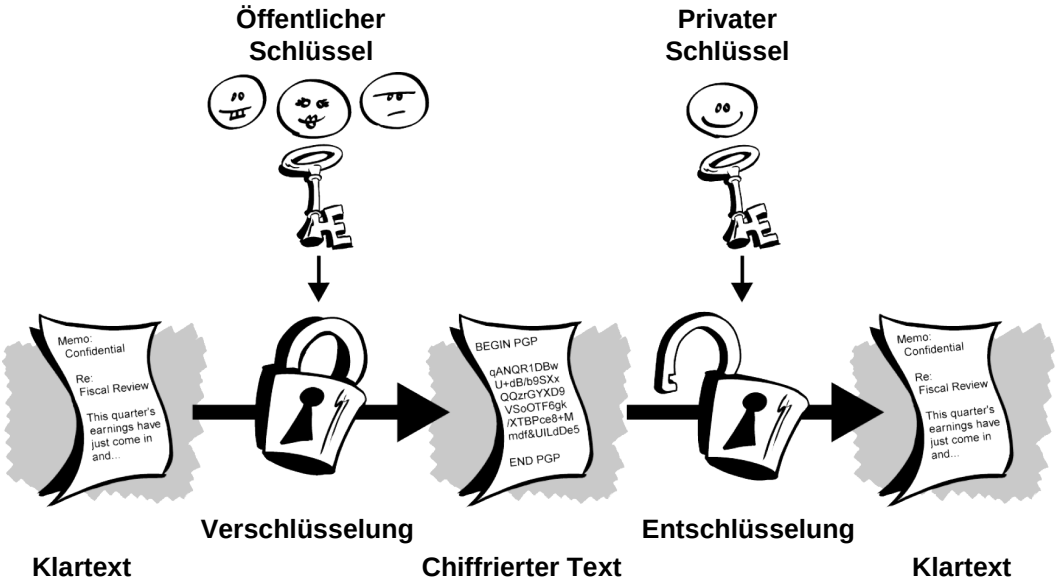

Abbildung 1-3. Verschlüsselung mit öffentlichen Schlüsseln

1. J. H. Ellis, „The Possibility of Secure Non-Secret Digital Encryption“, CESG-Bericht, Januar 1970. [CESG ist die für öffentliche Nutzung der Kryptographie zuständige Regierungsbehörde in Großbritannien.]

Der Hauptvorteil der Kryptographie mit öffentlichen Schlüsseln besteht darin, daß Nachrichten sicher ausgetauscht werden können, ohne daß vorher eine Sicherheitsabsprache getroffen werden muß. Das Übertragen von geheimen Schlüsseln zwischen Absender und Empfänger über einen sicheren Kanal ist nicht mehr notwendig. Für jede Kommunikation sind nur noch öffentliche Schlüssel erforderlich, private Schlüssel werden dagegen nicht übertragen oder gemeinsam verwendet. Beispiele für Verschlüsselungssysteme mit öffentlichen Schlüsseln sind Elgamal (nach dem Erfinder Taher Elgamal benannt), RSA (nach den Erfindern Ron Rivest, Adi Shamir und Leonard Adleman benannt), Diffie-Hellman (ebenfalls nach seinen Erfindern benannt) und DAS, der Digital Signature Algorithm (von David Kravitz).

Die konventionelle Verschlüsselung war lange Zeit die einzige Methode zum Übertragen geheimer Informationen, deren Nutzung aufgrund der hohen Kosten für die sicheren Kanäle und den Aufwand der Schlüsselverteilung auf Gruppen mit entsprechenden finanziellen Möglichkeiten, wie Regierungsbehörden und große Banken, begrenzt blieb. Die Verschlüsselung mit öffentlichen Schlüsseln ist die technologische Neuerung, mit der auch der Allgemeinheit eine starke Verschlüsselungstechnik zur Verfügung steht. Der Kurier mit dem mit Handschellen am Handgelenk befestigten Aktenkoffer ist dank dieser Verschlüsselungstechnik „arbeitslos“ (wahrscheinlich sehr zu seiner Erleichterung).

Funktionsweise von PGP

PGP ist ein *hybrides Verschlüsselungssystem*, in dem einige der besten Funktionen der konventionellen Verschlüsselung und der Verschlüsselung mit öffentlichen Schlüsseln kombiniert sind.

Beim Verschlüsseln von Klartext mit PGP wird dieser Text zuerst komprimiert. Durch Datenkomprimierung wird die Übertragungszeit bei Modemübertragungen verringert sowie Platz auf der Festplatte gespart und, was noch wichtiger ist, die kryptographische Sicherheit gesteigert. Die meisten kryptoanalytischen Verfahren nutzen im Klartext gefundene Muster zum Decodieren des Chiffriercodes. Durch die Datenkomprimierung werden diese Strukturen im Klartext reduziert, wodurch der Schutz vor kryptoanalytischen Angriffen deutlich vergrößert wird. (Dateien, die zum Komprimieren zu kurz sind oder die nicht gut komprimiert werden können, werden nicht komprimiert.)

PGP erstellt dann einen *Sitzungsschlüssel*, einen Geheimschlüssel zum einmaligen Gebrauch. Dieser Schlüssel ist eine Zufallszahl, die aus den willkürlichen Bewegungen, die Sie mit der Maus ausgeführt haben, und den von Ihnen ausgeführten Tastenanschlägen erstellt wird. Mit diesem Sitzungsschlüssel und einem sehr sicheren und schnellen konventionellen Verschlüsselungsalgorith-

mus wird der Klartext zu einem chiffrierten Text verschlüsselt. Nach der Verschlüsselung der Daten wird der Sitzungsschlüssel selbst mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. Dieser mit einem öffentlichen Schlüssel verschlüsselte Sitzungsschlüssel wird zusammen mit dem chiffrierten Text an den Empfänger übertragen.

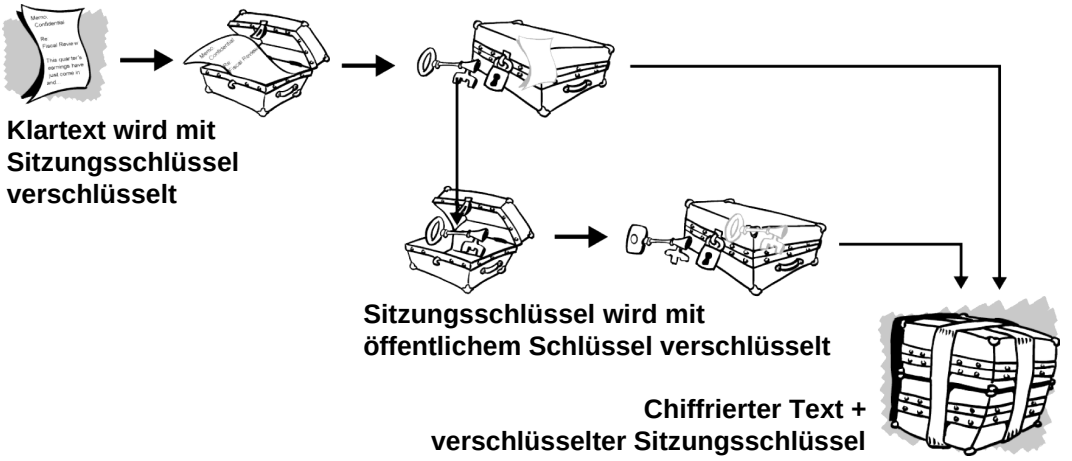

Abbildung 1-4. Funktionsweise der PGP-Verschlüsselung

Die Entschlüsselung läuft in umgekehrter Reihenfolge ab. In der PGP-Kopie des Empfängers wird dessen privater Schlüssel verwendet, um den temporären Sitzungsschlüssel wiederherzustellen. Diesen verwendet PGP anschließend, um den konventionell verschlüsselten chiffrierten Text zu entschlüsseln.

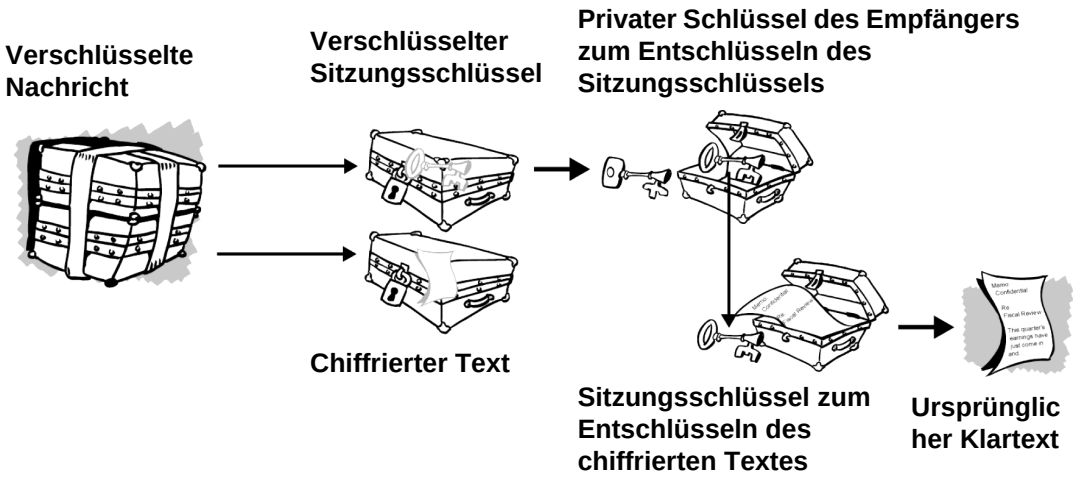

Abbildung 1-5. Funktionsweise der PGP-Entschlüsselung

Die Kombination zweier Verschlüsselungsmethoden vereint die Vorteile der Verschlüsselung mit öffentlichen Schlüsseln und die Geschwindigkeit der konventionellen Verschlüsselung. Die konventionelle Verschlüsselung ist ungefähr 1.000 mal schneller als die Verschlüsselung mit öffentlichen Schlüsseln. Mit öffentlichen Schlüsseln können aber die bisherigen Probleme der Schlüsselverteilung und der Datenübertragung gelöst werden. Durch eine gemeinsame Nutzung werden Leistungsfähigkeit und Schlüsselverteilung ohne Sicherheitseinbußen optimiert.

Schlüssel

Ein Schlüssel ist ein Wert, der zur Erstellung eines verschlüsselten Textes mit einem Verschlüsselungsalgorithmus arbeitet. Schlüssel sind im Prinzip sehr lange Zahlenketten. Die Schlüsselgröße wird in Bit angegeben. Die Zahl, die einen 1024-Bit-Schlüssel darstellt, ist riesig groß. Bei der Verschlüsselung mit öffentlichen Schlüsseln gilt: Je größer der Schlüssel, desto sicherer ist der verschlüsselte Text.

Die Größe von öffentlichen Schlüsseln steht jedoch nicht im Zusammenhang mit der Größe der geheimen Schlüssel bei der konventionellen Verschlüsselung. Ein konventioneller 80-Bit-Schlüssel ist so stark wie ein öffentlicher Schlüssel von 1024 Bit, ein konventioneller 128-Bit-Schlüssel ist so stark wie ein öffentlicher Schlüssel von 3000 Bit. Auch hier ist der größere Schlüssel der sicherere, jedoch sind die für die einzelnen Verschlüsselungstypen verwendeten Algorithmen so unterschiedlich, daß ein Vergleich nicht möglich ist.

Öffentliche und private Schlüssel stehen zwar mathematisch gesehen in Beziehung, es ist jedoch sehr schwierig, den privaten Schlüssel allein aus dem öffentlichen Schlüssel herzuleiten. Bei genügend Zeit und entsprechender Computertechnik ist dies jedoch nicht unmöglich. Daher ist es wichtig, daß Schlüssel ausgewählt werden, die ausreichend lang, aber gleichzeitig kurz genug sind, um eine relativ schnelle Anwendung zu ermöglichen. Sie sollten darüber hinaus in Betracht ziehen, wer mit welcher Intention und welchen Mitteln versuchen könnte, auf Ihre Dateien zuzugreifen.

Längere Schlüssel halten kryptoanalytischen Angriffen über einen längeren Zeitraum stand. Wenn Daten mehrere Jahre verschlüsselt bleiben sollen, ist die Verwendung eines sehr langen Schlüssels empfehlenswert. Es läßt sich natürlich nicht voraussagen, wie lange Ihr Schlüssel angesichts der schnelleren und noch effizienteren Computertechnik von morgen sicher ist. Auch ein symmetrischer 56-Bit-Schlüssel wurde einmal als extrem sicher angesehen.

Die Schlüssel selbst werden in verschlüsselter Form gespeichert. In PGP werden die Schlüssel auf Ihrer Festplatte in zwei Dateien gespeichert, einer Datei für öffentliche und einer für private Schlüssel. Diese Dateien werden als *Schlüsselbunde* bezeichnet. Bei Verwendung von PGP fügen Sie die öffentlichen Schlüssel der Empfänger Ihrem öffentlichen Schlüsselbund hinzu. Ihre privaten Schlüssel werden in Ihrem privaten Schlüsselbund gespeichert. Wenn Sie Ihr privates Schlüsselbund verlieren, können Sie die mit den Schlüsseln an diesem Bund verschlüsselten Informationen nicht mehr entschlüsseln.

Digitale Unterschriften

Ein wesentlicher Vorteil der Verschlüsselung mit öffentlichen Schlüsseln besteht in der Verwendung von *digitalen Unterschriften*. Mit digitalen Unterschriften können Empfänger die Informationen nach Erhalt auf deren Ursprung und Vollständigkeit überprüfen. Durch die digitalen Unterschriften auf öffentlichen Schlüsseln kann also die *Authentisierung* und die Daten*integrität* geprüft werden. Außerdem ist auch der *Urheberschaftsnachweis* möglich, wodurch der Absender nicht mehr behaupten kann, die betreffenden Informationen nicht gesendet zu haben. Diese Funktionen sind für die Verschlüsselung mindestens genauso wichtig wie die Geheimhaltung.

Eine digitale Unterschrift hat dieselbe Aufgabe wie eine Unterschrift von Hand. Handschriftliche Unterschriften sind jedoch leichter zu fälschen. Eine digitale Unterschrift hat gegenüber der Unterschrift von Hand den Vorteil, daß sie nahezu fälschungssicher ist und außerdem den Inhalt der Informationen und die Identität des Unterschreibenden bescheinigt.

Einige Benutzer nutzen die digitalen Unterschriften weitaus häufiger als die Verschlüsselung selbst. So kann es Ihnen beispielsweise gleichgültig sein, wer davon weiß, daß Sie 2.000 DM auf Ihr Konto eingezahlt haben, Sie müssen sich nur absolut sicher sein, daß Ihr Gegenüber dabei wirklich ein Bankangestellter ist.

Die grundlegende Methode der Erstellung von digitalen Unterschriften ist in Abbildung 1-6 dargestellt. Statt die Daten mit dem öffentlichen Schlüssel eines anderen Benutzers zu verschlüsseln, verwenden Sie dazu Ihren privaten Schlüssel. Wenn die Daten mit Ihrem öffentlichen Schlüssel entschlüsselt werden können, ist dies ein Beweis dafür, daß sie von Ihnen stammen.

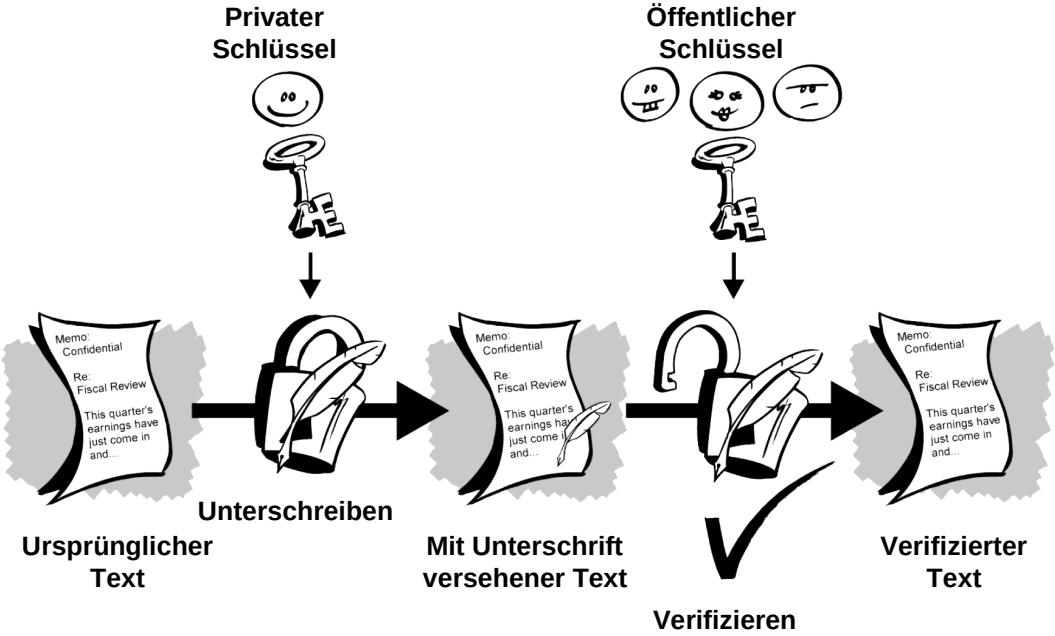

Abbildung 1-6. Einfache digitale Unterschriften

Hash-Funktionen

Das oben beschriebene System hat einige Nachteile: Es ist langsam und produziert eine gewaltige Datenmenge, mindestens das Doppelte der ursprünglichen Daten. Eine Verbesserung wird durch Hinzufügen einer einseitigen *Hash-Funktion* erzielt. Bei einer Einweg-Hash-Funktion wird eine Information beliebiger Länge eingegeben, beispielsweise eine Nachricht von tausend oder sogar mehreren Millionen Bit, und es wird eine Ausgabe fester Länge erzeugt (z. B. 160 Bit). Mit der Hash-Funktion wird gewährleistet, daß auch bei geringfügiger Änderung der Eingangsinformation ein völlig veränderter Ausgabewert erzeugt wird.

Mit PGP wird der vom Benutzer unterschriebene Klartext durch eine kryptographisch starke Hash-Funktion verschlüsselt. Dadurch wird ein Datenelement mit einer festen Länge erstellt, das auch als *Nachrichtenkern* bezeichnet wird. (Jede Änderung der Information resultiert in einem völlig veränderten Nachrichtenkern.)

Anhand des Nachrichtenkerns und des privaten Schlüssels wird dann die Unterschrift erstellt. Die Unterschrift und der Klartext werden zusammen übertragen. Bei Erhalt der Nachricht berechnet der Empfänger mit Hilfe von PGP den Nachrichtenkern neu und überprüft damit auch die Unterschrift. PGP kann den Klartext gegebenenfalls verschlüsseln. Das Unterschreiben des Klartextes ist immer dann sinnvoll, wenn einige Empfänger die Unterschrift nicht überprüfen möchten oder können.

Solange eine sichere Hash-Funktion verwendet wird, können Unterschriften nicht in andere Dokumente eingefügt oder unterschriebene Nachrichten geändert werden. Durch die geringfügigste Änderung eines unterschriebenen Dokuments wird die Verifizierung einer digitalen Unterschrift scheitern.

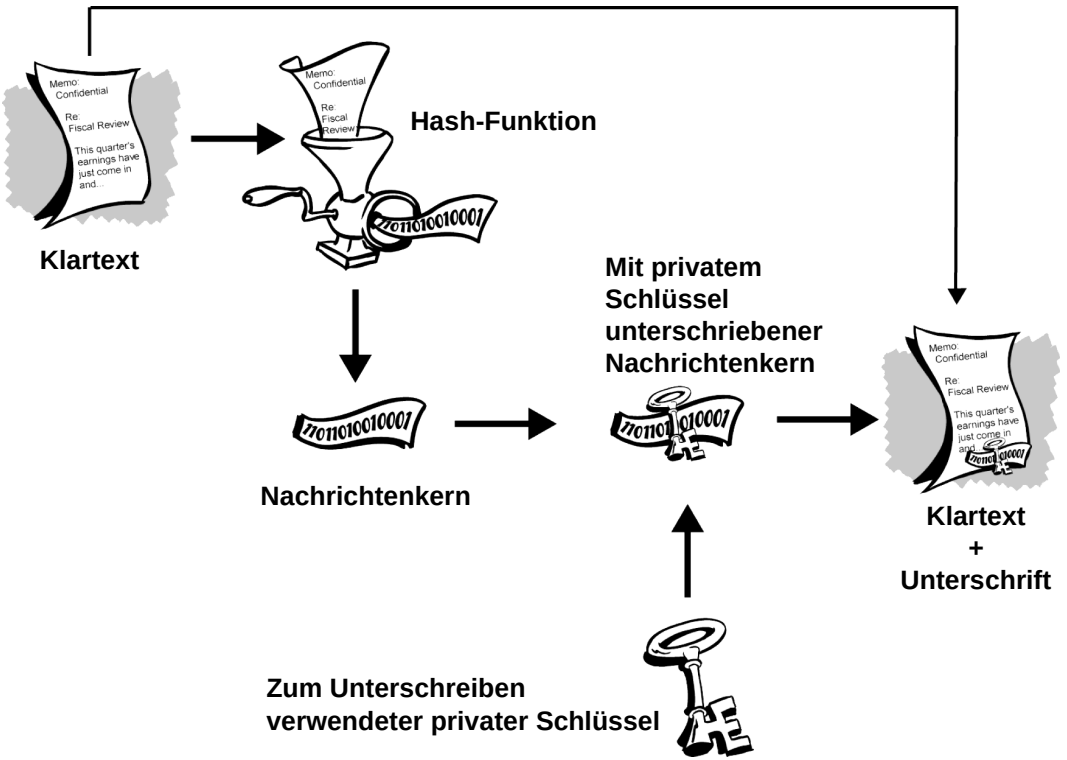

Abbildung 1-7. Sichere digitale Unterschriften

Digitale Unterschriften sind ein wichtiger Faktor bei der Authentisierung und *Überprüfung* der Schlüssel anderer PGP-Benutzer.

Digitalzertifikate

Ein Nachteil bei Verschlüsselungssystemen mit öffentlichen Schlüsseln besteht darin, daß Benutzer beim Verschlüsseln stets darauf achten müssen, daß Sie den Schlüssel des richtigen Benutzers verwenden. In einer Umgebung, in der es als sicher gilt, Schlüssel über öffentliche Server auszutauschen, stellen *Abfangangriffe* daher eine potentielle Gefahr dar. Dabei wird ein gefälschter Schlüssel mit dem Namen und der Benutzer-ID des eigentlichen Empfängers eingeschleust. Die verschlüsselten und vom wahren Eigentümer des gefälschten Schlüssels erhaltenen Daten gelangen somit in die falschen Hände.

In einer Umgebung mit öffentlichen Schlüsseln ist es äußerst wichtig, daß der verwendete öffentliche Schlüssel tatsächlich dem beabsichtigten Empfänger gehört und keine Fälschung ist. Sie könnten natürlich einfach nur die Schlüssel verwenden, die Ihnen persönlich überreicht wurden. Was aber, wenn Sie Daten mit Personen austauschen müssen, denen Sie nie zuvor begegnet sind? Wie können Sie sich sicher sein, daß Sie über den richtigen Schlüssel verfügen?

Durch *Digitalzertifikate* wird die Überprüfung, ob ein Schlüssel wirklich dem angegebenen Eigentümer gehört, vereinfacht.

Ein Zertifikat ist eine Beglaubigung, wie beispielsweise Ihr Ausweis, Ihre Versicherungskarte oder Ihre Geburtsurkunde. Jedes dieser Dokumente enthält Informationen, durch die Ihre Identität nachgewiesen wird, sowie eine Beglaubigung durch eine Behörde, die Ihre Identität bestätigt. Bei einigen dieser Dokumente, wie beispielsweise Ihrem Ausweis, müssen Sie besonders darauf achten, dieses Dokument nicht zu verlieren. Bei Verlust könnte sich jemand den Ausweis aneignen und sich für Sie ausgeben.

Bei einem Digitalzertifikat handelt es sich um Daten, deren Funktionsweise der eines physischen Zertifikats ähnelt. Ein Digitalzertifikat besteht aus Daten, die dem öffentlichen Schlüssel einer Person hinzugefügt werden. Anhand dieser Daten kann festgestellt werden, ob ein Schlüssel *gültig* ist. Damit können dann Versuche, den Schlüssel einer Person durch den einer anderen auszutauschen, vereitelt werden.

Ein Digitalzertifikat besteht aus folgenden Elementen:

- Einem öffentlichen Schlüssel.
- Zertifikatsdaten (Daten zur „Identität“ eines Benutzers, wie beispielsweise der Name, die Benutzer-ID etc.).
- Einer oder mehreren digitalen Unterschriften.

Mit einer digitalen Unterschrift auf einem Zertifikat sollen die Zertifikatsdaten durch eine dritte Person oder Behörde beglaubigt werden. Mit der digitalen Unterschrift wird nicht die Echtheit des gesamten Zertifikats bestätigt, sondern nur ausgesagt, daß die unterschriebenen Angaben zur Identität zum öffentlichen Schlüssel gehören oder an diesen *gebunden sind.*

Ein Zertifikat ist also im Grunde ein öffentlicher Schlüssel, dem eine oder zwei Arten von IDs und ein Genehmigungsstempel von einer anderen vertrauensvollen Person angehängt sind.

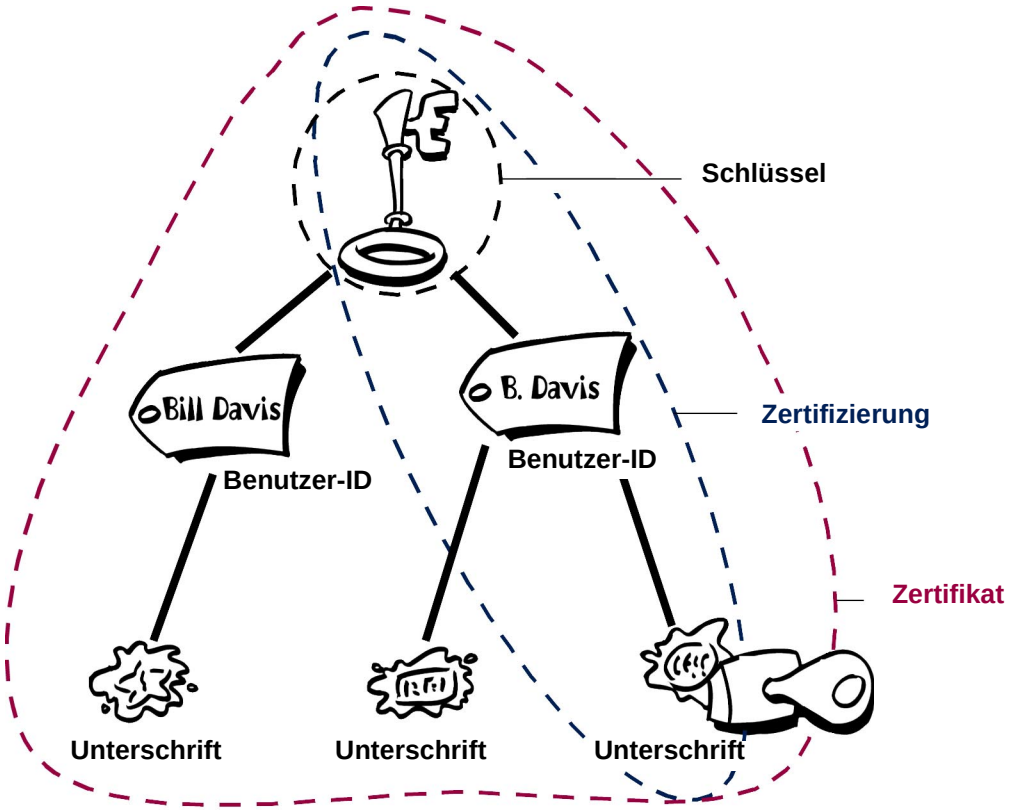

Abbildung 1-8. Bestandteile eines PGP-Zertifikats

Zertifikatsverteilung

Zertifikate werden verwendet, wenn es nötig ist, mit einer anderen Person die öffentlichen Schlüssel auszutauschen. Kleine Gruppen, die ihre Kommunikation untereinander geheim halten möchten, können manuell Disketten oder E-Mails mit den jeweiligen öffentlichen Schlüsseln der Eigentümer austauschen. Hierbei handelt es sich um die *manuelle Verteilung öffentlicher Schlüssel*, deren Anwendung nur bis zu einem gewissen Grad praktisch ist. Darüber hinaus müssen Systeme verwendet werden, die mit der notwendigen Sicherheit, Speicherkapazität und den notwendigen Austauschmechanismen ausgestattet sind, so daß Kollegen, Geschäftspartner oder Fremde bei Bedarf miteinander kommunizieren können. Beispielsweise in Form von Verwahrungsorten, die nur der Speicherung dienen, sogenannten *Certificate Servers* oder besser strukturierten Systemen, die zusätzliche Schlüsselverwaltungsfunktionen aufweisen und *Public Key Infrastructures (PKIs)* genannt werden.

Certificate Servers

Ein *Certificate Server* auch *Cert Server* oder *Schlüssel-Server* genannt, ist eine Datenbank, die es Benutzern ermöglicht, Digitalzertifikate zu übermitteln und abzurufen. Ein Cert Server verfügt normalerweise über einige Verwaltungsfunktionen zur Aufrechterhaltung der Sicherheitsrichtlinien für Unternehmen. So werden beispielsweise nur die Schlüssel gespeichert, die bestimmte Anforderungen erfüllen.

Public Key Infrastructures

Eine PKI weist die Zertifikatsspeicherungsfunktion eines Certificate Servers auf und bietet darüber hinaus Zertifikatsverwaltungsfunktionen (die Fähigkeit, Zertifikate auszustellen, zurückzunehmen, zu speichern, abzurufen und Zertifikaten zu vertrauen). Das Hauptmerkmal einer PKI ist die Einführung der *Zertifizierungsinstanz* oder *CA*. Hierbei handelt es sich um eine Person, Gruppe, Abteilung, Firma oder um einen anderen Personenzusammenschluß, der von einem Unternehmen zur Zertifikatsausstellung für die Computerbenutzer ermächtigt ist. (Die Funktion einer CA entspricht der einer Ausweisausstellungsbehörde eines Landes.) Eine CA erstellt Zertifikate und unterschreibt diese digital mit Hilfe des eigenen privaten Schlüssels. Die Funktion der Zertifikatserstellung macht die CA zur zentralen Komponente einer PKI. Mit dem öffentlichen Schlüssel der CA kann jeder, der die Echtheit eines Zertifikats überprüfen möchte, die digitale Unterschrift der ausstellenden CA und somit die Integrität des Zertifikatsinhalts verifizieren (hauptsächlich den öffentlichen Schlüssel und die Identität des Zertifikatsinhabers).

Zertifikatsformate

Bei einem digitalen Zertifikat handelt es sich im Grunde um eine Informationsansammlung zur Identifizierung. Diese Informationen sind durch einen öffentlichen Schlüssel zusammengefaßt und deren Echtheit ist durch einen autorisierten Dritten unterschrieben. Ein digitales Zertifikat hat eines der verschiedenen *Formate.*

Von PGP werden zwei verschiedene Zertifikatsformate anerkannt:

- PGP-Zertifikate
- X.509-Zertifikate

PGP-Zertifikatsformat

Ein PGP-Zertifikat enthält mindestens die folgenden Informationen:

- **Die PGP-Versionsnummer**. Hiermit wird gekennzeichnet, welche Version von PGP für die Erstellung des mit dem Zertifikat verbundenen Schlüssels verwendet wurde.
- **Der öffentliche Schlüssel des Zertifikatsinhabers**. Der öffentliche Anteil des Schlüsselpaars zusammen mit dem Algorithmus des Schlüssels: RSA, DH (Diffie-Hellman) oder DSA (Digital Signature Algorithm).
- **Die Daten des Zertifikatsinhabers**. Daten zur „Identität“ eines Benutzers, wie beispielsweise der Name, die Benutzer-ID, Foto usw.
- **Die digitale Unterschrift des Zertifikatseigentümers**, auch *eigene Unterschrift* genannt. Hierbei handelt es sich um die Unterschrift, für die der entsprechende, mit dem Zertifikat verbundene, private Schlüssel verwendet wird.
- **Die Gültigkeitsdauer des Zertifikats**, also das Anfangs- und Ablaufdatum des Zertifikats. Gibt an, wann das Zertifikat abläuft.
- **Der bevorzugte symmetrische Verschlüsselungsalgorithmus für die Schlüssel**. Gibt den Verschlüsselungsalgorithmus an, für den der Zertifikatseigentümer Informationen verschlüsselt haben möchte. Die unterstützten Algorithmen sind CAST (Standard), IDEA oder Triple-DES.

Sie halten ein PGP-Zertifikat möglicherweise für einen öffentlichen Schlüssel mit einer oder mehreren Bezeichnungen (siehe Abbildung 1-9). Diese „Bezeichnungen“ geben Informationen über den Schlüsseleigentümer an und enthalten die Unterschrift des Schlüsseleigentümers, die angibt, daß der Schlüssel und die Identifikation zusammengehören. (Diese bestimmte Unterschrift wird *eigene- Unterschrift* genannt. Jedes PGP-Zertifikat enthält eine eigene Unterschrift.)

Ein eindeutiger Aspekt des PGP-Zertifikatformats ist, daß ein einzelnes Zertifikat mehrere Unterschriften enthalten kann. Es können mehrere verschiedene Personen das Schlüssel-/Identifikationspaar unterschreiben, und somit zu ihrer eigenen Sicherheit bestätigen, daß der öffentliche Schlüssel eindeutig zum angegebenen Eigentümer gehört. Auf einem öffentlichen Certificate Server stellen Sie möglicherweise fest, daß bestimmte Zertifikate, wie beispielsweise das des Entwicklers von PGP, Phil Zimmermann, viele Unterschriften enthält.

Manche PGP-Zertifikate haben einen öffentlichen Schlüssel mit verschiedenen Bezeichnungen, von denen jeder den Schlüsseleigentümer auf eine andere Art identifiziert (z. B. Eigentümername und E-Mail-Adresse im Unternehmen, Spitzname des Eigentümers und E-Mail-Adresse zu Hause, ein Foto des Eigentümers, alles in einem Zertifikat). Die Liste der Unterschriften für jede dieser Identitäten kann unterschiedlich sein. Mit Unterschriften wird bestätigt, daß eine der Bezeichnungen zum öffentlichen Schlüssel gehört, es wird jedoch nicht die Echtheit aller Bezeichnungen bestätigt. (Beachten Sie, daß der Begriff „authentisch“ immer subjektiv ist. Unterschriften stellen eine Form der Meinungsäußerung dar. Es werden unterschiedliche Stufen der Sorgfalt bei der Authentisierungsprüfung angewandt, bevor ein Schlüssel unterschrieben wird.)

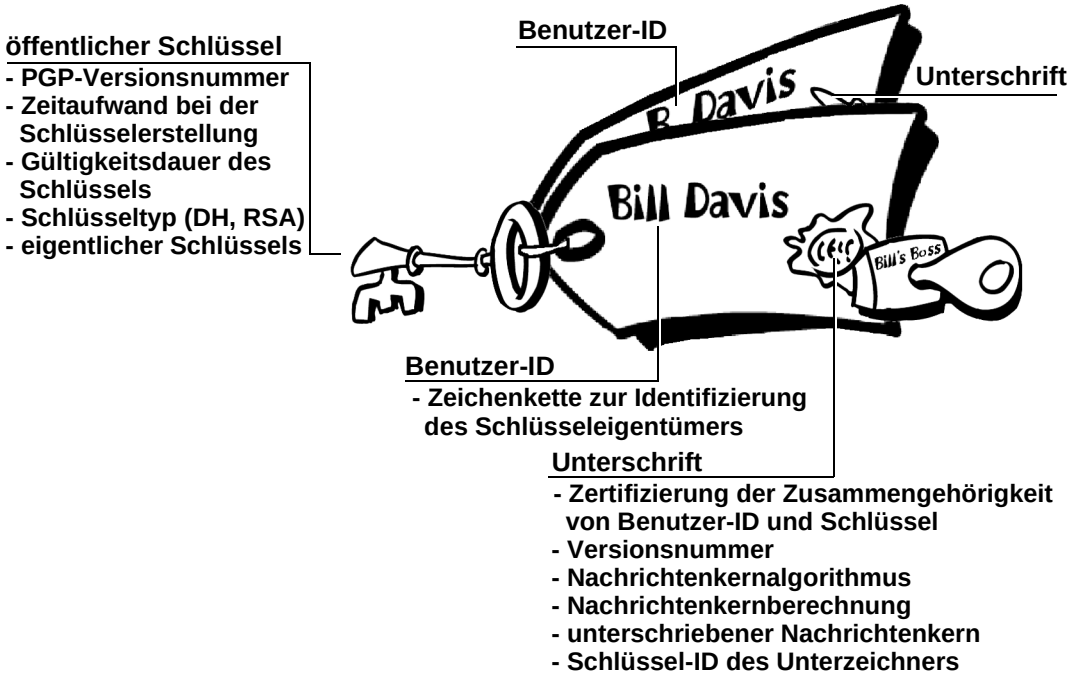

Abbildung 1-9. PGP-Zertifikat

X.509-Zertifikatsformat

X.509 ist ebenfalls ein bekanntes Zertifikatsformat. Alle X.509-Zertifikate stimmen mit dem internationalen Standard ITU-T X.509 überein. Deshalb können theoretisch X.509-Zertifikate, die für eine Anwendung erstellt wurden, von allen anderen Anwendungen, die X.509 einhalten, verwendet werden. In der Praxis haben unterschiedliche Unternehmen jedoch für ihre X.509-Zertifikate eigene Dateierweiterungen erstellt, von denen nicht alle zusammenarbeiten können.

Für ein Zertifikat muß überprüft werden, ob ein öffentlicher Schlüssel und der Name eines Schlüsseleigentümers zusammengehören. Bei einem PGP-Zertifikat kann jeder die Rolle der überprüfenden Person übernehmen. Bei einem X.509-Zertifikat handelt es sich bei der überprüfenden Person immer um eine Zertifizierungsinstanz oder um eine Person, die von einer CA benannt wurde. (Beachten Sie, daß PGP-Zertifikate eine hierarchische Struktur ebenfalls mit Hilfe einer *CA* für die Überprüfung von Zertifikaten vollständig unterstützen.)

Ein X.509-Zertifikat ist eine Sammlung von Standardfeldern, die Informationen über einen Benutzer oder ein Gerät und die entsprechenden öffentlichen Schlüssel enthalten. Der X.509-Standard legt fest, welche Informationen in das Zertifikat aufgenommen werden und beschreibt, wie es entschlüsselt wird (das Datenformat). Alle X.509-Zertifikate enthalten die folgenden Daten:

- **Die X.509-Versionsnummer**. Hiermit wird gekennzeichnet, welche X.509-Standardversion auf dieses Zertifikat zutrifft. Das hat Einfluß darauf, welche Informationen darin angegeben werden können. Die aktuelleste Version ist Version 3.
- **Der öffentliche Schlüssel des Zertifikatsinhabers**. Der öffentliche Schlüssel des Zertifikatsinhabers zusammen mit einer Algorithmuskennung, die das Verschlüsselungssystem bestimmt, dem der Schlüssel angehört, und alle zugehörigen Schlüsselparameter.
- **Die Seriennummer des Zertifikats**. Der Dritte (Anwendung oder Person), der das Zertifikat erstellt hat, muß dem Zertifikat eine eindeutige Seriennummer zuordnen, um es so von anderen ausgestellten Zertifikaten zu unterscheiden. Diese Informationen werden auf viele Arten verwendet. Wenn beispielsweise ein Zertifikat zurückgenommen wird, wird die Seriennummer in die *Liste der zurückgenommenen Zertifikate*oder *CRL* aufgenommen.

- **Die eindeutige Kennung des Zertifikatsinhabers** (oder *DN Eindeutiger Name*). Der Name sollte innerhalb des Internets eindeutig sein. Eine DN besteht aus mehreren Unterabschnitten und kann folgendermaßen aussehen:

  CN=Bob Allen, OU=Total Network Security Division, O=Network Associates, Inc., C=US

  (Diese beziehen sich auf den bekannten Namen (Common Name), die Firmenabteilung (Organizational Unit), die Firma (Organization) und das Land (Country) des Objekts.)

- **Die Gültigkeitsdauer des Zertifikats**, also das Anfangs- und Ablaufdatum des Zertifikats. Gibt an, wann das Zertifikat abläuft.

- **Der eindeutige Name des Zertifikatsausstellers**. Ein eindeutiger Name des Dritten, der das Zertifikat unterschrieben hat. Hierbei handelt es sich normalerweise um eine CA. Die Verwendung des Zertifikats setzt Vertrauen gegenüber dem Dritten, der das Zertifikat unterschrieben hat, voraus. (In einigen Fällen unterschreibt der Aussteller sein eigenes Zertifikat. Beispielsweise bei *Root*-CA-Zertifikaten oder CA-Zertifikaten der *obersten Stufe*.)

- **Die digitale Unterschrift des Ausstellers**. Die Unterschrift, für die der private Schlüssel des Dritten verwendet wird, der das Zertifikat ausgestellt hat.

- **Die Kennung für den Unterschriftenalgorithmus**. Kennzeichnet den von der CA für das Unterschreiben des Zertifikats verwendeten Algorithmus.

Es bestehen viele Unterschiede zwischen einem X.509- und einem PGP-Zertifikat. Die wichtigsten sind jedoch die folgenden:

- Sie können Ihr eigenes PGP-Zertifikat erstellen. Sie müssen jedoch die Ausstellung eine X.509-Zertifikats bei einer Zertifizierungsinstanz anfordern.

- X.509-Zertifikate unterstützen grundsätzlich nur einen einzigen Namen für einen Schlüsseleigentümer.

- X.509-Zertifikate unterstützen nur eine einzige digitale Unterschrift zur Bestätigung der Schlüsselgültigkeit.

Für den Erhalt eines X.509-Zertifikats müssen Sie bei einer CA die Ausstellung eines Zertifikats beantragen. Stellen Sie Ihren öffentlichen Schlüssel zur Verfügung und überprüfen Sie, ob Sie über den entsprechenden privaten Schlüssel und bestimmte Informationen über Ihre Person verfügen. Setzen Sie anschließend die digitale Unterschrift unter die Informationen und senden Sie das gesamte Paket der Zertifikatsanforderung an die CA. Die CA wendet anschließend die angemessene Sorgfalt an, um zu verifizieren, daß die angegebenen Informationen ihre Richtigkeit haben. Ist dies der Fall, erstellt sie das Zertifikat und sendet dieses an Sie zurück.

Sie stellen sich ein X.509-Zertifikat möglicherweise wie ein standardmäßiges Zertifikat auf Papier (ähnlich dem Zertifikat eines Erste Hilfe-Kurses) mit einem öffentlichen Schlüssel vor. Es enthält Ihren Namen und einige Informationen zu Ihrer Person sowie die Unterschrift der ausstellenden Person.

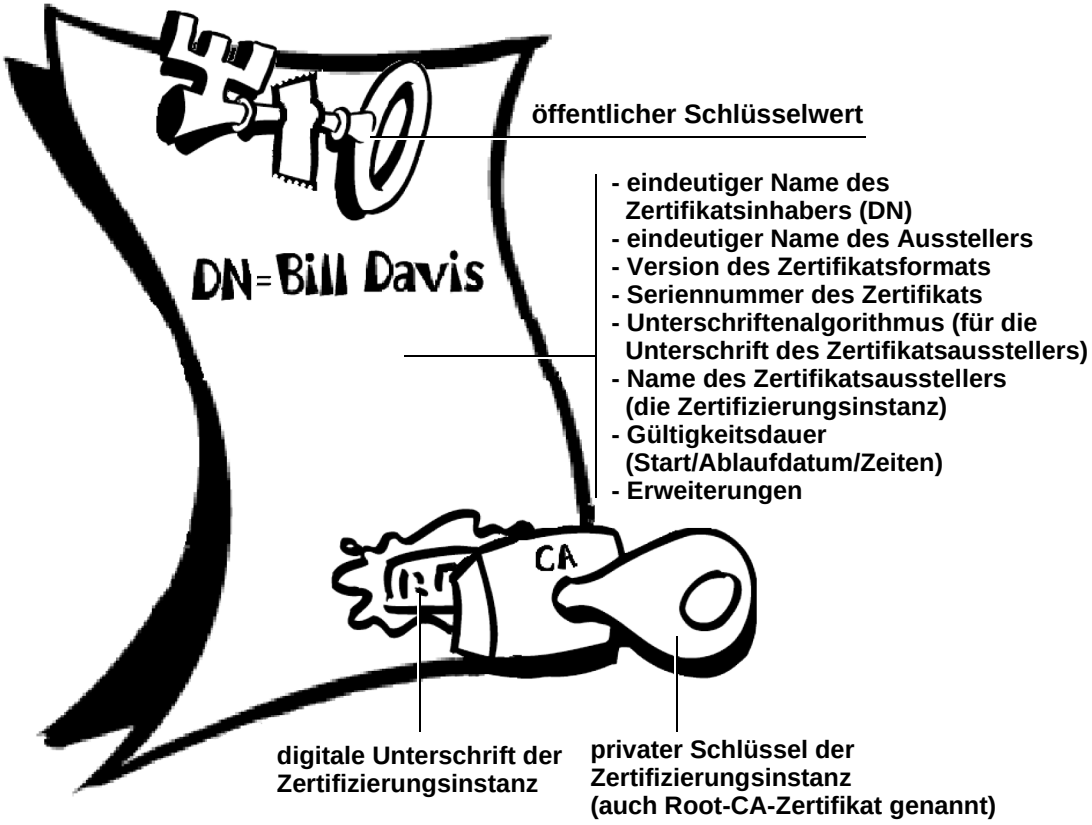

Abbildung 1-10. Ein X.509-Zertifikat

Heute werden X.509-Zertifikate vermutlich am häufigsten in Web-Browsern verwendet.

Gültigkeit und Vertrauen

Kein Benutzer eines Systems mit öffentlichen Schlüsseln ist davor gefeit, einen gefälschten Schlüssel (Zertifikat) mit einem echten Schlüssel zu verwechseln. *Gültigkeit* bedeutet Vertrauen dahingehend, daß ein öffentliches Schlüsselzertifikat dem angegebenen Eigentümer gehört. Gültigkeit ist in einer Umgebung mit öffentlichen Schlüsseln von großer Bedeutung, in der ständig überprüft werden muß, ob ein bestimmtes Zertifikat echt ist.

Wenn Sie sich davon überzeugt haben, daß ein Zertifikat eines anderen Benutzers gültig ist, können Sie die Kopie an Ihrem lokalen Schlüsselbund unterschreiben und damit bestätigen, daß Sie das Zertifikat geprüft und für echt befunden haben. Wenn Sie auch anderen Benutzern mitteilen möchten, daß Sie dem Zertifikat Ihren Genehmigungsstempel erteilt haben, können Sie die Unterschrift an einen Certificate Server exportieren, damit andere sie sehen können.

Wie im Abschnitt „Public Key Infrastructures“ beschrieben, benennen manche Unternehmen eine Zertifizierungsinstanz (CA) oder mehrere für die Angabe der Gültigkeit der Zertifikate. In einem Unternehmen, in dem eine PKI mit X.509-Zertifikat verwendet wird, liegt es in der Verantwortung der CA, die Zertifikate für die Benutzer *auszustellen*. Dieser Vorgang erfordert normalerweise die Beantwortung einer Benutzeranforderung für ein Zertifikat. In einem Unternehmen, in dem PGP-Zertifikate ohne PKI verwendet werden, liegt es im Verantwortungsbereich der CA, die Echtheit aller PGP-Zertifikate zu überprüfen und dann die gültigen zu unterschreiben. Der Hauptzweck einer CA ist grundsätzlich, einen öffentlichen Schlüssel mit im Zertifikat enthaltenen Identifikationsinformationen zu verbinden und somit Dritten zu versichern, daß eine gewisse Sorgfalt bei der Verbindung der Identifikationsinformationen verwendet wurde und der Schlüssel gültig ist.

Die CA ist die oberste Instanz für die Gültigkeitsprüfung in einem Unternehmen und genießt das volle Vertrauen aller. In einigen Unternehmen, in denen beispielsweise eine PKI verwendet wird, wird ein Zertifikat sogar erst dann als gültig angesehen, wenn dies von einer CA attestiert wurde.

Gültigkeit überprüfen

Eine Möglichkeit der Gültigkeitsbestätigung besteht in der manuellen Überprüfung. Dazu gibt es mehrere Optionen: Sie können vom beabsichtigten Empfänger verlangen, Ihnen eine Kopie des öffentlichen Schlüssels persönlich zu übergeben. Das ist jedoch oft umständlich und wenig effizient.

Eine andere Möglichkeit besteht in der Überprüfung des *Fingerabdrucks* des Zertifikats. Ein Fingerabdruck eines PGP-Zertifikats ist genauso einzigartig wie der eines Menschen. Der Fingerabdruck ist ein Hash des Zertifikats eines Benutzers. Er wird als eine der Eigenschaften des Zertifikats aufgeführt. In PGP kann ein Fingerabdruck als hexadezimale Zahl oder als eine Reihe sogenannter *biometrischer Wörter* angezeigt werden, die sich phonetisch voneinander unterscheiden und zur Vereinfachung des Identifikationsvorgangs des Fingerabdrucks dienen.

Sie können die Gültigkeit des Zertifikats überprüfen, indem Sie den Schlüsseleigentümer anrufen (so daß die Datenübertragung von Ihnen initiiert wird) und ihn darum bitten, den Fingerabdruck des Schlüssels durchzusagen. Sie können dann diesen Fingerabdruck mit dem vermeintlich richtigen vergleichen. Dies ist natürlich nur dann sinnvoll, wenn Sie die Stimme des Schlüsseleigentümers kennen. Wie können Sie jedoch die Identität einer unbekannten Person manuell überprüfen? Aus diesem Grund lassen einige Personen ihren Fingerabdruck auf ihre Visitenkarten drucken.

Eine andere Möglichkeit, ein Zertifikat auf dessen Gültigkeit zu überprüfen, besteht darin, darauf zu *vertrauen*, daß eine dritte Person die Überprüfung bereits vorgenommen hat.

So ist beispielsweise eine CA dafür zuständig, vor dem Ausstellen des Zertifikats sorgfältig zu prüfen, daß der öffentliche Schlüsselanteil tatsächlich dem angegebenen Eigentümer gehört. Jeder Benutzer, der der CA vertraut, betrachtet damit automatisch alle von der CA als gültig unterschriebenen Zertifikate als gültig.

Überprüfen Sie als anderen Aspekt der Gültigkeitsprüfung, daß ein Zertifikat nicht zurückgenommen wurde. Weitere Informationen finden Sie im Abschnitt „Zurücknahme von Zertifikaten“.

Vertrauen festlegen

Sie überprüfen *Zertifikate*. Sie vertrauen *Personen*. Genauer gesagt, vertrauen Sie anderen Personen dahingehend, daß sie die Gültigkeit der Zertifikate Dritter überprüfen. Wenn Ihnen das Zertifikat nicht von dessen Eigentümer persönlich überreicht wurde, müssen Sie sich hinsichtlich der Gültigkeit auf die Bestätigung einer anderen Person verlassen.

Höhergestellte und autorisierte Schlüsselverwalter

Meistens wird die CA bei der Überprüfung der Gültigkeit eines Zertifikats vollkommen vertraut. Dies bedeutet, daß alle darauf vertrauen, daß die CA für sie die gesamte manuelle Überprüfung vornimmt. Bis zu einer bestimmten Anzahl von Benutzern bzw. Standorten ist dieses Verfahren durchaus geeignet. Bei einer höheren Anzahl kann die CA aber nicht dasselbe Qualitätsniveau bei der Überprüfung gewährleisten. In diesem Fall müssen weitere Personen zur Überprüfung hinzugefügt werden.

Eine CA kann auch ein höhergestellter Schlüsselverwalter sein. Die Aufgabe eines höhergestellten Schlüsselverwalters beschränkt sich nicht nur auf die Gültigkeitsüberprüfung von Schlüsseln, sondern er kann auch anderen die *Fähigkeit, Schlüssel als echt zu kennzeichnen,* übertragen. So, wie früher ein König sein Siegel seinen engsten Beratern übergeben hat, so daß diese in seinem Namen handeln konnten, kann der höhergestellte Schlüsselverwalter andere zu *autorisierten Schlüsselverwaltern* ernennen. Autorisierte Schlüsselverwalter können die Gültigkeit von Schlüsseln in demselben Maße wie die höhergestellten Systemverwalter bestätigen. Sie können jedoch keine neuen autorisierten Schlüsselverwalter erstellen.

Die Begriffe „höhergestellter Schlüsselverwalter“ und „autorisierter Schlüsselverwalter“ sind PGP-Begriffe. In einer X.509-Umgebung wird der höhergestellte Schlüsselverwalter als *Root-Zertifizierungsinstanz (Root-CA*) und der autorisierte Schlüsselverwalter als *untergeordnete* Zertifizierungsinstanzen bezeichnet.

Die Root-CA verwendet den privaten Schlüssel, der im Zusammenhang mit einem bestimmten Zertifikatstyp (*Root-CA-Zertifikat*) steht, um Zertifikate zu unterschreiben. Alle Zertifikate, die durch das Root-CA-Zertifikat unterschrieben wurden, werden von allen anderen Zertifikaten, die durch das Stammverzeichnis unterschrieben wurden, als gültig angesehen. Dieser Überprüfungsvorgang ist auch auf Zertifikate übertragbar, die von anderen CAs im System unterschrieben wurden. Solange das Root-CA-Zertifikat das untergeordnete CA-Zertifikat unterschrieben hat, wird jedes von der CA unterschriebene Zertifikat für andere in der Hierarchie als gültig angesehen. Dieser Vorgang der rückwärtigen Überprüfung innerhalb des Systems um festzustellen, wer wessen Zertifikat unterschrieben hat, wird als Zurückverfolgung des *Zertifizierungspfades* oder der *Zertifizierungskette* bezeichnet.

Vertrauensmodelle

In relativ geschlossenen Systemen, beispielsweise innerhalb eines kleinen Unternehmens, ist es nicht sehr schwierig, einen Pfad bis zur ursprünglichen CA zurückzuverfolgen. Dennoch müssen Benutzer oft mit Personen außerhalb des Unternehmens kommunizieren, wobei es sich oft um völlig unbekannte Menschen handelt (beispielsweise Auftragnehmer, Kunden, Geschäftspartner etc.). Einen Vertrauenspfad zu jemandem herzustellen, dem von Ihrer CA nicht ausdrücklich vertraut wurde, ist sehr schwierig.

Von Unternehmen wird meist ein bestimmtes *Vertrauensmodell* verwendet, mit dem das Verfahren zur Bestimmung der Gültigkeit von Zertifikaten festgelegt wird. Es gibt drei unterschiedliche Vertrauensmodelle:

- DirectTrust
- Vertrauenshierarchie
- Web of Trust

Direktes Vertrauen

Direktes Vertrauen ist das einfachste Vertrauensmodell. Dabei vertraut ein Benutzer auf die Gültigkeit eines Schlüssels, da dessen Herkunft bekannt ist. Alle Verschlüsselungssysteme nutzen dieses Vertrauensmodell. So sind die ursprünglichen CA-Schlüssel in Web-Browsern beispielsweise direkt vertrauenswürdig, da Sie direkt vom Hersteller zur Verfügung gestellt werden. Eventuelle Hierarchiestufen ergeben sich aus den direkt autorisierten Zertifikaten.

Ein Benutzer, der in PGP die Schlüssel selbst überprüft und keinen anderen autorisierten Schlüsselverwalter einsetzt, arbeitet mit dem direkten Vertrauensmodell.

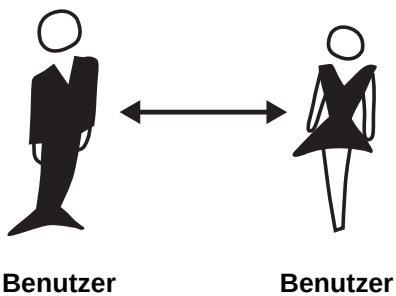

Abbildung 1-11. Direktes Vertrauen

Vertrauenshierarchie

In einem hierarchischen System gibt es eine Anzahl von Root-Zertifikaten („Stamm“-Zertifikate), aus denen sich Vertrauen ergibt. Das Vertrauen kann zwischen gleichrangigen Zertifikaten oder zwischen Zertifikaten unterschiedlicher Hierarchieebenen bestehen. Diese Hierarchien haben eine Baumstruktur, wobei die Echtheit der einzelnen Zertifikate dadurch überprüft werden kann, daß der Weg von ihrer Zertifizierungsinstanz über andere bis zu den Root-Zertifikaten („Stamm“-Zertifikaten) mit direktem Vertrauen zurückverfolgt wird.

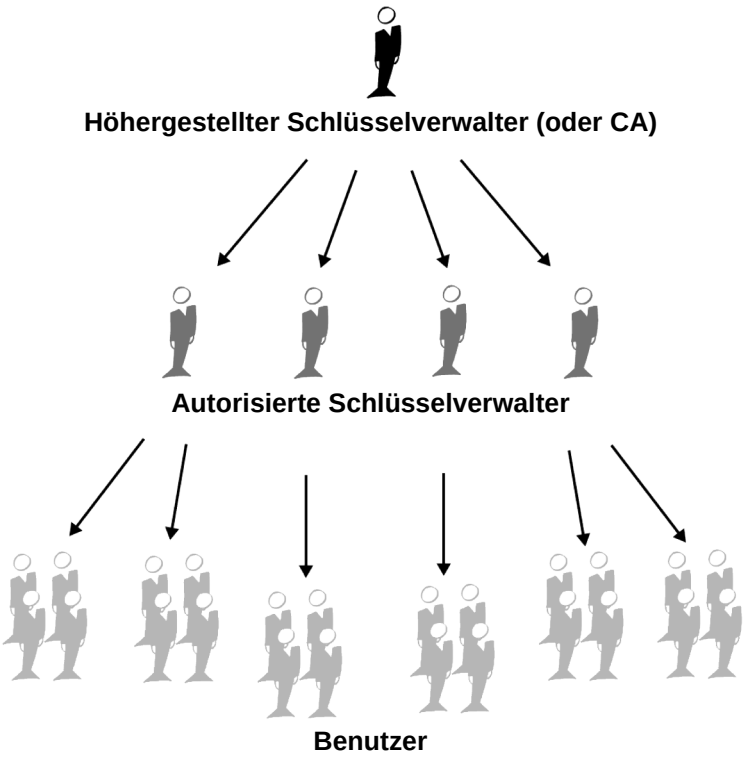

Abbildung 1-12. Vertrauenshierarchie

Web of Trust

In einem Web of Trust sind die beiden vorherigen Vertrauensmodelle kombiniert. Darüber hinaus wird davon ausgegangen, das Vertrauen immer subjektiv ist (realistische Sichtweise) und daß mehr Information auch mehr Sicherheit bedeutet. Es handelt sich hierbei um ein kumulatives Vertrauensmodell. Einem Zertifikat kann direkt, über einen bis auf das direkt vertrauenswürdige Root-Zertifikat (den höhergestellten Schlüsselverwalter) zurückgehenden Pfad oder durch mehrere Schlüsselverwalter vertraut werden.

Vielleicht ist Ihnen die Theorie der *sechs Trennungsebenen* bekannt, die besagt, daß jeder Mensch auf der Welt zu jedem anderen Menschen auf der Welt eine Verbindung herstellen kann, indem er höchstens sechs Menschen als Vermittler verwendet. Dies ist ein Netz von Vermittlern.

Dieses System wird auch im Vertrauensmodell von PGP verwendet. PGP verwendet als Form der Schlüsselverwaltung (oder Vermittlung) digitale Unterschriften. Wenn ein Benutzer den Schlüssel eines anderen unterzeichnet, wird er zum Schlüsselverwalter für diesen Schlüssel. Bei diesem Vorgang entsteht allmählich ein Netz bzw. ein *Web of Trust*.

In einer PGP-Umgebung kann *jeder* Benutzer als Zertifizierungsinstanz agieren. Jeder PGP-Benutzer kann also die Gültigkeit des Zertifikats für den öffentlichen Schlüssel eines anderen PGP-Benutzers bestätigen. Ein derartiges Zertifikat ist aber nur dann für den anderen Benutzer echt, wenn die überprüfende Person von der abhängigen Partei als ein autorisierter Schlüsselverwalter anerkannt wird. (Das heißt, Sie vertrauen hinsichtlich der Gültigkeit von Benutzerschlüsseln nur auf die Meinung eines autorisierten Schlüsselverwalters. Andernfalls ist diese Meinung über die Gültigkeit anderer Schlüssel nicht von Belang.)

Auf jedem öffentlichen Schlüsselbund eines Benutzers werden folgende Informationen gespeichert:

- Ob der Benutzer einen bestimmten Schlüssel als gültig betrachtet
- Die Vertrauensstufe, die der Benutzer dem Schlüssel zuordnet, d. h. die Eignung des Schlüsseleigentümers als Zertifizierungsinstanz für andere Schlüssel

Sie vermerken auf Ihrer Kopie des Schlüssels eines Benutzers, ob die Meinung dieses Schlüsseleigentümers für Sie von Belang ist. Es handelt sich also um ein System, das auf der Grundlage des guten Rufes beruht: Manche Personen haben den Ruf, vertrauenswürdige Unterschriften zu geben, daher wird ihnen vertraut, wenn sie die Gültigkeit anderer Schlüssel bestätigen.

Vertrauensstufen in PGP

Die höchste Vertrauensstufe eines Schlüssels, *implizites* Vertrauen, ist das Vertrauen in Ihr eigenes Schlüsselpaar. Bei PGP wird davon ausgegangen, daß bei Besitz eines privaten Schlüssels auch den Aktionen der zugeordneten öffentlichen Schlüssel vertraut werden muß. Alle Schlüssel, die vom Schlüssel mit dem impliziten Vertrauen unterschrieben wurden, sind echt.

Einem öffentlichen Schlüssel eines anderen Benutzers können drei Vertrauensstufen zugeordnet werden:

- *Volles* Vertrauen
- *Eingeschränktes* Vertrauen
- Kein Vertrauen (oder *Nicht vertrauenswürdig*)

Darüber hinaus gibt es drei Gültigkeitsstufen:

- Gültig
- Zweitrangig gültig
- Ungültig

So definieren Sie den Schlüssel eines anderen Benutzers als einen autorisierten Schlüsselverwalter

1. Beginnen Sie mit einem gültigen Schlüssel, der entweder
   - von Ihnen unterschrieben oder
   - von einem anderen autorisierten Schlüsselverwalter unterschrieben wurde.

   Anschließend
2. ordnen Sie dem Schlüsseleigentümer die Vertrauensstufe zu, die ihm Ihrer Ansicht nach zusteht.

Ihr Schlüsselbund enthält beispielsweise den Schlüssel von Anne. Sie haben die Gültigkeit von Annes Schlüssel mit Ihrer Unterschrift bestätigt. Sie wissen auch, daß Anne bei der Überprüfung anderer Schlüssel immer sehr sorgfältig ist. Aus diesem Grund weisen Sie ihrem Schlüssel volles Vertrauen zu. Auf diese Weise wird Alice zur Zertifizierungsinstanz. Wenn Anne nun den Schlüssel eines anderen Benutzers unterschreibt, wird dieser in Ihrem Schlüsselbund als gültig aufgenommen.

Um die Gültigkeit eines Schlüssels zu bestätigen, sind bei PGP eine Unterschrift der vollen Vertrauensstufe oder zwei Unterschriften der eingeschränkten Vertrauensstufe erforderlich. Die PGP-Methode, zwei eingeschränkt vertrauenswürdige Unterschriften mit einer voll vertrauenswürdigen Unterschrift gleichzusetzen, ähnelt dem Vorgehen eines Händlers, der zwei unterschiedliche Identitätsnachweise fordert. Sie betrachten z. B. sowohl Anne als auch Bob als nur bedingt vertrauenswürdig. Um zu verhindern, daß einer von beiden das Risiko eingeht, versehentlich einen gefälschten Schlüssel zu unterschreiben, möchten Sie keinem von beiden Ihr volles Vertrauen geben. Die Chancen, daß beide denselben gefälschten Schlüssel unterschreiben, sind dagegen ziemlich gering.

Zurücknahme von Zertifikaten

Zertifikate sind nur von Nutzen, solange sie gültig sind. Es kann nicht davon ausgegangen werden, daß ein Zertifikat unbeschränkte Gültigkeit hat. In den meisten Unternehmen und in allen PKIs ist die Lebensdauer von Zertifikaten beschränkt. Hiermit wird der Zeitraum eingeschränkt, in dem ein System für eventuell auftretende Gefährdungen der Zertifikate ausgesetzt ist.

Zertifikate werden deshalb mit einer vorher geplanten *Gültigkeitsdauer* erstellt: einem Anfangsdatum / -zeit und einem Ablaufdatum / -zeit. Es wird angenommen, daß das Zertifikat über die gesamte Gültigkeitsdauer (seine *Lebensdauer*) verwendet werden kann. Wenn das Zertifikat abläuft, ist es nicht mehr gültig, da die Echtheit des Schlüssel- / Identifikationspaar nicht länger gewährleistet ist. (Das Zertifikat kann weiterhin zur sicheren Bestätigung von innerhalb der Gültigkeitsdauer verschlüsselten oder unterschriebenen Informationen verwendet werden. Es sollte jedoch nicht für weitere Verschlüsselungen eingesetzt werden.)

Es können ebenfalls Situationen auftreten, in denen es notwendig ist, ein Zertifikat vor Ablauf der Gültigkeit ungültig zu machen. Dies ist beispielsweise der Fall, wenn die Beschäftigungsdauer eines Zertifikatseigentümers in einem Unternehmen abläuft oder vermutet wird, daß der entsprechende private Schlüssel des Zertifikats nicht mehr sicher ist. Dies wird *Zurücknahme* genannt. Ein zurückgenommenes Zertifikat ist *viel* verdächtiger als ein abgelaufenes Zertifikat. Abgelaufene Zertifikate sind nicht weiter einsetzbar, stellen jedoch nicht dieselbe Beschädigungsgefahr dar, wie ein zurückgenommenes Zertifikat.

Jeder, der ein Zertifikat unterschrieben hat, kann seine Unterschrift auf einem Zertifikat zurücknehmen (vorausgesetzt, es wird derselbe private Schlüssel verwendet wie für die Erstellung der Unterschrift). Eine zurückgenommene Unterschrift zeigt an, daß der Unterzeichner nicht mehr von der Zusammengehörigkeit des öffentlichen Schlüssels und der Identifikationsinformationen überzeugt ist, oder daß der öffentliche Schlüssel des Zertifikats (oder entsprechend der private Schlüssel) nicht mehr sicher ist. Eine zurückgenommene Unterschrift sollte dieselbe Gewichtung wie ein zurückgenommenes Zertifikat haben.

Bei einem X.509-Zertifikat hat eine zurückgenommene Unterschrift dieselbe Bedeutung wie ein zurückgenommenes Zertifikat, vorausgesetzt, es handelt sich bei der einzigen Unterschrift auf dem Zertifikat um die autorisierende Unterschrift der CA. PGP-Zertifikate bieten die Zusatzfunktion, mit der Sie das gesamte Zertifikat (nicht nur die darauf enthaltenen Unterschriften) zurücknehmen können, wenn Sie die Vermutung haben, daß das Zertifikat nicht mehr sicher ist.

Nur der Eigentümer des Zertifikats (der Inhaber des entsprechenden privaten Schlüssels) oder eine Person, den der Zertifikatseigentümer den Rücknahmeschlüssel *zugeordnet* hat, kann ein PGP-Zertifikat zurücknehmen. (Die Zuordnung eines Rücknahmeschlüssels ist ein nützlicher Vorgang, da es in vielen Fällen auf den Verlust der Paßphrase für den entsprechenden privaten Schlüssel des Zertifikats zurückzuführen ist, daß ein PGP-Benutzer sein Zertifikat zurücknimmt. Dieser Vorgang ist jedoch nur durchführbar, wenn diese Person auf den privaten Schlüssel zugreifen kann.) Nur der Zertifikatsaussteller kann ein X.509-Zertifikat zurücknehmen.

Zurückgenommenes Zertifikat bekanntgeben

Wenn ein Zertifikat zurückgenommen wurde, ist es von Bedeutung, mögliche Benutzer über die Ungültigkeit zu informieren. Bei den PGP-Zertifikaten ist die gängigste Art und Weise der Bekanntgabe eines zurückgenommenen Zertifikats, dieses auf einem Certificate Server abzulegen, so daß Dritte, die möglicherweise mit Ihnen in Kontakt treten möchten, die Warnung erhalten, diesen öffentlichen Schlüssel nicht zu verwenden.

In einer PKI-Umgebung lassen sich zurückgenommene Zertifikate am effektivsten über eine von der CA veröffentlichte Datenstruktur mit dem Namen *Liste der zurückgenommenen Zertifikate* oder *CRL* bekanntgeben. Die CRL enthält eine gültige Liste aller zurückgenommenen, nicht abgelaufenen Zertifikate im System mit Zeitmarkierungen. Zurückgenommene Zertifikate werden nur solange auf der Liste aufgeführt, bis sie ungültig werden. Anschließend werden sie alle von der Liste entfernt, damit diese nicht zu umfangreich wird.

Die CA verteilt in regelmäßigen, geplanten Abständen die CRL an Benutzer (und möglicherweise außerhalb des Zyklusses, wenn ein Zertifikat zurückgenommen wurde). So wird im Grunde verhindert, daß Benutzer unwissentlich ein unsicheres Zertifikat verwenden. Es ist möglich, daß zwischen der Ausgabe der CRLs ein vor kurzem unsicher gewordenes Zertifikat verwendet wird.

Was ist eine Paßphrase?

Die Zugriffsbeschränkung zu Computersystemen über ein *Paßwort* ist vielen Benutzern bekannt. Ein Paßwort ist dabei eine eindeutige Zeichenkette, die vom Benutzer als ein Identifizierungscode eingegeben wird.

Eine *Paßphrase* ist ein längeres Paßwort und theoretisch auch sicherer. Eine Paßphrase besteht aus mehreren Wörtern und ist damit sicherer vor standardmäßigen *Wörterbuchangriffen* geschützt, bei denen ein Hacker alle Wörter im Wörterbuch durchprobiert, um Ihr Paßwort zu bestimmen. Die sichersten Paßphrasen sind relativ lang und komplex und enthalten eine Kombination aus Klein- und Großbuchstaben, Zahl- und Interpunktionszeichen.

Bei PGP wird mit einer Paßphrase Ihr privater Schlüssel auf Ihrem Rechner verschlüsselt. Ihr privater Schlüssel wird auf Ihrer Festplatte verschlüsselt, wobei einige Zeichen Ihrer Paßphrase als geheimer Schlüssel verwendet werden. Mit der Paßphrase können Sie Ihren privaten Schlüssel entschlüsseln und verwenden. Die Paßphrase sollten Sie sich leicht merken können, für andere soll sie aber nicht einfach zu erraten sein. Sie sollten dafür eine Wendung wählen, die bereits Eingang in Ihr Langzeitgedächtnis gefunden hat, und nicht erst eine lange Wortfolge erfinden. Denn: **Wenn Sie Ihre Paßphrase vergessen sollten, können wichtige Daten eventuell nie mehr entschlüsselt werden**. Ihr privater Schlüssel ist ohne die Paßphrase absolut nutzlos und kann nicht wiederhergestellt werden. Wie bereits in diesem Kapitel erwähnt, sind Ihre Dateien mit der in PGP verwendeten Kryptographie sogar vor Eingriffen von seiten der Regierung sicher. Somit haben auch Sie ohne Ihren privaten Schlüssel keine Möglichkeit, auf Ihre Daten zuzugreifen. Ziehen Sie diesen Tatsache in Betracht, wenn Sie Ihre Paßphrase durch die Pointe eines Witzes ersetzen möchten, an den Sie sich nicht immer so ganz erinnern können.

Schlüsselaufteilung

Ein Geheimnis ist bekanntermaßen kein Geheimnis, wenn es mehr als einer Person bekannt ist. Durch die gemeinsame Nutzung eines privaten Schlüsselpaars ist ein derartiges Problem gegeben. Obwohl die gemeinsame Nutzung eines Schlüsselpaars nicht empfohlen wird, ist dies doch zuweilen unumgänglich. *Firmenweite Unterschriftenschlüssel* sind beispielsweise private Schlüssel, mit denen in einem Unternehmen Dokumente, vertrauliche private Personaldaten oder Presseveröffentlichungen unterschrieben werden, um deren Herkunft zu bestätigen. In diesem Fall ist es nützlich, wenn mehrere Mitarbeiter des Unternehmens Zugriff auf einen privaten Schlüssel haben. Dies bedeutet aber auch, daß ein Einzelner im Namen des Unternehmens unbeschränkt agieren kann.

Daher ist es empfehlenswert, einen Schlüssel zwischen mehreren Personen so aufzu *teilen*, daß immer mehr als eine oder zwei Personen einen Teil des Schlüssels vorlegen müssen, um diesen wieder zu einem wirksamen Schlüssel zusammensetzen zu können. Wenn nicht genügend Schlüsselteile verfügbar sind, bleibt der Schlüssel unwirksam.

So kann ein Schlüssel beispielsweise in drei Teile aufgeteilt und mit zwei Teilen wiederhergestellt oder in zwei Teile aufgeteilt und mit beiden wiederhergestellt werden. Wenn zur Wiederherstellung eine sichere Netzwerkverbindung verwendet wird, müssen die Halter des Schlüssels zur Zusammensetzung des Schlüssels physisch anwesend sein.

Technische Daten

In diesem Kapitel wurde eine anspruchsvolle und umfassende Einführung in die Kryptographie und in die zugehörige Terminologie gegeben. In Kapitel 2 finden Sie eine von Phil Zimmermann, dem Entwickler von PGP, verfaßte tiefergehende Diskussion zur Geheimhaltung und Privatsphäre, der technischen Informationen zur Funktionsweise von PGP, einschließlich einer Erläuterung der verschiedenen in PGP verwendeten Algorithmen, und der verschiedenen Angriffsarten und möglichen Schutzmaßnahmen.

Weitere Informationen zur Kryptographie finden Sie in einigen der im Abschnitt „Weitere Publikationen zum Thema“ im Vorwort aufgeführten Bücher.

Phil Zimmermann über PGP 2

Dieses Kapitel enthält eine Einführung und Hintergrundinformationen zur Kryptographie und zu PGP, verfaßt von Phil Zimmermann.

Weshalb ich PGP entwickelt habe

„Was auch immer du tust, ist nicht von Bedeutung. Aber es ist sehr wichtig, daß du es tust.“
—Mahatma Gandhi.

Es ist persönlich. Es ist vertraulich. Und außer Sie geht es niemanden etwas an. Unter Umständen bereiten Sie derzeit eine politische Kampagne vor, sprechen über Ihre Steuerangelegenheiten oder haben eine geheime Liebesaffäre. Oder aber Sie stehen mit einem politischen Dissidenten in einem autoritären Staat in Kontakt. Worum es sich auch handeln mag, Sie möchten sicherlich nicht, daß eine dritte Person Ihre elektronische Post (E-Mail) oder Ihre vertraulichen Dokumente liest. Es ist völlig normal, daß Sie Ihre Privatsphäre bewahren möchten. Die Wahrung der Privatsphäre ist genauso selbstverständlich wie die amerikanische Verfassung.

Das Recht auf Privatsphäre ist implizit durchgehend in den verfassungsmäßig garantierten Grundrechten der Vereinigten Staaten, der Bill of Rights, enthalten. Aber als die amerikanische Verfassung aufgesetzt wurde, sahen die Gründerväter keine Notwendigkeit, das Recht auf private Kommunikation ausdrücklich festzuschreiben. Dafür gab es ja damals auch noch keinen Grund. Schließlich waren vor zweihundert Jahren alle Unterhaltungen privat. Wenn sich eine andere Person näherte, ist man eben einfach hinter die nächste Scheune gegangen und hat das Gespräch dort fortgesetzt. Es war unmöglich, fremde Gespräche heimlich zu belauschen. Das Recht auf private Unterhaltung war ein natürliches Recht, und zwar nicht nur im philosophischen Sinne, sondern sozusagen als physikalisches Gesetz aufgrund des damaligen Standes der Technik.

Dies jedoch sollte sich mit dem Beginn des Informationszeitalters, das durch die Erfindung des Telefons eingeläutet wurde, schlagartig ändern. Heutzutage werden die meisten Unterhaltungen unter Nutzung elektronischer Medien geführt. Damit sind all unsere Unterhaltungen, auch die noch so privaten, fremden Personen ohne unser Wissen zugänglich. Mobiltelefone können von jedermann mit einem Funkgerät abgehört werden. Viel sicherer als über Mobiltelefone geführte Gespräche sind auch die via Internet übermittelten E-Mail-Nachrichten nicht. E-Mail-Nachrichten laufen den herkömmlichen, per Post versandten Briefen zunehmend den Rang ab. Sie werden immer

selbstverständlicher und sind längst nicht mehr so außergewöhnlich wie noch vor wenigen Jahren. E-Mail-Nachrichten können jedoch von interessierten Dritten regelmäßig und auf automatische Weise nach beliebigen Schlüsselwörtern durchsucht werden – auf breit angelegter Basis und ohne Nachweismöglichkeit. Dies ist vergleichbar mit dem Treibnetzfischen.

Möglicherweise sind Sie der Meinung, daß der Inhalt Ihrer E-Mail-Nachricht legitim genug ist und eine Verschlüsselung ungerechtfertigt wäre. Doch wenn Sie wirklich ein gesetzestreuer Bürger sind, der nichts zu verbergen hat – warum verschicken Sie Ihre herkömmliche Post dann nicht immer in Form von Postkarten? Warum fänden Sie es nicht in Ordnung, wenn sich jedermann auf Verlangen einem Drogentest unterziehen müßte? Warum würden Sie bei einer Hausdurchsuchung durch die Polizei einen Durchsuchungsbefehl verlangen? Haben Sie vielleicht etwas zu verbergen? Ist die Tatsache, daß Sie Ihre Post in Briefumschlägen verbergen, ein Zeichen dafür, daß Sie subversive Absichten haben, ein Drogenhändler sind oder unter Verfolgungswahn leiden? Haben Bürger, die die Gesetze befolgen, irgendeinen Grund, ihre E-Mail-Nachrichten zu verschlüsseln?

Was wäre, wenn die allgemeine Ansicht bestünde, daß gesetzestreue Bürger ausschließlich Postkarten für ihre Post verwenden müßten? Wenn ein Mensch, der diese allgemeine Ansicht nicht teilt, zum Schutz seiner Privatsphäre einen Umschlag für seine Post verwenden würde, würde er Verdacht auf sich ziehen. Die Behörden würden möglicherweise die Post öffnen, um herauszufinden, was diese Person verbirgt. Glücklicherweise ist dies nicht die Realität, da die meisten Briefe durch Briefumschläge geschützt werden. Und niemand, der Briefumschläge zum Schutz seiner Privatsphäre verwendet, macht sich dadurch verdächtig. Mit dem, was alle machen, liegt man am sichersten. Im gleichen Maße wäre es gut, wenn jeder seine E-Mails verschlüsseln würde, unabhängig davon, ob schuldig oder unschuldig, so daß keiner sich durch Verschlüsselung von E-Mails zum Schutze seiner Privatsphäre verdächtig machen würde. Betrachten Sie es einfach als eine Form von Solidarität.

Bis jetzt mußte die Regierung, wenn sie in die Privatsphäre eines normalen Bürgers eindringen wollte, eine bestimmte Menge an Geld und Arbeit investieren, um Briefpost abzufangen, den Umschlag mit Wasserdampf zu öffnen und den Brief zu lesen. Bei telefonischer Kommunikation mußten Telefongespräche abgehört und möglicherweise transkribiert werden, zumindest bevor automatische Spracherkennung verfügbar wurde. Solche arbeitsaufwendigen Überwachungsmaßnahmen waren in einem großen Maßstab nicht zweckmäßig. Sie wurden lediglich in wichtigen Fällen durchgeführt, für die sich der Aufwand zu lohnen schien.

Die „Senate Bill 266“, eine 1991 eingebrachte, allgemeine Gesetzesvorlage zur Verbrechensbekämpfung, sah einen beunruhigenden Handlungsspielraum vor. Wenn dieser nicht bindende Beschluß zum Gesetz geworden wäre, wären Hersteller von sicheren Kommunikationsanlagen gezwungen worden, spezielle „Zugangstüren“ in ihre Produkte einzubauen. Auf diese Weise hätte die Regierung verschlüsselte Nachrichten von beliebigen Personen lesen können. Die Gesetzesvorlage drückt die Auffassung des Kongresses aus, daß Firmen, die elektronische Kommunikationsdienste anbieten, und Firmen, die Anlagen für elektronische Kommunikationsdienste herstellen, sicherstellen sollen, daß die Kommunikationssysteme der Regierung die Möglichkeit eröffnen, auf die Klartextinhalte von Sprach- und anderen Daten sowie auf sonstige übertragene Informationen zuzugreifen, wenn die entsprechende gesetzliche Grundlage dafür besteht. Dieser Beschluß gab den Ausschlag für mich, PGP im selben Jahr auf elektronischem Wege kostenfrei zugänglich zu machen, kurz bevor die Maßnahme nach heftigem Protest durch Bürgerrechtsvereinigungen und Vertreter der Industrie abgewendet wurde.

Die Gesetzesvorlage bezüglich digitaler Telefone von 1994 (Digital Telephony Bill) sah vor, daß Telefongesellschaften in die digitalen Schalter ihrer Zentrale fernbedienbare Abhöranschlüsse einbauen sollten, um so eine neue technische Infrastruktur zum Abhören per Mausklick zu schaffen. Dadurch müssen die zuständigen Staatsbediensteten nicht einmal mehr ihr Büro verlassen und vor Ort Krokodilklemmen an Telefonleitungen installieren. Stattdessen können sie nun in ihrem Hauptsitz in Washington bleiben und nach Belieben Ihren Telefongesprächen zuhören. Selbstverständlich ist nach diesem Gesetz immer noch eine gerichtliche Verfügung zur Abhörung eines Gesprächs erforderlich. Doch während eine technische Infrastruktur mehrere Generationen lang bestehen kann, können Gesetze und Richtlinien sich über Nacht ändern. Wenn sich eine Kommunikationsinfrastruktur, die für Überwachungszwecke optimiert wurde, etabliert, kann ein Wechsel der politischen Gegebenheiten zu einem Mißbrauch dieses neu geschaffenen Machtmittels führen. Politische Verhältnisse können sich durch die Wahl einer neuen Regierung ändern, aber unter Umständen auch ganz plötzlich, beispielsweise durch die Bombardierung eines Bundesgebäudes.

Ein Jahr, nachdem die Digital Telephony Bill von 1994 verabschiedet wurde, enthüllte das FBI Pläne, nach denen die Telefongesellschaften verpflichtet werden sollten, in ihrer Infrastruktur die Möglichkeit zu schaffen, 1 Prozent aller Telefongespräche in den größten amerikanischen Städten zur gleichen Zeit abzuhören. Dies würde im Vergleich zur vorherigen Situation die Anzahl der abhörbaren Telefone vertausendfachen. Vor 1994 wurden lediglich ungefähr tausend gerichtliche Abhörverfügungen pro Jahr in den USA ausgestellt, alle Verfügungen auf Bundes-, Staats- und lokaler Ebene zusammengenommen. Es ist schwer vorstellbar, wie die Regierung auch nur genug Richter einstellen könnte, um genügend gerichtliche Abhörverfügungen für 1 Prozent sämtlicher in den USA geführten Telefongespräche unterzeichnen zu können, und es ist noch weniger vorstellbar, wie genügend Bundesbeamte eingestellt

werden könnten, um alle Gespräche in Echtzeit abzuhören. Die einzig plausible Erklärung zur Verarbeitung dieser Gesprächsmengen wäre die Verwendung einer automatisierten Spracherkennungstechnologie in Orwellschen Dimensionen, um alle Gespräche zu „durchsieben“ und nach interessanten Schlüsselwörtern oder nach der Stimme eines bestimmten Sprechers zu suchen. Falls die Regierung im ersten 1-Prozent-Anteil der Telefongespräche nicht findet, was sie sucht, können die Abhörmaßnahmen auf einen anderen 1-Prozent-Anteil gerichtet werden, bis das Gesuchte gefunden wird – oder bis die Telefonleitungen aller Personen auf subversive Gespräche hin überprüft worden sind. Laut FBI wird diese Kapazität benötigt, damit sich auf künftige Gegebenheiten eingestellt werden könne. Dieses Vorhaben führte zu einer solchen Entrüstung, daß es im Kongreß nicht angenommen wurde – zumindest in diesem Fall, im Jahre 1995. Doch die bloße Tatsache, daß das FBI um die Einräumung dieser enormen Machtmittel gebeten hat, sagt einiges über seine Absichten aus. Die Ablehnung des Plans stimmt auch nicht ausschließlich positiv, wenn Sie daran denken, daß die Digital Telephony Bill von 1994 auch beim ersten Antrag im Jahre 1993 abgelehnt wurde.

Der technische Fortschritt erschwert die Aufrechterhaltung des privaten Status Quo. Dieser Zustand ist alles andere als stabil. Wenn wir nichts unternehmen, werden der Regierung durch neue Technologien neue Möglichkeiten der automatisierten Überwachung eröffnet, von denen Stalin nur träumen konnte. Der einzige Weg, die Privatsphäre auch im Informationszeitalter zu schützen, ist die Verwendung einer effizienten Kryptographie.

Sie müssen nicht unbedingt der Regierung mißtrauen, um Kryptographie verwenden zu wollen. Ihr Unternehmen kann von Konkurrenzfirmen, dem organisierten Verbrechen oder ausländischen Regierungen abgehört werden. Mehrere ausländische Regierungen sind beispielsweise dafür bekannt, daß sie das Signalerkennungssystem ihres Nachrichtendienstes gegen Unternehmen aus anderen Ländern einsetzt, um ihren eigenen Firmen einen Wettbewerbsvorteil zu verschaffen. Ironischerweise haben die Beschränkungen der US-Regierung im Hinblick auf die Kryptographie die Schutzmöglichkeiten amerikanischer Firmen gegenüber ausländischen Geheimdiensten und dem organisierten Verbrechen untergraben.

Die Regierung ist sich der zentralen Rolle bewußt, die die Kryptographie im Machtverhältnis gegenüber der Bevölkerung spielen wird. Im April 1993 gab die Clinton-Regierung eine neue politische Initiative zum Thema Verschlüsselung bekannt, die der Nationale Sicherheitsdienst (NSA) seit Beginn der Amtszeit von Präsident Bush entwickelt hatte. Das Kernstück dieser Initiative besteht aus einem von der Regierung hergestellten Verschlüsselungsgerät, dem „Clipper-Chip“, der einen neu klassifizierten NSA-Verschlüsselungsalgorithmus enthält. Die Regierung versuchte, die Privatindustrie zu ermutigen, diesen Clip in all ihre Geräte zur abhörgeschützten Kommunikation zu integrieren, wie beispielsweise abhörgeschützte Telefone, abhörgeschützte Faxgeräte usw. AT&T integrierte den Clipper-Chip in seine abhörgeschützten

Sprachprodukte. Der Haken an der Sache: Bei der Herstellung wird jeder Clipper-Chip mit einem eigenen, eindeutigen Schlüssel geladen, und die Regierung erhält eine Kopie dieses Schlüssels, die hinterlegt wird. Es besteht jedoch kein Grund zur Beunruhigung: Die Regierung verspricht, diese Schlüssel nur zum Abhören zu verwenden, wenn sie dazu „durch ein Gesetz ordnungsgemäß ermächtigt“ ist. Der nächste logische Schritt zur vollständig effektiven Verwendung des Clipper-Chips bestünde dann natürlich im Verbot anderer Formen von Kryptographie.

Die Regierung wies anfangs darauf hin, daß der Gebrauch des Clipper-Chips nicht vorgeschrieben sei, und daß niemand gezwungen würde, diese Technologie anstelle anderer Formen von Kryptographie zu verwenden. Aber die öffentliche Reaktion auf den Clipper-Chip war stark, stärker, als von der Regierung erwartet. Die Computer-Industrie sprach sich einheitlich gegen die Verwendung des Clipper-Chip aus. FBI-Direktor Louis Freeh antwortete 1994 auf eine Frage in einer Pressekonferenz, daß im Falle einer Nichtakzeptanz des Clipper-Chip durch die Öffentlichkeit und dem Umgehen von FBI-Abhöreinrichtungen durch nicht von der Regierung kontrollierte Kryptographie seiner Behörde nur der Ausweg einer Rechtsklage bliebe. Später, nach der Tragödie von Oklahoma City, sagte Louis Freeh vor dem Rechtskomitee des Senats aus, daß der Zugang der Öffentlichkeit zu einer effizienten Kryptographie durch die Regierung eingeschränkt werden müsse (obwohl niemand die Vermutung ausgesprochen hatte, daß die Bombenleger Kryptographie verwendet hätten).

Das Informationszentrum zum Schutz der Privatsphäre in elektronischen Medien (EPIC) gelangte in den Besitz einiger aufschlußreicher Dokumente, die unter das Gesetz zur Wahrung des Rechts auf Auskunft (Freedom of Information Act) fallen. In einem Informationsdokument über die Bedrohung, Anwendungen und mögliche Lösungen des Phänomens Verschlüsselung (Originaltitel: „Encryption: The Threat, Applications and Potential Solutions“), das im Februar 1993 an den Nationalen Sicherheitsrat geschickt worden war, kamen das FBI, der NSA und das Justizministerium zu dem Schluß, daß „bestehende technische Lösungen nur funktionieren werden, wenn sie in alle Verschlüsselungsprodukte integriert werden“. Um dies sicherzustellen, müsse durch die Gesetzgebung die Verwendung von staatlich genehmigten Verschlüsselungsprodukten oder die Befolgung von staatlich vorgegebenen Verschlüsselungskriterien vorgeschrieben werden.

Die politische Vergangenheit stärkt nicht gerade das Vertrauen der Bevölkerung darauf, daß ein Mißbrauch von Bürgerrechten seitens der Regierung absolut ausgeschlossen ist. Das COINTELPRO-Programm des FBI war gegen Gruppen gerichtet, die die Regierungspolitik ablehnten. Die Anti-Kriegs-Bewegung und die Bürgerrechtsbewegung wurden bespitzelt. Das Telefon von Martin Luther King Jr. wurde abgehört. Nixon hatte eine

„Feindliste“. Nicht zu vergessen die Watergate-Affäre. Der Kongreß ist nun offenbar bestrebt, Gesetze zu verabschieden, die die Bürgerrechte im Medium Internet einschränken. Zu keiner Zeit im vergangenen Jahrhundert war ein Mißtrauen gegenüber der Öffentlichkeit von seiten der Regierung so weit über das gesamte politische Spektrum verteilt wie heutzutage.

Wenn wir uns dem beunruhigenden Trend der Regierung widersetzen möchten, Kryptographie gesetzlich zu verbieten, besteht eine Möglichkeit des Widerstands darin, Kryptographie so intensiv wie möglich zu verwenden, solange es noch legal ist. Je stärker sich die Verwendung von effizienter Kryptographie verbreitet, desto schwieriger wird es für die Regierung, die Verwendung unter Strafe zu stellen. Aus diesem Grund trägt die Verwendung von PGP zum Erhalt der Demokratie bei.

Wenn Privatsphäre nicht mehr legal ist, ist die Privatsphäre den Gesetzesbrechern vorbehalten. Geheimdienste haben Zugang zu guten Verschlüsselungstechniken. Dies trifft ebenfalls auf große Waffen- und Drogenhändler zu. Aber die allgemeine Bevölkerung und politische Basisorganisationen hatten normalerweise keinen Zugang zu Kryptographietechniken mit öffentlichen Schlüsseln, die erschwinglich und zugleich so sicher wie die für militärische Zwecke verwendeten Verschlüsselungsmethoden waren. Bis jetzt.

PGP ist ein Instrument, mit dem Menschen den Schutz ihrer Privatsphäre in die eigene Hand nehmen können. In unserer Gesellschaft besteht dafür ein wachsendes Bedürfnis. Deshalb habe ich PGP entwickelt.

Die symmetrischen Algorithmen von PGP

PGP verfügt über verschiedene Geheimschlüsselalgorithmen zur Verschlüsselung der eigentlichen Nachricht. Als Geheimschlüsselalgorithmus bezeichnet man eine konventionelle oder symmetrische Blockchiffre, die denselben Schlüssel zum Ver- und zum Entschlüsseln verwendet. Bei den drei symmetrischen, von PGP angebotenen Blockchiffren handelt es sich um CAST, Triple-DES und IDEA. Diese Algorithmen entsprechen den höchsten professionellen Anforderungen und wurden von renommierten Kryptographen-Teams entwickelt.

Für diejenigen, die sich näher für Kryptographie interessieren, sei angemerkt, daß alle drei Chiffren auf der Basis von 64-Bit-Blöcken von Klar- und chiffriertem Text funktionieren. CAST und IDEA verfügen über Schlüsselgrößen von 128 Bit, während Triple-DES einen 168-Bit-Schlüssel verwendet. Wie der Data Encryption Standard (DES), können alle drei Verschlüsselungsarten in den Modi Cipher Feedback ((CFB) oder Cipher Block Chaining (CBC) verwendet werden. Sie werden von PGP im 64-Bit-CFB-Modus verwendet.

Der CAST-Verschlüsselungsalgorithmus wurde in PGP aufgenommen, da es sich dabei um einen vielversprechenden, sehr schnellen und kostenfreien 128-Bit-Blockchiffrierer handelt. Der Name dieses Algorithmus wurde aus den Anfangsbuchstaben seiner Entwickler abgeleitet, Carlisle Adams und Stafford Tavares von Northern Telecom (Nortel). Nortel hat zwar ein Patent für CAST angemeldet, die Firma hat jedoch schriftlich zugesichert, CAST jedem ohne Lizenzgebühren zur Verfügung zu stellen. CAST ist ein hervorragend entwickelter Algorithmus, der von Personen mit einem guten Namen in diesem Bereich entwickelt wurde. Die Entwicklung basiert auf einem sehr formalen Ansatz, mit einigen formal nachweisbaren Hypothesen. Daraus ergeben sich gute Gründe für die Annahme, daß der 128-Bit-Schlüssel dieses Algorithmus mit den gegenwärtig bekannten Verfahren nicht entschlüsselt werden kann. CAST hat keine ineffizienten oder halb-effizienten Schlüssel. Es sprechen viele Argumente dafür, daß CAST immun gegen lineare und differentiale Kryptoanalyse ist. Diese Methoden werden in der Fachliteratur allgemein als die leistungsfähigsten Kryptoanalyseformen dargestellt, und waren gleich leistungsstark im Dekodieren von DES (Data Encryption Standard). CAST ist noch zu neu, um anhand konkreter Ergebnisse beurteilt werden zu können, aber seine formale Gestaltung und der gute Ruf seiner Entwickler werden sicherlich die Aufmerksamkeit sowie kryptoanalytische Angriffe des Rests der akademischen kryptographischen Gemeinschaft auf sich ziehen. Ich habe fast das gleiche gute Gefühl und Vertrauen in CAST, wie ich es vor Jahren für IDEA hatte, den Chiffriercode, den ich für frühere PGP-Versionen ausgewählt hatte. Zu dieser Zeit war IDEA auch noch nicht längerfristig erprobt, aber es hat die Erwartungen nicht enttäuscht.

Die Blockchiffre IDEA (International Data Encryption Algorithm; internationaler Datenverschlüsselungsalgorithmus) basiert auf dem Entwicklungskonzept, Vorgänge von verschiedenen algebraischen Gruppen zu mischen. Der Algorithmus wurde von James L. Massey und Xuejia Lai an der ETH in Zürich entwickelt und 1990 veröffentlicht. In früheren Veröffentlichungen über den Algorithmus wurde er als IPES (Improved Proposed Encryption Standard; verbesserter, vorgeschlagener Verschlüsselungsstandard) bezeichnet, der Name wurde später jedoch in IDEA geändert. Bis heute hat IDEA Angriffen wesentlich besser widerstanden als andere Chiffren (beispielsweise FEAL, REDOC-II, LOKI, Snefru und Khafre). Darüber hinaus widersteht IDEA den höchst erfolgreichen differential-kryptoanalytischen Angriffen von Biham und Shamir sowie Attacken durch lineare Kryptoanalyse besser als DES. Da weiterhin viele Kryptoanalyse-Spezialisten vergeblich versuchen, IDEA zu dekodieren, wächst das Vertrauen in IDEA mit der Zeit immer mehr. Leider war das größte Hindernis für die Akzeptanz von IDEA als Standard die Tatsache, daß Ascom Systec ein Patent auf seine Entwicklung hat und IDEA im Gegensatz zu DES und CAST nicht allgemein kostenfrei zur Verfügung gestellt wurde.

Als Schutz enthält PGP im Repertoire seiner Blockchiffren Drei-Schlüssel-Triple-DES. DES wurde von IBM Mitte der 70er Jahre entwickelt. Obwohl er gut entwickelt ist, ist die Schlüsselgröße von 56 Bit für heutige Standards zu gering. Triple-DES ist sehr effizient und wurde mehrere Jahre lang ausführlich untersucht. Er könnte also eine sicherere Chiffre sein als die neueren Chiffren CAST und IDEA. Triple-DES bedeutet, daß DES dreimal auf den gleichen Datenblock angewandt wird. Dabei werden drei verschiedene Schlüssel verwendet; der zweite DES-Vorgang wird rückwärts, im Entschlüsselungsmodus, durchgeführt. Triple-DES ist zwar deutlich langsamer als CAST oder IDEA, jedoch ist die Geschwindigkeit für E-Mail-Anwendungen normalerweise nicht von großer Bedeutung. Obwohl Triple-DES eine Schlüsselgröße von 168 Bit verwendet, scheint es über eine effektive Schlüsselstärke von mindestens 112 Bit bei Angriffen mit einer äußerst großen Datenspeicherungskapazität zu verfügen. Gemäß einer Veröffentlichung von Michael Weiner auf der Crypto96 würde eine auch nur annähernd ausreichende Datenspeicherungsmöglichkeit dem Hacker einen Angriff ermöglichen, der ebensoviel Aufwand wie das Aufbrechen eines 129-Bit-Schlüssels erfordern würde. Die Verwendung von Triple-DES wird durch keinerlei Patente beschränkt.

Die öffentlichen Schlüssel, die mit PGP Version 5.0 oder höher erzeugt werden, enthalten eingebettete Daten, die dem Absender mitteilen, welche Blockchiffren von der Empfängersoftware verstanden werden, so daß die Software des Absenders „weiß“, welche Chiffriercodes zum Verschlüsseln verwendet werden können. Die öffentlichen Diffie-Hellman / DSS-Schlüssel akzeptieren CAST, IDEA oder Triple-DES als Blockchiffre, mit CAST als Standardeinstellung. Zur Zeit bieten RSA-Schlüssel aus Kompatibilitätsgründen diese Funktion nicht an. Zum Senden von Nachrichten an RSA-Schlüssel wird von PGP nur die IDEA-Verschlüsselung verwendet, da ältere PGP-Versionen nur RSA und IDEA unterstützen.

PGP-Datenkomprimierungsroutinen

PGP komprimiert normalerweise den Klartext vor der Verschlüsselung, da der Klartext nach der Verschlüsselung nicht mehr komprimiert werden kann; verschlüsselte Daten können nicht komprimiert werden. Durch Datenkomprimierung wird die Übertragungszeit bei Modemübertragungen verringert sowie Platz auf der Festplatte gespart und, was wichtiger ist, die kryptographische Sicherheit gesteigert. Die meisten kryptoanalytischen Verfahren nutzen im Klartext gefundene Wiederholungen zum Decodieren der Chiffre. Durch Datenkomprimierung wird diese Redundanz im Klartext reduziert, wodurch der Schutz vor kryptoanalytischen Angriffen deutlich vergrößert wird. Die Komprimierung des Klartextes bedeutet einen zusätzlichen Zeitaufwand, doch vom Sicherheitsstandpunkt aus gesehen lohnt sich der Aufwand.

Dateien, die zum Komprimieren zu kurz sind oder die nicht gut komprimiert werden können, werden von PGP nicht komprimiert. Außerdem erkennt das Programm Dateien, die mit den meisten bekannten Komprimierungsprogrammen erstellt wurden, wie beispielsweise PKZIP, und versucht nicht, Dateien zu komprimieren, die bereits komprimiert worden sind.

Zur Information für die technisch Interessierten sei angemerkt, daß das Programm die Freeware-ZIP-Komprimierungsroutinen verwendet, die von Jean-Loup Gailly, Mark Adler und Richard B. Wales geschrieben wurden. Diese ZIP-Software verwendet Komprimierungsalgorithmen, die in ihrer Funktionsweise den von PKZIP 2.x von PKWare verwendeten Algorithmen entsprechen. Diese ZIP-Komprimierungssoftware wurde für PGP hauptsächlich aufgrund des guten Komprimierungsverhältnisses und aufgrund ihrer Schnelligkeit ausgewählt.

Als Sitzungsschlüssel verwendete Zufallszahlen

PGP verwendet zur Erstellung von temporären Sitzungsschlüsseln einen kryptographisch leistungsfähigen Generator für Pseudo-Zufallswerte. Wenn diese Datei mit Zufallswerten nicht existiert, wird sie automatisch erstellt und mit echten Zufallswerten aufgefüllt. Diese Zufallswerte werden durch das PGP-Programm aus Zufallsereignissen auf der Grundlage der zeitlichen Koordination von Tastaturbetätigungen und Mausbewegungen abgeleitet.

Dieser Generator füllt die Zufallswertedatei bei jeder Verwendung mit neuen Zufallswerten auf. Dabei wird neues Datenmaterial, das teilweise von der Tageszeit oder anderen echten Zufallsquellen abgeleitet wurde, hinzugefügt und mit den alten Daten vermischt. Der konventionelle Verschlüsselungsalgorithmus wird dabei als Motor für den Zufallswertegenerator verwendet. Die Datei mit den Zufallswerten enthält sowohl Zufallsdatenmaterial als auch Zufallsverschlüsselungsmaterial, das zur Verschlüsselung des konventionellen Verschlüsselungsmotors für den Zufallsgenerator verwendet wird.

Diese Zufallswertedatei sollte besonders geschützt werden, um das Risiko zu verringern, daß ein Hacker Ihre nächsten oder zuvor verwendeten Sitzungsschlüssel aus ihr ableiten kann. Der Hacker hätte zwar sehr viel Mühe, nützliche Informationen aus dieser Datei mit Zufallswerten zu ziehen, da die Datei vor und nach jeder Verwendung kryptographisch „gereinigt“ wird. Dennoch ist es sinnvoll, sie vor unbefugtem Zugriff zu schützen. Stellen Sie nach Möglichkeit sicher, daß nur Sie diese Datei lesen können. Falls dies nicht möglich ist, lassen Sie andere Personen nicht beliebig Dateien von Ihrem Computer kopieren.

Nachrichtenkern

Der Nachrichtenkern ist die kompakte „Essenz“ von 160 oder 128 Bit Größe Ihrer Nachricht oder eine Dateiprüfsumme. Sie können ihn sich als „Fingerabdruck“ der Nachricht oder der Datei vorstellen. Der Nachrichtenkern „repräsentiert“ Ihre E-Mail-Nachricht. Wenn die Nachricht in irgendeiner Form verändert wird, ändert sich auch der aus ihr berechnete Nachrichtenkern. Dadurch können alle von einem Fälscher an der Nachricht vorgenommenen Änderungen aufgedeckt werden. Der Nachrichtenkern wird mit Hilfe einer kryptographisch leistungsfähigen, einseitigen Hash-Funktion der Nachricht berechnet. Für einen Hacker sollte es rechnerisch unmöglich sein, eine Ersatznachricht zu erstellen, die einen identischen Nachrichtenkern erzeugen würde. In dieser Hinsicht ist ein Nachrichtenkern sehr viel besser als eine Prüfsumme, da es einfach ist, eine Nachricht it anderem Inhalt zu erstellen, die dieselbe Prüfsumme erzeugt. Wie bei einer Prüfsumme können Sie die Originalnachricht jedoch nicht von ihrem Nachrichtenkern herleiten.

Der derzeit in PGP (Version 5.0 oder höher) verwendete Nachrichtenkernalgorithmus wird SHA (Secure Hash Algorithmus; Sicherer Hash-Algorithmus) genannt. Er wurde vom NSA für das nationale Institut für Standards und Technologie (National Institute of Standards and Technology; NIST) entwikkelt. SHA ist ein 160-Bit-Hash-Algorithmus. Es mag Personen geben, die dem nationalen Sicherheitsdienst NSA skeptisch gegenüberstehen, da der NSA auf das Abhören von Gesprächen und Entschlüsseln von Codes spezialisiert ist. Bedenken Sie jedoch, daß der NSA kein Interesse am Fälschen von Unterschriften hat, und daß die Regierung von einem nicht zu fälschenden Unterschriftenstandard profitieren würde, der verhindert, daß jemand seine Unterschrift zurückweist. Dies hat verschiedene Vorteile für die Strafverfolgung und das Sammeln von Beweisen. Der Algorithmus wurde außerdem in der gängigen Literatur veröffentlicht und von vielen der weltweit besten Kryptologen, die sich auf Hash-Funktionen spezialisiert haben, genauestens überprüft. Es besteht die allgemeine Meinung, daß SHA ausgesprochen gut entwickelt ist. Der Algorithmus verfügt über einige Verbesserungen in der Entwicklung, mit denen alle in Nachrichtenkernalgorithmen beobachteten Schwächen, die von Kryptologen bislang entdeckt wurden, behoben werden. Alle neuen PGP-Versionen verwenden SHA als Nachrichtenkernalgorithmus, um Unterschriften mit den neuen DSS-Schlüsseln zu erstellen, die dem digitalen Standard für Unterschriften NIST entsprechen. Aus Kompatibilitätsgründen wird in neuen PGP-Versionen immer noch MD5 für RSA-Unterschriften verwendet, da MD5 bereits in älteren PGP-Versionen für RSA-Unterschriften verwendet wurde.

Der von älteren PGP-Versionen verwendete Nachrichtenkernalgorithmus ist der MD5-Nachrichtenkernalgorithmus, der durch RSA Data Security frei zugänglich gemacht wurde. MD5 ist ein 128-Bit-Hash-Algorithmus. 1996 wäre es dem deutschen Kryptologen Hans Dobbertin fast gelungen, MD5 zu entschlüsseln. Obwohl MD5 zu diesem Zeitpunkt noch nicht vollständig entschlüsselt wurde, wurden doch so ernsthafte Schwächen festgestellt, daß es nicht mehr zur Erzeugung von Unterschriften verwendet werden sollte. Weitere Anstrengungen auf diesem Gebiet könnten dazu führen, daß der Algorithmus vollständig entschlüsselt wird und Unterschriften somit gefälscht werden könnten. Wenn Sie nicht eines Tages Ihre digitale PGP-Unterschrift auf einem gefälschten Geständnis finden möchten, sind Sie am besten beraten, wenn Sie die neuen PGP-DSS-Schlüssel in Zukunft bevorzugt zum Erstellen von digitalen Unterschriften verwenden, da DSS SHA als sicheren Hash-Algorithmus verwendet.

So schützen Sie öffentliche Schlüssel vor Manipulation

In einem Verschlüsselungssystem mit öffentlichen Schlüsseln brauchen Sie öffentliche Schlüssel nicht nach außen zu schützen. Es ist sogar besser, sie so weit wie möglich zu verbreiten. Es ist jedoch wichtig, öffentliche Schlüssel vor Manipulation zu schützen. Nur so können Sie sicherstellen, daß ein öffentlicher Schlüssel tatsächlich der Person gehört, zu der er zu gehören scheint. Dies ist wahrscheinlich die größte potentielle Schwachstelle in einem Kryptosystem mit öffentlichen Schlüsseln. Im folgenden wird zuerst eine Situation beschrieben, die im schlimmsten Fall eintreten könnte, und dann erläutert, wie Sie solch eine Katastrophe mit PGP sicher verhindern können.

Angenommen, Sie möchten an eine Person namens Susanne eine private Nachricht senden. Sie laden das öffentliche Schlüsselzertifikat von Susanne von einem elektronischen BBS (Bulletin Board System), d. h. einer Mailbox, herunter. Sie verschlüsseln Ihre Nachricht an Susanne mit diesem öffentlichen Schlüssel und senden ihn über die E-Mail-Funktion der Mailbox an sie.

Unglücklicherweise ist, ohne Ihr oder Susannes Wissen, ein anderer Benutzer in die Mailbox eingedrungen, den wir Rainer nennen. Rainer hat einen eigenen öffentlichen Schlüssel erzeugt und die Benutzer-ID von Susanne mit diesem öffentlichen Schlüssel verknüpft. Er hat heimlich den echten öffentlichen Schlüssel von Susanne durch seinen unechten Schlüssel ersetzt. Sie benutzen nun unwissentlich diesen unechten Schlüssel von Rainer anstatt Susannes öffentlichen Schlüssel. Diese Situation bleibt unbemerkt, da der unechte Schlüssel die Benutzer-ID von Susanne hat. Rainer kann nun die für Susanne bestimmte Nachricht dechiffrieren, da er über den passenden privaten Schlüssel verfügt. Er könnte sogar die dechiffrierte Nachricht mit dem

echten öffentlichen Schlüssel von Susanne wieder verschlüsseln und sie an Susanne schicken, so daß kein Verdacht entsteht. Zudem kann er mit diesem privaten Schlüssel scheinbar gültige Unterschriften von Susanne erzeugen, da alle den unechten Schlüssel zur Überprüfung von Susannes Unterschrift verwenden.

Sie können dies nur verhindern, indem Sie öffentliche Schlüssel vor jeglicher Manipulation schützen. Wenn Sie den öffentlichen Schlüssel von Susanne direkt von Susanne erhalten, besteht keinerlei Problem. Dies könnte jedoch mit Schwierigkeiten verbunden sein, wenn Susanne tausende von Kilometern entfernt wohnt oder zur Zeit nicht erreichbar ist.

Möglicherweise können Sie den öffentlichen Schlüssel von Susanne über einen gemeinsamen Freund, Claus, erhalten, der weiß, daß er über eine echte Kopie von Susannes öffentlichem Schlüssel verfügt. Claus könnte Susannes öffentlichen Schlüssel unterschreiben und sich somit für die Echtheit von Susannes Schlüssel verbürgen. Claus würde diese Unterschrift mit seinem eigenen privaten Schlüssel erstellen.

Dadurch würde ein Unterschriftszertifikat für den öffentlichen Schlüssel erstellt, das beweist, daß Susannes Schlüssel nicht manipuliert wurde. Voraussetzung hierfür ist, daß Sie über eine anerkannt echte Kopie von Claus' öffentlichem Schlüssel zum Überprüfen seiner Unterschrift verfügen. Möglicherweise könnte Claus Susanne auch eine unterschriebene Kopie Ihres öffentlichen Schlüssels zur Verfügung stellen. Claus würde dann als „Schlüsselverwalter“ für Sie und Susanne fungieren.

Dieses unterschriebene Zertifikat für den öffentlichen Schlüssel von Susanne könnte von Claus oder Susanne in die Mailbox geladen werden. Sie haben die Möglichkeit, es später wieder herunterzuladen. Sie könnten dann die Unterschrift mit Hilfe von Claus' öffentlichem Schlüssel überprüfen und folglich sicher sein, daß es sich tatsächlich um Susannes öffentlichen Schlüssel handelt. Ein Betrüger könnte Sie nicht täuschen und dazu verleiten, seinen falschen Schlüssel als Susannes Schlüssel zu akzeptieren, da keine andere Person von Claus erzeugte Unterschriften fälschen kann.

Eine allgemein als vertrauenswürdig erachtete Person könnte sich sogar darauf spezialisieren, als Schlüsselverwalter für Benutzer zu fungieren, indem sie Unterschriftszertifikate für öffentliche Schlüssel dieser Benutzer liefert. Diese vertrauenswürdige Person könnte als „Zertifizierungsinstanz“ betrachtet werden. Bei allen Zertifikaten für öffentliche Schlüssel, die über die Unterschrift der Zertifizierungsinstanz verfügen, könnte vollständig darauf vertraut werden, daß der öffentliche Schlüssel tatsächlich der Person zugehört, der er angeblich gehört. Alle Benutzer, die teilnehmen möchten, benötigen lediglich eine bekanntermaßen gute Kopie des öffentlichen Schlüssels der Instanz, um die Unterschriften der Zertifizierungsinstanz verifizieren zu kön-

nen. In manchen Fällen kann die Zertifizierungsinstanz auch als Schlüssel-Server fungieren. Benutzer, die an ein Netzwerk angeschlossen sind, könnten dann über den Schlüssel-Server öffentliche Schlüssel in Erfahrung bringen. Es besteht jedoch kein Grund für eine Zertifizierung der Schlüssel durch den Schlüssel-Server.

Eine vertrauenswürdige Zertifizierungsinstanz bietet sich besonders für große, anonyme und zentral geleitete Firmen oder Regierungsinstitutionen an. In einigen institutionellen Arbeitsumgebungen existieren Hierarchien von Zertifizierungsinstanzen.

Bei dezentralisierteren Umgebungen ist es wahrscheinlich effektiver, es allen Benutzern zu ermöglichen, als vertrauenswürdige Schlüsselverwalter für ihre Freunde zu fungieren, anstatt auf eine zentralisierte Schlüsselzertifizierungsinstanz zurückzugreifen.

Eine der herausragenden Funktionen von PGP ist, daß das Programm sowohl in einer zentralisierten Umgebung mit einer Zertifizierungsinstanz als auch in einer weiter dezentralisierten Umgebung, in der einzelne Personen ihre privaten Schlüssel miteinander austauschen, verwendet werden kann.

Der Schutz öffentlicher Schlüssel vor möglicher Verfälschung ist das schwierigste Problem in der praktischen Anwendung der Kryptographie mit öffentlichen Schlüsseln. Dieses Problem ist die „Achillessehne“ der Kryptographie mit öffentlichen Schlüsseln, und große Teile der Software sind nur dazu da, dieses Problem zu lösen.

Sie sollten einen öffentlichen Schlüssel nur verwenden, wenn Sie sicher sind, daß es sich um einen echten öffentlichen Schlüssel handelt, der nicht verfälscht wurde, und daß er tatsächlich der Person zugehört, zu der er angeblich gehört. Sie können sicher sein, daß dies der Fall ist, wenn Sie das Zertifikat für den öffentlichen Schlüssel direkt von seinem Eigentümer erhalten haben, oder wenn es über die Unterschrift einer dritten Person verfügt, der Sie vertrauen und von der Sie bereits einen echten öffentlichen Schlüssel erhalten haben. Darüber hinaus sollte die Benutzer-ID den vollständigen Namen des Schlüssel-Eigentümers enthalten, nicht nur den Vornamen.

Sie sollten *in keinem Fall*, so einfach es auch erscheinen mag, einem öffentlichen Schlüssel vertrauen, den Sie von einer Mailbox heruntergeladen haben, wenn dieser nicht von einer Person unterschrieben wurde, der Sie vertrauen. Dieser nicht zertifizierte öffentliche Schlüssel kann durch eine beliebige Person verfälscht worden sein, möglicherweise sogar durch den Systemadministrator der Mailbox.

Wenn Sie gebeten werden, das Zertifikat des öffentlichen Schlüssels einer anderen Person zu unterschreiben, sollten Sie sicherstellen, daß es tatsächlich von der Person stammt, die in der Benutzer-ID dieses Zertifikats genannt wird. Denn mit Ihrer Unterschrift auf dem Zertifikat des öffentlichen Schlüssels dieser Person verbürgen Sie sich dafür, daß dieser öffentliche Schlüssel tatsächlich ihr gehört. Andere Personen, die Ihnen vertrauen, akzeptieren den öffentlichen Schlüssel dieser Person, weil er mit Ihrer Unterschrift versehen ist. Sie sollten nicht auf Informationen aus zweiter Hand vertrauen. Unterschreiben Sie den öffentlichen Schlüssel der anderen Person erst, wenn Sie über unabhängige Informationen aus erster Hand verfügen, daß der Schlüssel tatsächlich zu dieser Person gehört. Sie sollten ihn nur dann unterschreiben, wenn Sie ihn direkt von der betreffenden Person selbst erhalten haben.

Um einen öffentlichen Schlüssel zu unterschreiben, müssen Sie nicht nur sicherstellen, daß der Schlüssel tatsächlich zum angegebenen Eigentümer gehört, da Sie den Schlüssel nicht nur zum Verschlüsseln einer Nachricht verwenden möchten. Zertifizierende Unterschriften von autorisierten Schlüsselverwaltern sollten ausreichend sein, um Sie davon zu überzeugen, daß ein Schlüssel wirklich echt ist und Sie ihn verwenden können. Wenn Sie jedoch selbst einen Schlüssel unterschreiben möchten, sollten Sie über unabhängige Informationen aus erster Hand zu dem Eigentümer dieses Schlüssels verfügen. Sie könnten beispielsweise den Eigentümer des Schlüssels anrufen und ihm den Fingerabdruck des Schlüssels nennen, um zu bestätigen, daß der Schlüssel, den Sie haben, tatsächlich der Schlüssel dieser Person ist. Stellen Sie sicher, daß Sie mit der richtigen Person sprechen.

Denken Sie daran, daß Sie sich mit Ihrer Unterschrift für das Zertifikat des öffentlichen Schlüssels nicht für die Integrität dieser Person verbürgen, sondern lediglich für die Integrität dieses öffentlichen Schlüssels, d. h. für die Tatsache, daß der Schlüssel zu dieser Person gehört. Sie riskieren also Ihre Glaubwürdigkeit nicht, wenn Sie den öffentlichen Schlüssel eines Kriminellen unterschreiben, wenn Sie absolut sicher sind, daß dieser Schlüssel tatsächlich zu ihm gehört. Andere Personen werden dann den Schlüssel als seinen Schlüssel akzeptieren, da er von Ihnen unterschrieben wurde (vorausgesetzt, diese Personen vertrauen Ihnen), doch sie würden deshalb nicht dem Eigentümer des Schlüssels vertrauen. Vertrauen in einen Schlüssel ist nicht identisch mit dem Vertrauen in den Eigentümer eines Schlüssels.

Es ist empfehlenswert, Ihren eigenen öffentlichen Schlüssel zusammen mit einer Sammlung zertifizierender Unterschriften von verschiedenen Schlüsselverwaltern aufzubewahren. So besteht die Chance, daß die meisten Personen zumindest einem der Schlüsselverwalter vertrauen, die sich für die Gültigkeit Ihres öffentlichen Schlüssels verbürgen. Sie könnten Ihren Schlüssel mit der angehängten Sammlung zertifizierender Unterschriften in verschiedenen Mailboxen ablegen. Wenn Sie den öffentlichen Schlüssel einer anderen Person unterschreiben, senden Sie ihn mit Ihrer Unterschrift an diese Person zurück, so daß diese Person Ihre Unterschrift in ihre Sammlung an Authentisierungen für ihren eigenen öffentlichen Schlüssel aufnehmen kann.

Stellen Sie sicher, daß keine andere Person die Möglichkeit hat, Ihren eigenen öffentlichen Schlüsselbund zu verfälschen. Die Überprüfung eines neu unterzeichneten Zertifikats für einen öffentlichen Schlüssel hängt letztlich von der Integrität der vertrauenswürdigen öffentlichen Schlüssel ab, die sich bereits in Ihrem Schlüsselbund befinden. Stellen Sie sicher, daß Sie die physische Kontrolle über Ihren öffentlichen Schlüsselbund haben. Er sollte sich, wie Ihr privater Schlüssel, vorzugsweise auf Ihrem eigenen PC befinden und nicht auf einem entfernten Mehrbenutzersystem. Dadurch schützen Sie den öffentlichen Schlüsselbund vor Verfälschungen, nicht vor Zugriff. Bewahren Sie eine Sicherungskopie Ihres öffentlichen Schlüsselbundes und Ihres privaten Schlüssels auf einem schreibgeschützten Medium auf.

Da Ihr eigener vertrauenswürdiger öffentlicher Schlüssel die letztgültige Instanz zum direkten oder indirekten Zertifizieren aller anderen Schlüssel in Ihrem Schlüsselbund ist, ist er der wichtigste Schlüssel, der vor Fälschungsversuchen geschützt werden muß. Bewahren Sie eine Sicherungskopie auf einer schreibgeschützten Diskette auf.

PGP arbeitet allgemein unter der Voraussetzung, daß Sie die physische Sicherheit Ihres Systems und Ihrer Schlüsselbunde und auch Ihrer PGP-Version selbst sicherstellen. Wenn ein Eindringling die Möglichkeit hat, Ihre Festplatte zu manipulieren, kann er theoretisch auch Änderungen am Programm vornehmen und Sicherheitsfunktionen des Programms ausschalten, mit denen das Verfälschen von Schlüsseln verhindert wird.

Eine etwas komplizierte Art, Ihren gesamten öffentlichen Schlüsselbund vor Verfälschung zu schützen, besteht darin, den gesamten Schlüsselbund mit Ihrem eigenen privaten Schlüssel zu unterschreiben. Dies ist beispielsweise möglich durch das Erstellen eines separaten Unterschriftszertifikats von Ihrem öffentlichen Schlüsselbund.

Wie verfolgt PGP, welche Schlüssel gültig sind?

Lesen Sie zuerst den vorangegangenen Abschnitt „So schützen Sie öffentliche Schlüssel vor Manipulation“, bevor Sie mit diesem Abschnitt beginnen.

PGP zeichnet auf, welche Schlüssel Ihres öffentlichen Schlüsselbundes ordnungsgemäß mit Unterschriften von vertrauenswürdigen Schlüsselverwaltern zertifiziert wurden. Sie müssen PGP lediglich mitteilen, welchen Personen Sie als Schlüsselverwaltern vertrauen, und deren Schlüssel mit Ihrem eigenen, unbedingt vertrauenswürdigen Schlüssel selbst unterschreiben. PGP kann dann das „Steuer übernehmen“ und automatisch andere Schlüssel überprüfen, die die von Ihnen bestimmten Schlüsselverwalter unterschrieben haben. Und Sie können selbstverständlich auch selbst weitere Schlüssel direkt unterschreiben.

PGP verwendet zur Beurteilung des Wertes eines öffentlichen Schlüssels zwei voneinander völlig unabhängige Kriterien, die Sie nicht miteinander verwechseln sollten:

1. Gehört der Schlüssel tatsächlich zu der Person, zu der er zu gehören scheint? Anders ausgedrückt: Wurde der Schlüssel durch eine vertrauenswürdige Unterschrift zertifiziert?

2. Gehört der Schlüssel zu einer Person, der Sie bezüglich der Zertifizierung anderer Schlüssel vertrauen können?

PGP kann die Antwort auf die erste Frage errechnen. Die Antwort auf die zweite Frage müssen Sie PGP genau mitteilen. Wenn Sie Frage 2 beantwortet haben, kann PGP die Antwort zu Frage 1 für andere Schlüssel berechnen, die von dem Schlüsselverwalter unterschrieben wurden, dem Sie Ihr Vertrauen ausgesprochen haben.

Schlüssel, die von einem autorisierten Schlüsselverwalter zertifiziert worden sind, werden von PGP für echt gehalten. Die zu autorisierten Schlüsselverwaltern gehörenden Schlüssel wiederum müssen entweder von Ihnen oder von anderen vertrauenswürdigen Schlüsselverwaltern zertifiziert werden.

Darüber hinaus können Sie mit PGP die Eignung von bestimmten Personen als Schlüsselverwalter durch Zuweisung eines bestimmten Vertrauensgrads präzisieren. Das Vertrauen, das Sie einem Schlüsseleigentümer bezüglich seiner Eignung als Schlüsselverwalter aussprechen, spiegelt nicht nur Ihre Einschätzung der persönlichen Integrität dieser Personen wider. Es sollte auch ausdrücken, in welchem Maße Sie dieser Person Kompetenz bei der Schlüsselverwaltung und gutes Urteilsvermögen beim Unterschreiben von Schlüsseln zutrauen. Sie können einer Person kein, geringes oder volles Vertrauen zum Zertifizieren von anderen öffentlichen Schlüsseln aussprechen. Der angege-

bene Vertrauensgrad wird in Ihrem Schlüsselbund zusammen mit dem Schlüssel dieser Personen gespeichert. Wenn Sie PGP jedoch zum Kopieren eines Schlüssels von Ihrem Schlüsselbund auffordern, werden diese Vertrauensinformationen nicht mitkopiert, da Ihre private Meinung bezüglich des Vertrauens vertraulich behandelt wird.

Wenn PGP die Gültigkeit eines öffentlichen Schlüssels berechnet, überprüft es den Vertrauensgrad aller angehängten zertifizierenden Unterschriften. Es berechnet einen abgewogenen Echtheitswert. Zwei Unterschriften mit einem geringen Vertrauen werden beispielsweise als genauso vertrauenswürdig betrachtet wie eine Unterschrift mit vollem Vertrauen. Die Skepsis des Programms kann eingestellt werden. Sie können beispielsweise PGP so einstellen, daß zwei Unterschriften mit vollem Vertrauen oder drei Unterschriften mit geringem Vertrauen notwendig sind, damit ein Schlüssel als echt beurteilt wird.

Ihr eigener Schlüssel wird „axiomatisch“ von PGP als echt anerkannt und benötigt keine Unterschrift eines Schlüsselverwalters als Gültigkeitsbeweis. PGP weiß, welche öffentlichen Schlüssel zu Ihnen gehören, indem es im privaten Schlüsselbund nach den entsprechenden privaten Schlüsseln sucht. PGP geht auch davon aus, daß Sie sich selbst zum Zertifizieren anderer Schlüssel volles Vertrauen aussprechen.

Im Laufe der Zeit werden Sie über immer mehr Schlüssel von anderen Personen verfügen, die Sie möglicherweise als autorisierte Schlüsselverwalter bestimmen möchten. Alle anderen Personen werden ihre eigenen autorisierten Schlüsselverwalter wählen. So bauen alle nach und nach eine Sammlung von zertifizierenden Unterschriften anderer Personen auf und verteilen sie mit ihrem Schlüssel in der Hoffnung, daß die Empfänger zumindest einer oder zwei der Unterschriften vertrauen. Dadurch entsteht ein dezentrales, fehlertolerantes Vertrauensnetz für alle öffentlichen Schlüssel.

Dieser einzigartige basisorientierte Ansatz unterscheidet sich erheblich von den üblichen Verwaltungssystemen für öffentliche Schlüssel, die von der Regierung und anderen Institutionen entwickelt wurden, wie beispielsweise Internet Privacy Enhanced Mail (PEM), die auf einer zentralisierten Kontrolle und vorgeschriebenem zentralisiertem Vertrauen basieren. Diese Standardsysteme beruhen auf einer Hierarchie von Zertifizierungsinstanzen, die vorschreiben, wem Sie vertrauen müssen. Die dezentralisierte, probabilistische Methode des Programms zur Bestimmung der Legitimität öffentlicher Schlüssel stellt das Herzstück seiner Schlüsselverwaltungsarchitektur dar. In PGP bestimmen Sie allein, wem Sie vertrauen, so daß Sie an der Spitze Ihrer privaten Zertifizierungspyramide stehen. PGP ist für Personen bestimmt, die Verantwortung lieber selbst wahrnehmen.

Die Betonung dieses dezentralisierten, basisorientierten Ansatzes bedeutet jedoch nicht, daß PGP in stärker hierarchisch ausgeprägten, zentralisierten Verwaltungssystemen für öffentliche Schlüssel nicht ebenso leistungsfähig ist. Beispielsweise ziehen es große Unternehmen möglicherweise vor, das Unterschreiben aller Mitarbeiterschlüssel von einer zentralen Stelle oder Person vornehmen zu lassen. PGP ermöglicht dieses zentralisierte Szenario als speziellen Ausnahmefall im Rahmen des allgemeineren Vertrauensmodells von PGP.

So schützen Sie private Schlüssel vor unbefugtem Zugriff

Schützen Sie Ihren privaten Schlüssel und Ihre Paßphrase sorgfältig. Falls Ihr privater Schlüssel nicht mehr sicher sein sollte, sollten Sie so schnell wie möglich alle betroffenen Personen darüber informieren, bevor eine dritte Person diesen Schlüssel verwendet, um in Ihrem Namen zu unterschreiben. Ein Dritter könnte beispielsweise den privaten Schlüssel zum Unterschreiben von gefälschten Zertifikaten für öffentliche Schlüssel verwenden. Dies könnte für viele Personen problematisch werden, insbesondere dann, wenn ein großer Personenkreis Ihrer Unterschrift vertraut. Eine Gefährdung Ihres eigenen privaten Schlüssels könnte selbstverständlich auch zur Offenlegung aller an Sie gesendeten Nachrichten führen.

Um Ihren privaten Schlüssel zu schützen, sollten Sie ihn zuallererst stets sicher aufbewahren. Sie können ihn auf Ihrem PC zu Hause oder auf Ihrem Notebook-Computer speichern, den Sie mit sich führen. Wenn Sie einen Computer im Büro verwenden müssen, zu dem nicht nur Sie allein physischen Zugang haben, sollten Sie Ihren öffentlichen und privaten Schlüsselbund auf einer schreibgeschützten Diskette aufbewahren und diese nicht unbeaufsichtigt lassen. Es ist nicht ratsam, den privaten Schlüssel auf einem entfernten Host, wie beispielsweise einem UNIX-System zur Ferneinwahl aufzubewahren. Jemand könnte heimlich Ihre Modem-Leitung abhören, Ihre Paßphrase abfangen und dann Ihren privaten Schlüssel von dem entfernten System abrufen. Sie sollten einen privaten Schlüssel nur auf einem Computer verwenden, auf den Sie ständig zugreifen.

Speichern Sie Ihre Paßphrase nicht auf dem Computer, auf dem sich Ihre private Schlüsseldatei befindet. Das Speichern Ihres privaten Schlüssels und der Paßphrase auf dem gleichen Computer ist genauso gefährlich wie das Aufbewahren der Karte für den Geldautomaten zusammen mit der Geheimnummer in einem Portemonnaie. Die Paßphrase darf sich also nicht auf demselben Datenträger befinden wie die private Schlüsseldatei. Am sichersten ist es, wenn Sie Ihre Paßphrase auswendig lernen und sie ausschließlich in Ihrem Kopf speichern. Wenn Sie Ihre Paßphrase aufschreiben müssen, sollten Sie eine sichere Stelle wählen, möglicherweise sogar sicherer als die Stelle, an der Sie Ihre private Schlüsseldatei aufbewahren.

Fertigen Sie außerdem Sicherungskopien von Ihrem privaten Schlüssel an. Denken Sie daran, daß Sie über die einzige Kopie Ihres privaten Schlüssels verfügen. Wenn Sie diese Kopie verlieren, sind alle Kopien Ihres öffentlichen Schlüssels, die Sie über die ganze Welt hinweg verteilt haben, nicht mehr zu verwenden.

Der dezentralisierte, nicht institutionelle Ansatz, den PGP zur Verwaltung von öffentlichen Schlüsseln unterstützt, hat seine Vorteile. Sein Nachteil ist, daß es keine einzige zentralisierte Liste von Schlüsseln gibt, die nicht mehr sicher sind. Dadurch wird es etwas schwieriger, den durch unsicher gewordene Schlüssel verursachten Schaden einzugrenzen. Sie können nur die Information verbreiten und darauf hoffen, daß sie bei allen betroffenen Personen ankommt.

Im schlimmsten Fall, d. h., wenn sowohl Ihr privater Schlüssel als auch die Paßphrase nicht mehr sicher sind (und Sie dies hoffentlich auch entdecken), müssen Sie ein „Schlüsselzurücknahmezertifikat“ ausstellen. Mit diesem Zertifikat warnen Sie andere Personen davor, Ihren öffentlichen Schlüssel weiterhin zu verwenden. Sie können ein solches Zertifikat mit PGP erstellen, indem Sie im PGPkeys-Menü den Zurücknehmen-Befehl wählen. Alternativ kann der zugeordnete Rücknahmeschlüssel diese Aufgabe für Sie übernehmen. Sie müssen das Zertifikat anschließend an den Certificate Server senden, so daß andere Benutzer auf das Zertifikat zugreifen können. Die PGP-Software der Empfänger wiederum installiert das Zurücknahmezertifikat für den Schlüssel in deren öffentlichen Schlüsselbunden und verhindert automatisch, daß Ihr öffentlicher Schlüssel versehentlich wieder verwendet wird. Sie können dann ein neues Schlüsselpaar (d. h. einen neuen privaten und einen zugehörigen öffentlichen Schlüssel) erstellen und den neuen öffentlichen Schlüssel veröffentlichen. Sie können auch Ihren neuen öffentlichen Schlüssel und das Zurücknahmezertifikat für den Schlüssel für Ihren alten Schlüssel zusammen verschicken.

Was passiert, wenn Sie Ihren privaten Schlüssel verlieren?

Sie können Ihren eigenen privaten Schlüssel zurücknehmen, indem Sie im PGPkeys-Menü den Zurücknehmen-Befehl wählen und ein Zurücknahmezertifikat ausstellen, das mit Ihrem eigenen privaten Schlüssel unterschrieben wird.

Aber was können Sie tun, wenn Sie Ihren privaten Schlüssel verlieren, oder wenn Ihr privater Schlüssel zerstört wurde? Sie können den öffentlichen Schlüssel nicht selbst zurücknehmen, da Sie Ihren eigenen privaten Schlüssel zum Zurücknehmen benötigen, diesen aber nicht mehr besitzen. Wenn Sie Ihrem Schlüssel keinen Rücknahmeschlüssel zugeordnet haben (d. h., einen PGP-Benutzer, der den Schlüssel in Ihrem Namen zurücknehmen kann), so

müssen Sie jeden Benutzer, der Ihren Schlüssel unterzeichnet hat, darum bitten, seine Zertifizierung zurückzunehmen. Dadurch erfahren alle Personen, die Ihren Schlüssel aufgrund des ausgesprochenen Vertrauens einer Ihrer Schlüsselverwalter verwenden möchten, daß Sie Ihrem öffentlichen Schlüssel nicht vertrauen können.

Weitere Informationen über zugeordnete Rücknahmeschlüssel finden Sie im *PGP-Benutzerhandbuch.*

Lassen Sie sich nicht täuschen

Wenn Sie ein kryptographisches Software-Paket überprüfen, stellt sich am Ende immer die Frage, warum Sie diesem Produkt trauen sollten. Selbst wenn Sie den Quellcode selbst überprüfen, haben Sie vielleicht nicht genügend Erfahrung in der Kryptographie, um die Sicherheit wirklich beurteilen zu können. Und selbst wenn Sie viel Erfahrung in der Kryptographie besitzen, können Sie kleine Schwächen in den Algorithmen möglicherweise übersehen.

Als Student erfand ich in den frühen siebziger Jahren ein meiner Meinung nach brillantes Verschlüsselungssystem. Um chiffrierten Text zu erzeugen, fügte ich zum Klartextdatenstrom einen einfachen Datenstrom aus Pseudozufallswerten hinzu. Ich war der Ansicht, daß dadurch jedwede Häufigkeitsanalyse an dem chiffrierten Text vereitelt würde und selbst die raffiniertesten Geheimdienste der Regierung den Text nicht decodieren könnten. Ich war mehr als stolz auf meine Idee.

Jahre später entdeckte ich genau dieses System in mehreren einleitenden Texten und Lernmaterialien zur Kryptographie. Großartig. Andere Kryptologen hatten dieselbe Idee gehabt. Leider wurde das System als einfache Übung zu dem Thema verwendet, wie ein Verschlüsselungssystem mit einfachen kryptographischen Techniken aufgebrochen werden kann. So viel zu meiner genialen Idee.

Aus dieser demütigenden Erfahrung lernte ich, wie schnell man beim Entwikkeln eines Verschlüsselungsalgorithmus ein falsches Sicherheitsgefühl entwickeln kann. Die wenigsten Menschen sind sich bewußt, wie extrem schwierig es ist, einen Verschlüsselungsalgorithmus zu entwickeln, der andauernden und hartnäckigen Angriffen eines raffinierten Gegners widerstehen kann. Viele allgemein ausgebildete Software-Ingenieure haben in bester Absicht ebenso einfach zu decodierende Verschlüsselungssysteme (oftmals sogar dasselbe Verschlüsselungssystem) entwickelt, und manche dieser Systeme wurden in kommerzielle Verschlüsselungssoftwarepakete eingebunden und für sehr viel Geld an Tausende arglose Benutzer verkauft.

Dies ist vergleichbar mit dem Verkauf eines Sicherheitsgurtes, dessen Design vom äußeren Eindruck her überzeugend ist, der jedoch bei der geringsten Geschwindigkeit im Aufpralltest aufspringt. Sich auf diese Sicherheitsgurte zu verlassen, kann schlimmere Folgen haben, als gar keinen Sicherheitsgurt zu verwenden. Denn niemand vermutet, daß Gurte untauglich sind – bis es wirklich zum Unfall kommt. Wenn Sie sich auf eine schwache kryptographische Software verlassen, setzen Sie unter Umständen wichtige und vertrauliche Daten unbewußt einem Risiko aus, was Sie ohne die kryptographische Software vielleicht nicht getan hätten. Möglicherweise fällt Ihnen noch nicht einmal auf, daß eine unbefugte Person auf Ihre Daten zugegriffen hat.

In manchen kommerziellen Software-Paketen wird der DES-Standard (Federal Data Encryption Standard) verwendet, ein recht guter, konventioneller Algorithmus, der von der Regierung für den professionellen Gebrauch (seltsamerweise jedoch nicht für unter Geheimschutz gestellte Informationen – hmmm…) empfohlen wird. DES kann in verschiedenen „Betriebsmodi“ verwendet werden, wobei einige qualitativ besser sind als andere. Die Regierung empfiehlt ausdrücklich, für Nachrichten nicht den einfachsten und unsichersten Modus, den ECB -Modus (Electronic Codebook), zu verwenden. Sie empfiehlt jedoch die leistungsstärkeren und komplexeren Modi CFB (Cipher Feedback) und CBC (Cipher Block Chaining).

Leider wird in den meisten mir bekannten kommerziellen Verschlüsselungsprogrammpaketen der ECB-Modus verwendet. Als ich mit einigen der Entwickler dieser Programme sprach, sagten sie mir, daß sie noch nie vom CBC- oder CFB-Modus gehört hätten und daß ihnen nichts über die Schwächen des ECB-Modus bekannt sei. Schon allein die Tatsache, daß die Entwickler dieser Programme über so wenig kryptographische Kenntnisse verfügen, daß ihnen diese elementaren Konzepte nicht bekannt sind, ist nicht gerade beruhigend. Außerdem werden die DES-Schlüssel in diesen Programmen zum Teil auf ungeeignete und unsichere Weise verwaltet. Diese Software-Pakete enthalten oft auch einen zweiten, schnelleren Verschlüsselungsalgorithmus, der anstelle des langsameren DES verwendet werden kann. Die Entwickler dieser Programmpakete waren oft der Meinung, daß der eigene schnelle Algorithmus genauso sicher wie DES sei, doch nach einigen Nachfragen stellte ich immer wieder fest, daß es sich lediglich um eine Variante des „genialen Systems“ aus meiner Studentenzeit handelte. Teilweise wollten die Entwickler die Funktionsweise ihrer eigenen Verschlüsselungssysteme überhaupt nicht preisgeben, versicherten mir jedoch, es handle sich um ein geniales System, und ich solle ihnen ruhig vertrauen. Ich bin sicher, daß die Entwickler ihren Algorithmus für genial halten, aber wie kann ich sicher sein, wenn ich ihn mir nicht ansehen kann?

Fairerweise muß ich an dieser Stelle anmerken, daß diese extrem leistungsschwachen Produkte in den meisten Fällen nicht von Firmen stammen, die sich auf kryptographische Technologie spezialisiert haben.

Selbst die wirklich guten Software-Pakete, die DES in den korrekten Betriebsmodi verwenden, weisen noch Probleme auf. Der Standard-DES-Modus verwendet einen 56-Bit-Schlüssel, der nach heutigen Standards zu klein ist und auf dem gegenwärtigen Stand der Technik durch umfangreiche Schlüssel-Suchfunktionen auf speziellen, extrem leistungsfähigen Rechnern leicht aufgebrochen werden kann. Der DES-Algorithmus hat seinen Zweck erfüllt und sollte nun in Rente gehen, ebenso wie die Software-Pakete, die auf diesem Algorithmus aufbauen.

Der Hersteller AccessData (http://www.accessdata.com) bietet ein kostengünstiges Software-Paket an, durch das die in WordPerfect, Lotus 1-2-3, MS Excel, Symphony, Quattro Pro, Paradox, MS Word und PKZIP verwendeten integrierten Verschlüsselungssysteme aufgebrochen werden. Es errät nicht nur einfach Paßwörter – es bedient sich richtiger Kryptoanalyse. Manche Personen kaufen es, weil sie das Paßwort für ihre eigenen Dateien vergessen haben. Strafrechtliche Behörden nutzen diese Programme ebenfalls, um die von ihnen beschlagnahmten Dateien lesen zu können. Der Entwickler des Programms, Eric Thompson, erzählte mir, daß sein Programm zum Entschlüsseln lediglich den Bruchteil einer Sekunde benötigt, doch daß er einige Verzögerungsschleifen eingebaut habe, um den Decodierungsprozeß zu verlangsamen, so daß dieser für den Kunden nicht zu einfach erscheint.

Im Bereich abhörsicherer Telefonanlagen sind Ihre Auswahlmöglichkeiten beschränkt. Das meistverkaufte System ist die STU-III (Secure Telephone Unit), hergestellt von Motorola und AT&T für einen Preis zwischen 2.000 und 3.000 US-Dollar und von der Regierung für Geheimhaltungszwecke verwendet. Es verwendet leistungsfähige Kryptographie. Zum Kauf dieser leistungsfähigen Version benötigt man jedoch eine spezielle Lizenz von der Regierung. Auf dem Markt ist eine Version von STU-III erhältlich, die entsprechend den Wünschen des NSA abgeschwächt wurde. Darüber hinaus gibt es eine Exportversion, die noch wesentlich stärker abgeschwächt wurde. Außerdem gibt es das System Surity 3600 von AT&T für 1.200 US-Dollar, das den berühmten Clipper-Chip der Regierung zur Verschlüsselung verwendet, mit bei der Regierung hinterlegten Schlüsseln, um Abhöraktionen zu erleichtern. Darüber hinaus gibt es natürlich noch die analogen (nicht digitalen) Sprachverwürfler, die Sie über Kataloge für Möchtegernspione bestellen können und die im Sinne der Kryptographie absolut nutzlos sind. Sie werden jedoch als „sichere“ Kommunikationsprodukte an Kunden verkauft, die sich in der Materie nicht auskennen.

Auf eine gewisse Art ist Kryptographie mit Medikamenten zu vergleichen. Die richtige Qualität und Zusammensetzung kann von größter Bedeutung sein. Penicillin schlechter Qualität sieht genauso aus wie Penicillin guter Qualität. Sie können feststellen, ob Ihr Tabellenkalkulationsprogramm funktioniert, aber wie stellen Sie fest, ob das Kryptographieprogramm leistungsschwach ist? Von einem schwachen Verschlüsselungsalgorithmus erzeugter chiffrierter Text sieht genauso überzeugend aus wie von einem effi-

zienten Verschlüsselungsalgorithmus erzeugter chiffrierter Text. Es gibt viel unwirksame Medizin auf dem Markt. Und es gibt viele Kurpfuscher. Doch im Gegensatz zu den Wunderdoktoren von früher wissen die Software-Entwickler von heute oft noch nicht einmal, daß ihr Produkt wirkungslos ist. Sie mögen gute Software-Ingenieure sein, doch sie haben im Regelfall nicht eine einzige wissenschaftliche Veröffentlichung über Kryptographie gelesen. Sie sind jedoch der Meinung, daß sie ein gutes kryptographisches Programm schreiben können. Und warum auch nicht? Schließlich scheint es vom Gefühl her so einfach zu sein. Und ihre Programme scheinen gut zu funktionieren.

Jeder, der der Meinung ist, ein nicht zu entschlüsselndes Verschlüsselungssystem entwickelt zu haben, ist entweder ein unglaublich begnadetes Genie oder naiv und unerfahren. Unglücklicherweise habe ich es manchmal mit Möchtegernkryptologen zu tun, die „Verbesserungen“ an PGP durch Hinzufügen von selbstentwickelten Verschlüsselungsalgorithmen durchführen möchten.

Ich erinnere mich an ein Gespräch mit Brian Snow, einem angesehenen NSA-Kryptologen. Er sagte mir, er würde keinem Verschlüsselungsalgorithmus vertrauen, dessen Entwickler sein Metier nicht „von der Pike auf“ durch intensive Beschäftigung mit dem Entschlüsseln von Codes erlernt hätte. Das hörte sich sehr vernünftig an. Ich stellte fest, daß so gut wie kein beruflicher Kryptograph dieses Kriterium erfüllte. „Stimmt,“ sagte er mit einem selbstbewußten Lächeln, „und das macht die Arbeit für den NSA um einiges einfacher.“ Ein beängstigender Gedanke. Auch ich erfüllte dieses Kriterium nicht.

Und auch die Regierung hat unwirksame Medizin verbreitet. Nach dem Zweiten Weltkrieg verkauften die USA deutsche Enigma-Chiffriergeräte an Regierungen der Dritten Welt. Sie sagten ihnen jedoch nicht, daß die Alliierten den Enigma-Code schon während des Krieges entschlüsselt hatten. Diese Tatsache wurde jahrelang geheimgehalten. Selbst heute wird weltweit in vielen UNIX-Systemen noch die Enigma-Chiffre zur Verschlüsselung von Dateien verwendet, was teilweise darin begründet ist, daß die Regierung der Verwendung von besseren Algorithmen durch Gesetze Steine in den Weg gelegt hat. Sie versuchte sogar, die erstmalige Veröffentlichung des RSA-Algorithmus im Jahre 1977 zu verhindern. Außerdem bekämpft die Regierung seit Jahren rigoros alle Anstrengungen von seiten der Wirtschaft, sichere Telefone für die breite Öffentlichkeit zu entwickeln.

Die wichtigste Aufgabe des Nationalen Sicherheitsdienstes der amerikanischen Regierung besteht im Sammeln von Informationen, in erster Linie durch verdecktes Abhören von Privatgesprächen (Buchtip: *The Puzzle Palace* von James Bamford). Der NSA hat erhebliche Fähigkeiten und Ressourcen zum Entschlüsseln von Codes aufgebaut. Wenn die Bevölkerung keine Möglichkeit hat, ihre Privatsphäre durch Anwendung effektiver kryptographischer Methoden zu schützen, wird dem NSA die Arbeit um einiges leichter gemacht. Der NSA hat auch das Recht, Verschlüsselungsalgorithmen zu bewilligen und zu empfehlen. Manche Kritiker führen an, daß hier ein Inter-

essenkonflikt vorliegt, so als würde man „den Bock zum Gärtner machen“. In den 80er Jahren unterstützte der NSA intensiv einen konventionellen Verschlüsselungsalgorithmus, der von ihm selbst entwickelt wurde (das COMSEC-Programm) – über die Funktionsweise konnte jedoch keine Auskunft gegeben werden, da diese der Geheimhaltung unterlag. Der NSA wollte erreichen, daß andere dem Algorithmus vertrauen und ihn verwenden. Aber jeder Kryptologe kann Ihnen sagen, daß ein gut entwickelter Verschlüsselungsalgorithmus nicht geheimgehalten werden muß, um sicher zu bleiben. Es müssen lediglich die Schlüssel geschützt werden. Wie kann irgend jemand wirklich wissen, ob der von der NSA geheimgehaltene Algorithmus sicher ist? Es ist nicht schwer für den NSA, einen Verschlüsselungsalgorithmus zu entwickeln, der nur von ihm entschlüsselt werden kann, wenn niemand sonst den Algorithmus überprüfen kann.

Es gibt drei Hauptfaktoren, die die Qualität von kommerziellen kryptographischen Programmen in den USA unterminiert haben:

- Der erste Faktor ist das praktisch allgegenwärtige Kompetenzdefizit bei Programmierern kommerzieller Verschlüsselungsprogramme (obwohl sich dies seit der Veröffentlichung von PGP allmählich ändert). Jeder Software-Ingenieur hält sich für einen Kryptologen, was zu einer enormen Verbreitung von äußerst schlechter Verschlüsselungssoftware geführt hat.

- Der zweite Faktor ist, daß der NSA absichtlich und systematisch alle guten kommerziellen Verschlüsselungstechnologien durch Einschüchterungsmaßnahmen und wirtschaftlichen Druck unterdrückt. Eine Methode sind u. a. strikte Exportkontrollen für Verschlüsselungsprogramme, was aufgrund der wirtschaftlichen Gesetzmäßigkeiten im Software-Marketing dazu führt, daß amerikanische Verschlüsselungsprogramme im internationalen Wettbewerb direkt benachteiligt werden.

- Die dritte der drei wichtigsten Unterdrückungsmethoden besteht darin, daß alle Softwarepatente für alle auf öffentlichen Schlüsseln basierenden Verschlüsselungsalgorithmen an eine einzige Firma vergeben wurden, wodurch ein Hindernis geschaffen wurde, durch das die Verbreitung dieser Technologie weiter unterdrückt wurde (obwohl dieses Kartell für kryptographische Patente im Herbst 1995 zusammenbrach).

Die eindeutige Konsequenz all dieser Faktoren war, daß vor der Veröffentlichung von PGP in den USA kaum ein Verschlüsselungsprogramm erhältlich war, das höchsten Sicherheitsanforderungen entsprach und vielseitig einsetzbar war.

Ich bin nicht so überzeugt von der Sicherheit von PGP, wie ich als Student von der Genialität meines Verschlüsselungsprogramms überzeugt war. Wenn ich so sicher wäre, wäre das ein schlechtes Zeichen. Aber ich glaube nicht, daß PGP eklatante Schwächen aufweist (obwohl ich ziemlich sicher bin, daß es Fehler enthält). Ich habe die besten Algorithmen aus der kryptographischen

Standardliteratur ausgewählt. Die meisten dieser Algorithmen wurden von Experten genauestens überprüft. Ich kenne viele der weltweit führenden Kryptologen und habe mit einigen von ihnen eine Vielzahl der in PGP verwendeten kryptographischen Algorithmen und Protokolle besprochen. Das Programm ist ausgiebig erforscht und geprüft worden und wurde nach jahrelanger Arbeit fertiggestellt. Und ich arbeite nicht für den NSA. Aber Sie müssen sich bezüglich der kryptographischen Verläßlichkeit von PGP nicht bloß auf mein Wort verlassen, da der Quellcode zum Überprüfen meiner Aussage zur Verfügung steht.

Noch eine letzte Aussage zu meiner Bemühung um kryptographische Qualität in PGP: Seit der Entwicklung und Freigabe der ersten PGP-Version im Jahr 1991 wurde drei Jahre lang vom amerikanischen Zoll wegen der Verbreitung von PGP außerhalb der USA strafrechtlich gegen mich ermittelt. Es bestand die Gefahr einer strafrechtlichen Verfolgung und jahrelanger Gefängnisstrafe. Die Regierung zeigte übrigens bei keinem anderen kryptographischen Programm irgendwelche Zeichen von Aufregung. Erst PGP löste Alarm aus. Was sagt Ihnen dies bezüglich der Qualität von PGP? Mein Ruf beruht auf der kryptographischen Qualität meiner Produkte. Ich werde meinen Einsatz für unser Recht auf Privatsphäre, für das ich meine Freiheit aufs Spiel gesetzt habe, nicht verraten. Ich werde kein Produkt zulassen, das meinen Namen trägt und über geheime Hintertüren verfügt.

Sicherheitsrisiken

„Wenn alle PCs weltweit – d. h. 260 Millionen Computer – an einer einzigen von PGP verschlüsselten Nachricht arbeiten würden, würde es im Schnitt immer noch ungefähr 12 Millionen mal das Alter des Universums dauern, bis eine einzige Nachricht decodiert werden könnte.“

William Crowell, Stellvertretender Direktor des Nationalen Sicherheitsdienstes der USA (NSA), 20. März 1997.

Es gibt kein Datensicherheitssystem, das absolut sicher ist. PGP kann auf verschiedene Weise umgangen werden. In allen Datensicherheitssystemen müssen Sie sich selbst die Frage stellen, ob der Wert der Daten, die Sie zu schützen versuchen, für den Hacker höher einzustufen ist als die Kosten für den Angriff. Sie sollten sich also vor Angriffen schützen, die geringen Aufwand erfordern, und sich keine Sorgen über aufwendige Angriffe machen.

Einige der im folgenden beschriebenen Szenarios erscheinen vielleicht übermäßig paranoid, doch ein solcher Ansatz ist geeignet, um eine vernünftige Diskussion über Sicherheitsrisiken zu führen.

Kompromittierte Paßphrasen oder private Schlüssel

Der wahrscheinlich einfachste Angriff ist möglich, wenn Sie die Paßphrase für Ihren privaten Schlüssel aufschreiben. Wenn jemand die Paßphrase herausfindet und zudem Zugriff auf Ihre private Schlüsseldatei erhält, kann er Ihre Nachrichten lesen und Nachrichten und Dateien in Ihrem Namen unterschreiben.

Im folgenden finden Sie einige Empfehlungen zum Schutz Ihrer Paßphrase:

1. Verwenden Sie keine Paßphrasen, die leicht erraten werden können, wie beispielsweise den Namen Ihrer Kinder oder Ihres Partners.

2. Verwenden Sie Leerzeichen und eine Kombination aus Zahlen und Buchstaben in Ihrer Paßphrase. Wenn Sie ein einziges Wort für Ihre Paßphrase verwenden, kann es von einem Computer leicht durch Ausprobieren aller Wörter im Wörterbuch gefunden werden. Deshalb ist eine Paßphrase wesentlich besser als ein Paßwort. Ein raffinierterer Hacker könnte allerdings auch ein Buch mit berühmten Zitaten in seinen Computer einscannen, um Ihre Paßphrase zu finden.

3. Seien Sie kreativ. Verwenden Sie eine leicht zu merkende, aber schwer zu erratende Paßphrase. Sie können schnell selbst eine Paßphrase erfinden, indem Sie kreativ unsinnige Redewendungen oder unbekannte oder leicht veränderte literarische Zitate verwenden.

Verfälschter öffentlicher Schlüssel

Eines der größten Sicherheitsrisiken besteht, wenn öffentliche Schlüssel verfälscht werden. Dies ist möglicherweise das größte Sicherheitsrisiko in einem Kryptosystem mit öffentlichen Schlüsseln, zum Teil deshalb, weil die meisten Neueinsteiger es nicht direkt erkennen.

Noch einmal zusammengefaßt: Vergewissern Sie sich, wenn Sie den öffentlichen Schlüssel von einer anderen Person verwenden, daß dieser Schlüssel nicht verfälscht wurde. Sie sollten einem neuen öffentlichen Schlüssel einer anderen Person nur trauen, wenn Sie ihn direkt von seinem Eigentümer erhalten haben oder wenn er von jemandem unterschrieben wurde, dem Sie vertrauen. Stellen Sie sicher, daß keine andere Person die Möglichkeit hat, Ihren eigenen öffentlichen Schlüsselbund zu verfälschen. Stellen Sie sicher, daß Sie die physische Kontrolle über Ihren öffentlichen Schlüsselbund und Ihren privaten Schlüssel haben. Ihr Schlüsselpaar sollte sich vorzugsweise auf Ihrem eigenen PC und nicht auf einem entfernten Mehrbenutzersystem befinden. Behalten Sie eine Sicherungskopie von beiden Schlüsselbunden.

Nicht vollständig gelöschte Dateien

Ein weiteres potentielles Sicherheitsproblem wird durch die Art und Weise verursacht, mit der in den meisten Betriebssystemen das Löschen von Dateien gehandhabt wird. Wenn Sie eine Datei verschlüsseln und dann die ursprüngliche Klartextdatei löschen, werden die Daten durch das Betriebssystem nicht wirklich physisch gelöscht. Es markiert die Datenblöcke auf der Festplatte lediglich als gelöscht, um so zu kennzeichnen, daß der Speicherplatz später wieder verwendet werden kann. Das ist so, als ob man vertrauliche Papierdokumente nicht in den Papier-Shredder füttern, sondern in die Schmierpapierablage legen würde. Die Datenblöcke auf der Festplatte enthalten immer noch die ursprünglichen, vertraulichen Daten, die Sie löschen wollten, und werden wahrscheinlich später einmal durch neue Daten überschrieben. Wenn ein Hacker diese gelöschten Datenblöcke von Ihrer Festplatte kurz nach der Zuordnungsaufhebung einliest, könnte er Ihren Klartext wiederherstellen.

Dies könnte sogar versehentlich geschehen, falls ein Problem mit der Festplatte besteht und Dateien unabsichtlich gelöscht oder beschädigt wurden. Ein Wiederherstellungsprogramm für die Festplatte kann zur Wiederherstellung der beschädigten Dateien verwendet werden. Das hat jedoch oft zur Folge, daß vorher gelöschte Dateien zusammen mit allen anderen Daten wiederhergestellt werden. Ihre vertraulichen Dateien, die Sie nie mehr wiederzusehen glaubten, könnten dann wieder auftauchen und von der Person, die versucht, Ihre beschädigte Festplatte wiederherzustellen, eingesehen werden. Auch während Sie die ursprüngliche Nachricht mit einem Textverarbeitungsprogramm oder einem Texteditor erstellen, können, bedingt durch die interne Arbeitsweise dieser Programme, möglicherweise mehrere temporäre Kopien Ihres Textes auf der Festplatte erstellt werden. Diese temporären Kopien Ihres Textes werden vom Textverarbeitungsprogramm nach der Fertigstellung gelöscht, doch die heiklen Daten befinden sich als Fragmente immer noch irgendwo auf Ihrer Festplatte.

Die einzige Möglichkeit, die Wiederherstellung des Klartextes unmöglich zu machen, besteht darin, die gelöschten Klartextdateien auf irgendeine Art zu überschreiben. Wenn Sie nicht sicher sind, ob die gelöschten Datenblöcke auf der Festplatte bald überschrieben werden, müssen Sie absolut sicherstellen, daß die Klartextdatei sowie alle Dateifragmente, die möglicherweise vom Textverarbeitungsprogramm auf der Festplatte zurückgelassen wurden, überschrieben werden. Sie können alle auf der Festplatte verbliebenen Klartextfragmente überschreiben. Verwenden Sie dazu PGP Secure Wipe oder PGP Freespace Wipe.

Viren und Trojanische Pferde

Ein Angriff könnte auch durch einen speziell entwickelten, feindlichen Computer-Virus oder „-Wurm“ erfolgen, der PGP oder Ihr Betriebssystem infizieren könnte. Dieser hypothetische Virus könnte so programmiert sein, daß er Ihre Paßphrase, Ihren privaten Schlüssel oder dechiffrierte Nachrichten erfaßt und die erfaßten Daten in eine Datei schreibt oder über ein Netzwerk an den Eigentümer des Virus schickt. Der Virus könnte möglicherweise auch die Funktionsweise von PGP verändern, so daß Unterschriften nicht mehr richtig überprüft werden. Dieser Angriff ist kostengünstiger als ein kryptoanalytischer Angriff.

Der Schutz vor dieser Art von Angriffen fällt in den Bereich des allgemeinen Schutzes vor Virusinfektionen. Es werden einige relativ brauchbare Antivirenprodukte auf dem Markt angeboten, und es gibt einige „Hygienemaßnahmen“, mit denen die Gefahr einer Virusinfektion in hohem Maße verringert werden kann. Eine vollständige Darstellung möglicher Maßnahmen gegen Viren und Würmer geht über den Rahmen dieses Dokuments hinaus. PGP verfügt über keine Verteidigungsmechanismen gegen Viren und geht davon aus, daß Ihr PC eine sichere Umgebung für die Ausführung des Programms darstellt. Falls tatsächlich ein Virus oder Wurm der oben beschriebenen Art auftreten sollte, würde sich das hoffentlich bald herumsprechen, so daß alle betroffenen Personen gewarnt würden.

Ein ähnlicher Angriff könnte durch eine geschickt gestaltete Imitation von PGP erfolgen, die sich zwar weitgehend wie PGP verhält, jedoch nicht in der vorgesehenen Art funktioniert. Das Programm könnte beispielsweise absichtlich deformiert worden sein, so daß Unterschriften nicht mehr korrekt überprüft werden, wodurch gefälschte Schlüsselzertifikate akzeptiert würden. Diese PGP-Version, deren Wirkungsweise mit einem *Trojanischen Pferd* vergleichbar ist, kann leicht erstellt werden, da der PGP-Quellcode überall verfügbar ist, so daß jeder den Quellcode verändern und somit ein PGP-Imitat erstellen kann, das zwar echt aussieht, in Wahrheit aber eine Fälschung ist. Diese Trojanische PGP-Version könnte dann in Umlauf gebracht werden, da an der Echtheit keine Zweifel bestehen. Wie heimtückisch.

Sie sollten sich daher bemühen, Ihre PGP-Kopie direkt von Network Associates, Inc., zu erwerben.

Sie können auch mit Hilfe von digitalen Unterschriften überprüfen, ob PGP verfälscht worden ist. Sie könnten beispielsweise eine andere PGP-Version, der Sie vertrauen, zum Überprüfen der Unterschrift einer verdächtigen PGP-Version verwenden. Allerdings ist dies nicht von Nutzen, wenn Ihr Betriebssystem infiziert ist, und es kann dadurch auch nicht festgestellt werden, ob die ursprüngliche Kopie der Datei PGP.EXE absichtlich so verändert

wurde, daß die Funktion des Programms zur Überprüfung von Unterschriften beschädigt wurde. Dieser Test geht außerdem von der Voraussetzung aus, daß Sie über eine gute, vertrauenswürdige Kopie des öffentlichen Schlüssels verfügen, mit dem die Unterschrift der verdächtigen ausführbaren PGP-Datei überprüft wird.

Auslagerungsdateien und virtueller Speicher

PGP wurde ursprünglich für MS-DOS entwickelt, ein nach heutigen Standards einfaches Betriebssystem. Als es auf andere, komplexere Betriebssysteme, wie Microsoft Windows oder Macintosh OS portiert wurde, brachte dies ein neues Sicherheitsrisiko mit sich. Dieses Risiko liegt in der Tatsache begründet, daß diese neuen, aufwendigeren Betriebssysteme über einen sogenannten *virtuellen Speicher* verfügen.

Aufgrund des virtuellen Speichers können auf dem Computer riesige Programme ausgeführt werden, deren Größe den Speicherplatz überschreiten, der auf den Halbleiterspeicherchips des Computers zur Verfügung steht. Dies ist sehr nützlich, da Software mehr und mehr „aufgeblasen“ wurde, seit grafische Benutzeroberflächen zur Norm wurden und Benutzer anfingen, mehrere große Anwendungen zur gleichen Zeit auszuführen. Das Betriebssystem verwendet die Festplatte zur Zwischenspeicherung von Softwareteilen, die zur Zeit nicht benötigt werden. Dies hat zur Folge, daß das Betriebssystem möglicherweise ohne Ihr Wissen Daten auf die Festplatte schreibt, die sich Ihrer Meinung nach nur im Hauptspeicher befinden, wie beispielsweise Schlüssel, Paßphrasen oder dechiffrierten Klartext. PGP bewahrt wichtige und vertrauliche Daten dieser Art nicht länger als nötig im Speicher auf, möglicherweise schreibt das Betriebssystem die Daten aber trotzdem auf die Festplatte.

Die Daten werden in einen Notizblockbereich auf der Festplatte geschrieben, der auch als *Auslagerungsdatei* bekannt ist. Wieder benötigte Daten werden wieder aus der Auslagerungsdatei eingelesen, so daß sich jeweils nur ein Teil des Programms oder der Daten im physischen Speicher befindet. All diese Vorgänge sind für den Benutzer nicht sichtbar, er registriert lediglich, daß die Festplatte arbeitet. Microsoft Windows lagert Teile des Speichers, sogenannte *Seiten*, mit Hilfe eines LRU-Seitenersetzungsalgorithmus (Least Recently Used (LRU)) ein und aus. Dies bedeutet, daß die Seiten, die den längsten Zeitraum über nicht mehr verwendet wurden, zuerst auf die Festplatte ausgelagert werden. Dieser Ansatz läßt vermuten, daß in den meisten Fällen das Risiko relativ gering ist, daß vertrauliche Daten auf die Festplatte ausgelagert werden, da PGP diese Daten nur für kurze Zeit im Speicher aufbewahrt. Eine Garantie wird von uns allerdings nicht gegeben.

Jede Person, die physischen Zugriff auf Ihren Computer hat, kann auf die Auslagerungsdatei zugreifen. Wenn Sie gegen dieses Problem etwas unternehmen möchten, können Sie beispielsweise spezielle Software zum Überschreiben der Auslagerungsdatei erwerben. Eine andere Möglichkeit besteht in der Deaktivierung der Funktion des virtuellen Speichers in Ihrem Betriebssystem. Unter Microsoft Windows ist dies ebenso möglich wie unter Mac OS. Die Deaktivierung des virtuellen Speichers kann zur Folge haben, daß Sie mehr physische RAM-Chips installieren müssen, um alle Daten im RAM speichern zu können.

Physischer Eingriff in die Privatsphäre

Durch einen physischen Eingriff in Ihre Privatsphäre kann eine Person in den physischen Besitz Ihrer Klartextdateien oder ausgedruckter Nachrichten kommen. Ein entschlossener Gegner kann dies beispielsweise durch Einbruch, Durchsuchen des Abfalls, widerrechtliche Durchsuchung oder Beschlagnahme, Bestechung, Erpressung oder Einschleusen eines Mitarbeiters in Ihre Organisation erreichen. Manche dieser Angriffe können insbesondere bei politischen Basisorganisationen leicht durchzuführen sein, die mit einer Vielzahl freiwilliger Mitarbeiter arbeiten.

Verlieren Sie nicht durch ein falsches Sicherheitsgefühl Ihre Wachsamkeit, weil Sie über ein kryptograpisches Werkzeug verfügen. Kryptographische Techniken schützen Daten nur, während sie verschlüsselt sind. Direkte physische Sicherheitsverletzungen können weiterhin Klartextdaten oder schriftliche oder mündliche Informationen gefährden.

Diese Angriffe sind weniger aufwendig als kryptoanalytische Angriffe auf PGP.

Tempest-Angriffe

Eine andere Angriffsform, die von Gegnern mit einer sehr guten Ausrüstung verwendet werden kann, besteht im Aufzeichnen der durch Ihren Computer ausgegebenen elektromagnetischen Signale von einer entfernten Stelle aus. Dieser kosten- und relativ arbeitsintensive Angriff ist wahrscheinlich immer noch weniger aufwendig als ein direkter kryptoanalytischer Angriff. Ein für diesen Zweck ausgestattetes Fahrzeug, z. B. ein Lieferwagen, kann in der Nähe Ihres Büros geparkt werden und von dort aus all Ihre Tastenbetätigungen verfolgen und die auf Ihrem Computerbildschirm angezeigten Nachrichten aufzeichnen. Dadurch würden Ihre Paßwörter, Nachrichten usw. gefährdet. Diese Art von Angriff kann abgewehrt werden, indem Sie Ihre Computer-Ausrüstung und Ihre Netzwerkverkabelung mit einem Schutz ver-

sehen, so daß keine elektromagnetischen Signale mehr nach außen dringen können. Diese Schutztechnologie ist als „Tempest“ bekannt und wird von Regierungsdiensten und im Bereich der Verteidigung tätigen Unternehmen verwendet. Es gibt Hardware-Vertreiber, die den Tempest-Schutz auch kommerziell anbieten.

Schutz vor gefälschten Zeitmarkierungen

Ein unwahrscheinlicheres Sicherheitsrisiko von PGP ist die Möglichkeit, daß unehrliche Benutzer die Zertifikate für ihre eigenen öffentlichen Schlüssel und Unterschriften mit falschen Zeitmarkierungen versehen. Sie können diesen Abschnitt überspringen, wenn Sie PGP nur gelegentlich verwenden und sich nicht ausführlich mit den weniger wichtigen Aspekten des Umgangs mit öffentlichen Schlüssel-Protokollen befassen möchten.

Ein unehrlicher Benutzer kann ohne Probleme die Datums- und Zeiteinstellung seines eigenen Systems ändern und so eigene Zertifikate für öffentliche Schlüssel sowie Unterschriften erzeugen, die den Anschein erwecken, sie seien zu einem anderen Zeitpunkt erstellt worden. Er kann es so aussehen lassen, daß er etwas früher oder später unterschrieben hat, als es in Wirklichkeit der Fall war, oder daß sein Schlüsselpaar aus öffentlichem und privatem Schlüssel zu einem früheren oder späteren Zeitpunkt erstellt wurde. Dies kann für ihn mit einem rechtlichen oder finanziellen Vorteil verbunden sein, wenn er sich dadurch beispielsweise eine Möglichkeit schafft, seine eigene Unterschrift abzustreiten.

Meiner Meinung nach ist dieses Problem der gefälschten Zeitmarkierungen bei digitalen Unterschriften nicht gravierender, als es auch bei handschriftlichen Unterschriften ist. Jeder kann ein beliebiges Datum neben seine handschriftliche Unterschrift auf einen Vertrag schreiben, doch niemand zeigt sich aufgrund dieses Zustandes alarmiert. In manchen Fällen hat ein „inkorrektes“ Datum im Zusammenhang mit einer handschriftlichen Unterschrift vielleicht gar nichts mit einem tatsächlichen Betrug zu tun. Die Zeitangabe kann der Zeitpunkt sein, an dem der Unterschreibende bestätigt, daß er ein Dokument unterschrieben hat, oder vielleicht der Zeitpunkt, zu dem die Unterschrift wirksam werden soll.

In Situationen, in denen das richtige Datum einer Unterschrift von größter Wichtigkeit ist, kann einfach ein Notar herangezogen werden, um die handschriftliche Unterschrift zu bezeugen und zu datieren. Genauso kann bei digitalen Unterschriften ein vertrauenswürdiger Dritter herangezogen werden, wenn ein Unterschriftszertifikat in Verbindung mit einer zuverlässigen Zeitmarkierung unterschrieben werden soll. Dazu sind keine exotischen oder übermäßig formalen Protokolle notwendig. Unter Zeugen ausgeführte Unterschriften sind schon lange als eine rechtmäßige Form anerkannt, um den Zeitpunkt zu bestimmen, an dem ein Dokument unterschrieben wurde.

Eine vertrauenswürdige Zertifizierungsinstanz oder ein Notar könnte notariell beglaubigte Unterschriften mit einer zuverlässigen Zeitmarkierung versehen. Dazu wäre nicht notwendigerweise eine zentralisierte Instanz erforderlich. Gegebenenfalls könnten beliebige vertrauenswürdige Verwalter oder nicht betroffene Parteien diese Funktion übernehmen, in der gleichen Form, wie dies auch bei zur Beglaubigung von Dokumenten berechtigten öffentlichen Stellen der Fall ist. Wenn ein Notar Unterschriften anderer Personen unterschreibt, wird ein Unterschriftszertifikat von einem Unterschriftszertifikat erstellt. Dies würde die Unterschrift auf die gleiche Weise bezeugen, wie es bei der Bezeugung einer handschriftlichen Unterschrift durch einen vereidigten Notar der Fall ist. Der Notar könnte das Unterschriftszertifikat separat (ohne das eigentliche Dokument, das unterschrieben wurde) in eine spezielle, vom Notar kontrollierte Protokolldatei einfügen. Diese Protokolldatei könnte von jedermann eingesehen werden. Die Unterschrift des Notars würde über eine zuverlässige Zeitmarkierung verfügen, die möglicherweise eine größere Glaubwürdigkeit oder eine größere rechtliche Bedeutung hat als die Zeitmarkierung in der ursprünglichen Unterschrift.

Eine gute Abhandlung zu diesem Thema finden Sie in einem Artikel von Denning, der 1983 in „IEEE Computer“ veröffentlicht wurde. Zukünftige Erweiterungen von PGP werden möglicherweise über Funktionen verfügen, mit denen notariell beglaubigte Unterschriften für andere Unterschriften in Verbindung mit zuverlässigen Zeitmarkierungen auf einfache Weise verwaltet werden können.

Datengefährdung in Mehrbenutzersystemen

PGP wurde ursprünglich für Einzelbenutzer-PCs entwickelt, auf die der Eigentümer direkt zugreifen kann. Wenn Sie PGP zu Hause auf Ihrem eigenen PC ausführen, sind Ihre verschlüsselten Dateien relativ sicher, es sei denn, jemand bricht in Ihr Haus ein, stiehlt Ihren PC und bringt Sie dazu, Ihre Paßphrase preiszugeben (falls Ihre Paßphrase nicht sehr leicht erraten werden kann).

PGP ist nicht darauf ausgerichtet, Daten zu schützen, die sich in Klartextform auf einem nicht abgesicherten System befinden. PGP kann auch nicht verhindern, daß ein Eindringling ausgeklügelte Methoden verwendet, um Ihren privaten Schlüssel zu lesen, während er verwendet wird. Sie müssen diese Risiken auf einem Mehrbenutzersystem berücksichtigen und Ihre Erwartungen und Ihr Verhalten dementsprechend anpassen. Möglicherweise empfiehlt es sich in Ihrer Situation, PGP nur auf einem isolierten Einzelbenutzersystem zu verwenden, auf das Sie direkt zugreifen können.

Datenverkehrsanalyse

Selbst wenn der Hacker den Inhalt Ihrer verschlüsselten Nachrichten nicht entziffern kann, kann er möglicherweise zumindest einige nützliche Informationen aus Beobachtungen bezüglich der Herkunft und des Ziels der Nachrichten, ihrer Größe sowie der Tageszeit ziehen, zu der sie versendet wurden. Dies ist vergleichbar mit Informationen, die ein Hacker durch Untersuchung Ihrer detaillierten Telefonrechnung erhalten würde, um zu erfahren, mit wem Sie zu welchem Zeitpunkt wie lange telefoniert haben. Diese Informationen sind dem Hacker zugänglich, obwohl er den tatsächlichen Inhalt der Gespräche nicht kennt. Dies wird Datenverkehrsanalyse genannt. PGP allein schützt nicht gegen Datenverkehrsanalyse. Die Lösung dieses Problems würde spezielle Kommunikationsprotokolle erfordern, die speziell darauf ausgerichtet sind, das Ableiten von Informationen aus Ihrem Kommunikationssystem durch Datenverkehrsanalysen zu verringern, möglicherweise mit Hilfe von Kryptographie.

Kryptoanalyse

Ein aufwendiger und gefährlicher kryptoanalytischer Angriff könnte von einer Person oder Institution durchgeführt werden, der überdurchschnittliche Computer-Ressourcen zur Verfügung stehen, wie beispielsweise dem Geheimdienst einer Regierung. Dadurch könnte Ihr öffentlicher Schlüssel unter Verwendung einer neuen mathematischen Geheimmethode entschlüsselt werden. Die nichtmilitärische akademische Welt hat jedoch die Kryptographie mit öffentlichen Schlüsseln seit 1978 erfolglos attackiert.

Möglicherweise verfügt die Regierung über bestimmte Methoden zur Entschlüsselung der in PGP verwendeten konventionellen Verschlüsselungsalgorithmen. Dies ist der Alptraum eines jeden Kryptologen. In praktischen kryptographischen Anwendungen kann es keine absoluten Sicherheitsgarantien geben.

Ein gewisser Grad an Optimismus ist dennoch gerechtfertigt. Die in PGP verwendeten Algorithmen für öffentliche Schlüssel, Nachrichtenkernalgorithmen und Blockchiffrierer wurden von weltweit führenden Kryptographen entwickelt. Sie wurden von den besten Kryptoanalytikern umfangreichen Sicherheitsanalysen und Überprüfungen unterzogen.

Auch wenn die in PGP verwendeten Blockchiffrierer über leichte, nicht bekannte Schwächen verfügen sollten, werden diese Schwächen in hohem Maße dadurch reduziert, daß PGP den Klartext vor der Verschlüsselung komprimiert. Die rechnerische Arbeitsleistung, die zum Aufbrechen erforderlich wäre, wäre wahrscheinlich um ein Vielfaches umfangreicher, als es der Wert der Nachricht rechtfertigen würde.

Falls Sie Grund zu der Annahme haben, daß ernstzunehmende Angriffe dieser Größenordnung auf Ihre Daten vorgenommen werden könnten, sollten Sie möglicherweise einen Datensicherheitsberater zu Rate ziehen, der Ihnen an bestimmte Gegebenheiten angepaßte Sicherheitskonzepte vorstellen kann, die auf Ihre individuellen Bedürfnisse zugeschnitten sind.

Zusammenfassend ist festzuhalten, daß ohne effektiven kryptographischen Schutz ein Gegner keinerlei Mühe aufwenden muß, um Ihre Nachrichten abzuhören, und dies vielleicht sogar gewohnheitsmäßig tut, insbesondere, wenn diese Daten über eine Modemverbindung oder über ein E-Mail-System gesendet werden. Wenn Sie PGP verwenden und vernünftige Vorsichtsmaßnahmen treffen, erschweren Sie potentiellen Hackern den Eingriff in Ihre Privatsphäre ganz erheblich.

Wenn Sie sich gegen sämtliche Angriffe auf Ihre Privatsphäre schützen und sicherstellen möchten, daß keine über überdurchschnittliche Ressourcen verfügenden Personen in Ihre Privatsphäre eindringen können, sind Sie mit PGP hervorragend beraten. PGP schützt Ihre Privatsphäre ausgesprochen gut, daher auch der Name „Pretty Good Privacy“.

Glossar

A5	Ein brancheninterner kryptographischer Algorithmus, der in Europa für Mobiltelefone verwendet wird.
AES (Advanced Encryption Standard)	Vom National Institute of Standards and Technology (NIST) genehmigte Standards. In der Regel werden diese in den nächsten 20 bis 30 Jahren verwendet.
AKEP (Authentication Key Exchange Protocol)	Übertragung von Schlüsseln auf der Grundlage symmetrischer Verschlüsselung. Damit können zwei Parteien einen gemeinsam genutzten geheimen Schlüssel austauschen, der gegenüber passiven Gegnern geschützt ist.
Algorithmus (Hash)	Eine Reihe von mathematischen (logischen) Regeln, die für die Erstellung von Nachrichtenkernen und die Erzeugung von Schlüsseln / Unterschriften verwendet werden.
Algorithmus (Verschlüsselung)	Eine Reihe von mathematischen (logischen) Regeln, die für die Verschlüsselung und Entschlüsselung verwendet werden.
Anonymität	Ursprung oder Autor der Informationen ist unbekannt oder nicht angegeben, so daß die Identität des Erstellers / Absenders nicht herausgefunden werden kann.
ANSI (American National Standards Institute)	Entwickelt Standards über verschiedene akkreditierte Normen-Gremien (Accredited Standards Committee; ASC). Das X9-Komitee beschäftigt sich vorwiegend mit Sicherheitsstandards für Finanzdienstleistungen.
API (Application Programming Interface)	Schafft die Voraussetzungen für die Nutzung von Software-Funktionen, indem das Zusammenwirken von verschiedenen Software-Produkten ermöglicht wird.
ASN. 1 (Abstract Syntax Notation One)	ISO / IEC-Standard für Codierungsvorschriften, die in ANSI X. 509-Zertifikaten verwendet werden. Es existieren zwei Typen: Distinguished Encoding Rules (DER) und Basic Encoding Rules (BER).
Asymmetrische Schlüssel	Ein zwar separates, jedoch integriertes Benutzerschlüsselpaar, bestehend aus einem öffentlichen und einem privaten Schlüssel. Es handelt sich dabei um Einwegschlüssel, d. h. ein Schlüssel, der zur Verschlüsselung bestimmter Daten verwendet wurde, kann nicht zur Entschlüsselung derselben Daten benutzt werden.

Authentisierung	Prüfen der Echtheit durch Bestätigung der Identität eines Benutzers.
Beglaubigungsnachweis	Liefert die Basis für Vertrauen oder Glaubwürdigkeit.
Bevollmächtigung	Übertragen von offiziellen Genehmigungen, Zugriffsrechten oder juristischen Vollmachten an einen Benutzer.
Blankounterschrift	Möglichkeit zum Unterschreiben von Dokumenten ohne Kenntnis des Inhalts, ähnlich wie bei zur Beglaubigung von Dokumenten berechtigten öffentlichen Stellen.
Blockchiffrierer	Ein symmetrischer Chiffriercode, der auf der Basis von Blöcken (in der Regel 64-Bit-Blöcke) von Klartext und verschlüsseltem Text funktioniert.
Blowfish	Ein symmetrischer 64-Bit-Blockchiffrierer, der aus Schlüsselerweiterung und Datenverschlüsselung besteht. Ein frei zugänglicher, schneller, einfacher und kompakter Algorithmus, der von Bruce Schneier entwickelt wurde.
CA (Certificate Authority)	Ein vertrauenswürdiger Dritter (Trust Third- Party; TTP), der Zertifikate mit Beurteilungen über verschiedene Attribute erstellt und diese einem Benutzer und / oder dem zugehörigen öffentlichen Schlüssel zuordnet.
CAPI (Crypto API)	Die kryptographische API von Microsoft für Windows-basierte Betriebssysteme und Anwendungen.
Capstone	Ein vom NSA (National Security Agency) entwickelter kryptographischer Chip, der die Möglichkeit einer Schlüsselhinterlegung bei der US-Regierung implementiert.
CAST	Ein 64-Bit-Blockchiffrierer, der 64-Bit-Schlüssel, sechs S-Boxen mit 8-Bit-Eingabe und 32-Bit-Ausgabe verwendet. Er wurde in Kanada von Carlisle Adams und Stafford Tavares entwickelt.
CBC (Cipher Block Chaining)	Der Prozeß des Anwendens des XOR-Operators, um Klartext mit dem vorherigen chiffrierten Textblock in eine Entweder-Oder-Beziehung zu bringen, bevor dieser verschlüsselt wird. So wird einem Blockchiffrierer ein Rückkopplungsmechanismus hinzugefügt.
CDK (Crypto Developer Kit)	Eine dokumentierte Umgebung mit einer API für Dritte zum Schreiben von sicheren Anwendungen unter Verwendung einer kryptographischen Bibliothek eines bestimmten Anbieters.

CDSA (Common Data Security Architecture)
Dieses System wurde von Intel Architecture Labs (IAL) entwickelt, um Datensicherheitsprobleme im Internet und Intranet zu lösen, die in Internetprodukten von Intel und anderen Anbietern auftreten.

CERT (Computer Emergency Response Team)
Sicherheits-Dokumentationsstelle zur Förderung eines Sicherheitsbewußtseins. CERT bietet rund um die Uhr technische Unterstützung bei Vorfällen an, die die Sicherheit von Computern und Netzwerken betreffen. CERT hat seinen Sitz in Pittsburgh, PA, im Software Engineering Institute der Carnegie Mellon University.

CFM (Cipher Feedback Mode)
Ein Blockchiffrierer, der als selbstsynchronisierender Stromchiffriercode implementiert wurde.

CHAP (Challenge Authentication Protocol)
Ein zweiseitiges Paßwort-Authentisierungssystem auf Sitzungsgrundlage.

Chiffrierter Text
Das Ergebnis der Veränderung von Buchstaben oder Bits durch Ersetzung, Vertauschung oder beides.

Cookie
Benutzerdaten-Cookie (Persistent Client State HTTP Cookie). Eine Datei oder ein Token, die / der vom Web-Server an den Web-Client (Ihren Browser) übertragen wird. Er dient zu Ihrer Identifizierung und kann persönliche Daten aufzeichnen, wie beispielsweise die Benutzer-ID und das Paßwort, die E-Mail-Adresse, die Kreditkartennummer und andere Informationen.

CRAB
Ein 1024-Byte-Blockchiffrierer (ähnlich MD5), die Verfahren von einer Einweg-Hash-Funktion verwendet. Er wurde in den RSA Laboratories von Burt Kaliski und Matt Robshaw entwickelt.

CRL (Certificate Revocation List)
Eine aktualisierte Online-Liste mit älteren, nicht mehr gültigen Zertifikaten.

CRYPTOKI
Entspricht PKCS #11.

Datenintegrität
Ein Verfahren zum Prüfen, ob Informationen noch im Ursprungszustand vorliegen und nicht durch Unbefugte oder auf unbekannte Weise verändert wurden.

DES (Data Encryption Standard; Datenverschlüsselungsstandard)
Ein 64-Bit-Blockchiffrierer oder symmetrischer Algorithmus, der auch als Data Encryption Algorithm (DEA) (vom ANSI) bzw. DEA-1 (von der ISO) bezeichnet wird. Seit über 20 Jahren weit verbreitet, 1976 übernommen als „FIPS 46“.

Diffie-Hellman	Der erste Verschlüsselungsalgorithmus für öffentliche Schlüssel, der diskrete Logarithmen in einem endlichen Feld verwendete. Er wurde 1976 erfunden.
Digitale Unterschrift	Eine elektronische Identifizierung eines Benutzers oder eines Gegenstandes, die mit einem Verschlüsselungsalgorithmus für öffentliche Schlüssel erstellt wurde. Dient der Verifizierung der Datenintegrität und der Identität des Absenders der Daten durch den Empfänger.
Direktes Vertrauen	Schaffung von Vertrauen auf gegenseitiger Basis.
Diskreter Logarithmus	Das in asymmetrischen Algorithmen verwendete zugrundeliegende mathematische Prinzip, beispielsweise bei Diffie-Hellman und bei der Verschlüsselung mittels elliptischer Kurven. Es handelt sich um die Umkehrung des Problems der modularen Potenzierung (eine Einweg-Funktion).
DMS (Defense Messaging System)	Vom US-Verteidigungsministerium herausgegebene Standards zur Gewährleistung einer sicheren und zuverlässigen abteilungsübergreifenden Nachrichteninfrastruktur für Regierungsbehörden und militärische Einrichtungen.
DNSSEC (Domain Name System Security Working Group)	IETF-Entwurf hinsichtlich Verbesserungen am DNS-Protokoll zum Schutz des DNS gegen unbefugte Datenmanipulationen und gegen Verschleierung der Datenherkunft. Das DNS soll durch digitale Unterschriften eine erhöhte Datenintegrität und weitere Kapazitäten für die Authentisierung erhalten.
DSA (Digital Signature Algorithm)	Ein vom NIST entworfener digitaler Unterschriftenalgorithmus für öffentliche Schlüssel zur Verwendung in DSS.
DSS (Digital Signature Standard)	Ein vom NIST vorgeschlagener Standard (FIPS) für digitale Unterschriften unter Verwendung des DSA.
ECC (Elliptic Curve Cryptosystem)	Ein eindeutiges Verfahren zur Erstellung von Verschlüsselungsalgorithmen für öffentliche Schlüssel auf der Grundlage von mathematischen Kurven in endlichen Feldern oder mit großen Primzahlen.
EDI (Electronic Data Interchange)	Der direkte, standardisierte Austausch von Geschäftsdokumenten (Warenbestellungen, Rechnungen, Zahlungen, Inventaranalysen usw.) zwischen den Computern Ihres Unternehmens und denen Ihrer Lieferanten bzw. Kunden.
EES (Escrowed Encryption Standard)	Eine von der Regierung der USA vorgeschlagene Norm zur Hinterlegung privater Schlüssel.

Einfachfilter Eine Funktion zur Ausführung einer einzelnen Umformungsoperation an einer Eingabemenge. Das Ergebnis ist eine Ausgabemenge mit nur den Werten der Eingabemenge, die die Umformungsbedingungen erfüllen. Beispiel: Eine Suchfunktion, die jeweils nur eine Zeichenkette akzeptiert und eine Liste mit Zeilennummern ausgibt, in der die Zeichenkette gefunden wurde.

Einmalige Anmeldung Durch eine einzige Anmeldung wird der Zugang auf alle Ressourcen des Netzwerks möglich.

Einweg-Hash Eine Funktion einer variablen Zeichenfolge zum Erstellen eines Wertes mit fester Länge, der das ursprüngliche Abbild darstellt. Wird auch Nachrichtenkern, Fingerabdruck und Message Integrity Check (MIC) genannt.

Elektronisches Geld Geld in elektronischer Form, das über eine Vielzahl von komplexen Protokollen gespeichert und übertragen wird.

Elgamal-Schema Wird für digitale Unterschriften und zur Verschlüsselung auf der Basis von diskreten Logarithmen in einem endlichen Feld verwendet. Kann mit der DAS-Funktion kombiniert werden.

Entropie Ein mathematisches Maß für den Grad der Ungewißheit über den Ausgang eines Versuchs.

Entschlüsselung Der Prozeß des Rückumwandelns von chiffriertem (verschlüsseltem) Text in Klartext.

Ersetzungschiffriercode Die Zeichen des Klartextes werden durch andere Zeichen ersetzt, so daß chiffrierter Text entsteht.

FEAL Ein Blockchiffrierer, der einen 64-Bit-Block und einen 64-Bit-Schlüssel verwendet. Wurde von A. Shimizu und S. Miyaguchi von NTT Japan entwickelt.

Filter Eine Funktion, eine Gruppe von Funktionen oder eine Kombination von Funktionen zur Ausführung von Umformungsoperationen an einer Eingabemenge. Das Ergebnis ist eine Ausgabemenge mit nur den Werten der Eingabemenge, die die Umformungskriterien erfüllen. An diesen Werten können in der Ergebnismenge eventuell noch weitere Umformungsoperationen ausgeführt werden. Ein Beispiel hierfür ist eine Suchfunktion, die mehrere Zeichenfolgen akzeptiert, die in einer bestimmten Booleschen Beziehung zueinander stehen. Optional kann für die gefundenen Zeichenfolgen in der Ergebnisausgabemenge Groß- bzw. Kleinschreibung erzwungen werden.

Fingerabdruck
Eine eindeutige Kennung für einen Schlüssel, die über eine Hash-Funktion aus bestimmten Teilen der Schlüsseldaten errechnet wird.

FIPS (Federal Information Processing Standard)
Eine vom NIST veröffentlichte Norm der Regierung der USA.

Firewall
Eine Kombination aus Hardware und Software zum Schutz des öffentlichen / privaten Netzwerks gegen bestimmte Angriffe von außen zur Gewährleistung eines bestimmten Maßes an Sicherheit.

GAK (Government Access to Keys)
Ein Verfahren, das der Regierung die Hinterlegung der privaten Schlüssel von Personen ermöglicht.

Gegenseitige Zertifizierung
Zwei oder mehrere Organisationen oder Zertifizierungsinstanzen, die ein gewisses Maß an gegenseitigem Vertrauen besitzen.

Geheimer Schlüssel
Entweder der „private Schlüssel“ in (asymmetrischen) Verschlüsselungsalgorithmen für öffentliche Schlüssel oder der „Sitzungsschlüssel“ in symmetrischen Algorithmen.

Gost
Ein in der ehemaligen Sowjetunion entwickelter, symmetrischer 64-Bit-Blockchiffrierer, der einen 256-Bit-Schlüssel verwendet.

GSS-API (Generic Security Services API)
Eine Sicherheits-API höchster Ebene auf der Basis von IETF RFC 1508, die sitzungsorientierte Anwendungscodes von Implementierungsdetails isoliert.

Gültigkeitsprüfung
Gewährleistet die rechtzeitige Autorisierung, Informationen oder Ressourcen verwenden oder bearbeiten zu können.

Hash-Funktion
Eine Einweg-Hash-Funktion ist eine Funktion, die einen Nachrichtenkern erzeugt, der zur Erzeugung des Originals nicht umgekehrt werden kann.

HMAC
Eine schlüsselabhängige Einweg-Hash-Funktion, die speziell für die Verwendung mit MAC (Message Authentication Code) gedacht ist und auf IETF RFC 2104 basiert.

HTTP (HyperText Transfer Protocol)
Ein Protokoll zum Übertragen von Dokumenten zwischen Servern oder von einem Server zu einem Client.

IDEA (International Data Encryption Standard)
Ein symmetrischer 64-Bit-Blockchiffrierer unter Verwendung von 128-Bit-Schlüsseln. Er basiert auf dem Konzept, Vorgänge aus verschiedenen algebraischen Gruppen zu mischen. Wird als einer der wirksamsten Algorithmen angesehen.

Identitätszertifikat
Eine unterschriebene Aussage, die einen Schlüssel mit dem Namen einer Person verknüpft. Sie dient zur Übertragung von Vollmachten dieser Person an den öffentlichen Schlüssel.

IETF (Internet Engineering Task Force)
Eine umfangreiche offene internationale Gemeinschaft, bestehend aus Netzwerk-Entwicklern, Betreibern, Händlern und Forschungsspezialisten, deren Aufgabe die Entwicklung der Internetarchitektur und des reibungslosen Betriebs des Internets ist. Eine Mitarbeit steht jedem Interessenten offen.

Initialisierungsvektor (IV)
Ein Block aus willkürlichen Daten, der unter Verwendung eines „Chaining Feedback Mode“ (siehe „Cipher Block Chaining“) als Ausgangspunkt für einen Blockchiffrierer dient.

Integrität
Ein Beleg dafür, daß Daten bei der Speicherung oder Übertragung (durch unbefugte Personen) nicht verändert werden.

IPsec
Ein von der IETF in Erwägung gezogenes Verschlüsselungssystem auf TCP / IP-Ebene.

ISA/KMP (Internet Security Association, Key Mgt. Protocol)
Definiert die Prozeduren zur Authentisierung eines Kommunikationspartners, zur Aufstellung und Verwaltung von Sicherheitsvereinigungen, Verfahren zur Schlüsselerzeugung und zur Abwendung von Gefahren (z.B. Verweigerung von Diensten oder Abfangangriffe).

ISO (International Organization for Standardization)
Diese Organisation ist für eine Vielzahl von Normen verantwortlich, wie das OSI-Modell sowie internationale Beziehungen mit dem ANSI bezüglich X. 509.

ITU-T (International Telecommunication Union-Telecommunication)
Nichtoffizielle Bezeichnung für das CCITT (Consultative Committee for International Telegraph and Telephone), eine weltweite Organisation zur Standardisierung von Telekommunikationsverfahren.

Kerberos
Ein vom MIT entwickeltes Authentisierungsprotokoll für vertrauenswürdige Dritte (TTP).

Klartext
Daten oder Nachrichten in einer für den Menschen lesbaren Form vor dem Verschlüsseln (auch unverschlüsselter Text genannt).

Kryptoanalyse
Die Kunst oder Wissenschaft des Konvertierens von chiffriertem Text in Klartext ohne anfängliche Kenntnis des für die Verschlüsselung des Textes verwendeten Schlüssels.

Kryptographie
Die Kunst und Wissenschaft des Erstellens von Nachrichten, die eine beliebige Kombination der Attribute „vertraulich“, „unterschrieben“, „unverändert“ mit Urheberrechtsnachweis aufweisen.

LDAP (Lightweight Directory Access Protocol)
Ein einfaches Protokoll zur Unterstützung von Zugriff und Suchvorgängen in Verzeichnissen mit Informationen, wie beispielsweise Namen, Telefonnumnmern und Adressen in sonst inkompatiblen Systemen über das Internet.

Lexikalischer Abschnitt
Ein bestimmter Teil einer Nachricht, der eine bestimmte Datenklasse enthält, beispielsweise freigegebene Daten, verschlüsselte Daten oder Schlüsseldaten.

MAA (Message Authenticator Algorithm)
Eine ISO-Norm zur Erzeugung eines 32-Bit-Hash für IBM-Mainframes.

MAC (Message Authentication Code)
Eine schlüsselabhängige Einweg-Hash-Funktion, bei der zur Verifizierung des Hash der identische Schlüssel benötigt wird.

MD2 (Message Digest 2)
Eine von einer Zufallspermutation von Bytes abhängige Einweg-Hash-Funktion mit 128 Bit. Sie wurde von Ron Rivest entwickelt.

MD4 (Message Digest 4)
Eine Einweg-Hash-Funktion mit 128 Bit, in der ein einfacher Satz von Bit-Manipulationen mit 32-Bit-Operanden verwendet wird. Sie wurde von Ron Rivest entwickelt.

MD5 (Message Digest 5)
Eine verbesserte, komplexere Version von MD4. Es handelt sich jedoch immer noch um eine Einweg-Hash-Funktion mit 128 Bit.

MIC (Message Integrity Check)
Wurde anfangs in PEM zur Authentisierung mittels MD2 oder MD5 definiert. Micalg (Message Integrity Calculation) wird in sicheren MIME-Anwendungen eingesetzt.

MIME (Multipurpose Internet Mail Extensions)
Eine frei verfügbare Menge von Spezifikationen, mit denen Text in Sprachen mit verschiedenen Zeichensätzen sowie Multimedia-E-Mails zwischen vielen verschiedenen Computer-Systemen mit Internet-E-Mail-Standards ausgetauscht werden können.

MMB (Modular Multiplication-based Block)
Dieser von Joan Daemen entwickelte, symmetrische Algorithmus unter Verwendung von 128-Bit-Schlüsseln / 128-Bit-Blöcken basiert auf IDEA. Er wird aufgrund seiner Schwachstellen bei einer linearen Kryptoanalyse nicht verwendet.

MOSS (MIME Object Security Service)
Wird in RFC 1848 definiert. Dient zur Erleichterung der Verschlüsselungs- und Unterschriftendienste für MIME, einschließlich Schlüsselverwaltung auf der Grundlage asymmetrischer Verfahren (wenig verbreitet).

MSP (Message Security Protocol)
Das Gegenstück zu PEM für militärische Zwecke, ein X. 400-kompatibles Protokoll auf Anwendungsebene zur Sicherung von E-Mail-Nachrichten. Wurde vom NSA Ende der 80er Jahre entwickelt.

MTI
Ein Einweg-Schlüsselvereinbarungsprotokoll von Matsumoto, Takashima und Imai zur gegenseitigen Authentisierung von Schlüsseln ohne Schlüsselüberprüfung oder Authentisierung von Benutzern.

Nachrichtenkern
Ein aus einer Nachricht abgeleiteter Wert. Wenn Sie einen Buchstaben in der Nachricht ändern, ergibt die Nachricht einen anderen Nachrichtenkern.

NAT (Network Address Translator)
RFC 1631, ein Router zur Verbindung zweier Netzwerke. Das als inneres Netzwerk bezeichnete Netzwerk verfügt über private oder veraltete Adressen, die in gültige Adressen umgewandelt werden müssen, bevor Pakete an das andere (äußere) Netzwerk weitergeleitet werden.

NIST (National Institute for Standards and Technology)
Eine Abteilung des „U. S. Department of Commerce“ (Wirtschaftsministerium der USA). Veröffentlicht Normen bezüglich der Kompatibilität (FIPS).

Oakely
Der „Oakley Session Key Exchange“ (Oakley-Sitzungsschlüsselaustausch) ermöglicht einen hybriden Diffie-Hellman-Sitzungsschlüsselaustausch, der im ISA/KMP-Rahmen verwendet werden kann. Oakley hat die wichtige Eigenschaft der „perfekten vorwärts-Sicherheit“.

Öffentlicher Schlüssel
Die öffentlich verfügbare Komponente eines integrierten asymmetrischen Schlüsselpaares, die oft als Verschlüsselungsschlüssel bezeichnet wird.

One-Time-Pad
Eine zur Verschlüsselung verwendete große Menge von echten Zufalls-Schlüsselbuchstaben ohne Wiederholungen. Gilt als einziges perfektes Verschlüsselungssystem. Wurde 1917 von Major J. Mauborgne und G. Vernam erfunden.

Orange Book
Das vom National Computer Security Center herausgegebene Buch mit dem Titel „Department of Defense Trusted Computer Systems Evaluation Criteria“, in dem Sicherheitsanforderungen definiert werden.

PAP (Password Authentication Protocol)
Ein Authentisierungsprotokoll, mit dem PPP-Benutzer sich gegenseitig authentisieren können. Allerdings werden unbefugte Zugriffe nicht verhindert, sondern der Benutzer am entfernten Ende wird lediglich identifiziert.

Paßphrase
Eine einprägsame Wortgruppe, die eine höhere Sicherheit als ein einzelnes Paßwort gewährleistet. Durch „Verwürfeln“ von Schlüsseln wird sie in einen Zufallsschlüssel umgewandelt.

Paßwort
Eine Zeichenfolge oder ein Wort, die oder das eine Person zur Authentisierung, Überprüfung oder Verifizierung in ein System eingibt.

PCT (Private Communication Technology)
Ein von Microsoft und Visa entwickeltes Protokoll zur sicheren Kommunikation im Internet.

PEM (Privacy Enhanced Mail)
Ein Protokoll für sichere Internet-E-Mail-Nachrichten (RFC 1421-1424). Es enthält Dienste zur Verschlüsselung, Authentisierung, Nachrichtenintegrität und Schlüsselverwaltung. PEM verwendet ANSI X. 509-Zertifikate.

Perfekte vorwärts-Sicherheit
Ein Verschlüsselungssystem, bei dem der chiffrierte Text keinerlei Informationen über den Klartext liefert. Es können höchstens Angaben über die Länge enthalten sein.

PGP/MIME
Eine IETF-Norm (RFC 2015) zur Geheimhaltung und Authentisierung unter Verwendung der in RFC1847 erläuterten MIME-Sicherheitsinhaltstypen (Multipurpose Internet Mail Extensions; MIME). PGP / MIME wird momentan in PGP 5.0 und späteren Versionen verwendet.

PKCS (Public Key Crypto Standards)
Eine Reihe von De-facto-Normen zur Verschlüsselung mit öffentlichen Schlüsseln, die in Zusammenarbeit mit einem informellen Konsortium (Apple, DEC, Lotus, Microsoft, MIT, RSA und Sun) entwickelt wurden. Dazu gehören algorithmen-spezifische und von Algorithmen unabhängige Implementierungsnormen. Spezifikationen zur Definition von Nachrichtensyntax und anderen Protokollen, die von RSA Data Security, Inc., gesteuert werden.

PKI (Public Key Infrastructure)
Ein weitverbreitetes und zugängliches Zertifikatssystem zum Erhalt von öffentlichen Schlüsseln eines Benutzers, bei dem Sie bis zu einem gewissen Grad sicher sein können, daß Sie den „richtigen“ Schlüssel erhalten haben und daß dieser nicht zurückgenommen wurde.

Pretty Good Privacy (PGP)

Anwendung und Protokoll (RFC 1991) zur Gewährleistung von sicheren E-Mails und zur Dateiverschlüsselung. Wurde von Phil R. Zimmermann entwickelt und zuerst als Freeware veröffentlicht. Der Quellcode stand der Öffentlichkeit schon immer zur Analyse zur Verfügung. PGP verwendet eine Vielzahl von Algorithmen, wie beispielsweise IDEA, RSA, DSA, MD5 und SHA-1, zur Verschlüsselung, Authentisierung, Nachrichtenintegrität und Schlüsselverwaltung. PGP basiert auf dem „Web-of-Trust"-Modell und ist weltweit verbreitet.

Privater Schlüssel

Die im privaten Besitz befindliche „geheime" Komponente eines integrierten asymmetrischen Schlüsselpaares, die oft als Entschlüsselungsschlüssel bezeichnet wird.

Pseudo-Zufallszahl

Eine Zahl, die aus dem Anwenden von Algorithmen zur Erzeugung von Zufallswerten auf aus der Computerumgebung abgeleitete Eingabewerte errechnet wird (z.B. Mauskoordinaten). Siehe „Zufallszahl".

RADIUS (Remote Authentication Dial-In User Service)

Ein (von Livingston Enterprise entwickeltes) IETF-Protokoll zur Verteilung von Sicherheit, mit dem entfernte Zugriffe auf Netzwerke und Netzwerkdienste gegen unbefugten Zugriff gesichert werden. RADIUS setzt sich aus zwei Bestandteilen zusammen, dem Server-Code zur Authentisierung und aus Client-Protokollen.

RC2 (Rivest Cipher 2)

Symmetrischer 64-Bit-Blockchiffrierer mit variabler Schlüsselgröße, ein brancheninterner Schlüssel von RSA, SDI.

RC4 (Rivest Cipher 4)

Stromchiffriercode mit variabler Schlüsselgröße, war früher Eigentum von RSA Data Security, Inc.

RC5 (Rivest Cipher 5)

Ein Blockchiffrierer mit einer Vielzahl von Argumenten, einer Blockgröße, einer Schlüsselgröße und einer Anzahl von Durchläufen.

REDOC

Ein von M. Wood entwickelter, in den USA patentierter Blockchiffrier-Algorithmus, der einen 160-Bit-Schlüssel und einen 80-Bit-Block verwendet.

RFC (Request for Comment)

Ein IETF-Dokument, aus der Untergruppe FYI RFC (geben Überblicke und Einführungen) oder aus der Untergruppe STD RFC (geben Internet-Normen an). Die Abkürzung FYI steht für „For Your Information" (Zu Ihrer Information). Jede RFC hat zur Indizierung eine RFC-Nummer, anhand deren er abgerufen werden kann (www. ietf. org).

RIPE-MD

Ein für das RIPE-Projekt der EU entwickelter Algorithmus. Er kann von den bekannten Kryptoanalysen nicht entschlüsselt werden und erzeugt einen Hash-Wert von 128 Bit, eine Variante von MD4.

ROT-13 (Rotation Cipher)

Ein einfacher Ersetzungsverschlüsselungscode (Cäsar-Verschlüsselungscode), bei dem alle 26 Buchstaben um 13 Stellen verschoben werden.

RSA

Abkürzung von RSA Data Security, Inc. Steht auch für die Firmenchefs Ron Rivest, Adi Shamir und Len Adleman oder bezieht sich auf den von ihnen erfundenen Algorithmus. Der RSA-Algorithmus wird in der Kryptographie mit öffentlichen Schlüsseln verwendet. Seine Funktionsweise beruht auf der Tatsache, daß zwei große Primzahlen zwar leicht miteinander zu multiplizieren sind, aber das Produkt nur schwer wieder in sie zu zerlegen ist.

S/MIME (Secure Multipurpose Mail Extension)

Ein von Deming Software und RSA Data Security entwickelter Normvorschlag zum Verschlüsseln und/oder zur Authentisierung von MIME-Daten. S/MIME definiert ein Format für die MIME-Daten, für die zur Abstimmung der Kommunikationssysteme erforderlichen Algorithmen (RSA, RC2, SHA-1) und für die weiteren Betriebsfragen, wie beispielsweise ANSI X. 509-Zertifikate sowie die Übertragung über das Internet.

S/WAN (Secure Wide Area Network)

Von RSA Data Security, Inc., bereitgestellte Spezifikationen für die Implementierung von IPsec zur Gewährleistung der Kompatibilität von Firewall- und TCP/IP-Produkten. Das Ziel von S/WAN ist es, IPsec zu verwenden, so daß Unternehmen eine Kombination und Anpassung von Firewall- und TCP/IP-Stapelprodukten ermöglichen, um virtuelle private Netzwerke (Virtual Private Networks; VPNs) auf Internet-Basis zu erstellen.

SAFER (Secure And Fast Encryption Routine)

Ein Blockchiffrier-Algorithmus mit einem 64-Bit-Schlüssel. Dieser Algorithmus wurde nicht patentiert und ist lizenzfrei verfügbar. Er wurde von Massey entwickelt, der auch IDEA entwickelte.

Salt

Eine zufällige Zeichenkette, die mit Paßwörtern (oder Zufallszahlen) verknüpft wird, bevor an ihnen mit einer Einweg-Funktion Operationen durchgeführt werden. Durch diese Verkettung wird das Paßwort effektiv verlängert und verfremdet. Damit ist der chiffrierte Text besser gegen Wörterbuchangriffe geschützt.

Schlüssel

Ein Mittel zur Gewährung bzw. Verweigerung von Zugriff, Eigentumsrechten oder Steuerungsbefugnissen. Wird durch eine beliebige, große Anzahl von Werten dargestellt.

Schlüsselaufteilung Ein Verfahren zum Aufteilen von Schlüsselteilen auf mehrere Parteien, von denen keine die Fähigkeit zur Wiederherstellung des gesamten Schlüssels hat.

Schlüsselaustausch Ein Schema mit zwei oder mehreren Knoten zum Übertragen eines geheimen Sitzungsschlüssels über einen nicht gesicherten Kanal.

Schlüsselhinterlegung/-wiederherstellung Ein Verfahren, das Dritten das Abrufen von zur Geheimhaltung von Daten verwendeten kryptographischen Schlüsseln ermöglicht, um letztendlich die verschlüsselten Daten wiederherzustellen.

Schlüssellänge Die Anzahl der Bits zur Darstellung der Schlüsselgröße. Je länger der Schlüssel, desto stärker ist er.

Schlüsselverwaltung Das Verfahren zum sicheren Speichern und Verteilen akkurater kryptographischer Schlüssel. Der Gesamtprozeß des sicheren Erstellens und Verteilens von kryptographischen Schlüsseln an befugte Empfänger.

SDSI (Simple Distributed Security Infrastructure) Ein neuer PKI-Vorschlag von Ronald L. Rivest (MIT) und Butler Lampson (Microsoft). Er bietet eine Methode zum Definieren von Gruppen und Verleihen der Gruppenmitgliedschaft sowie von Zugriffssteuerungslisten und Sicherheitsrichtlinien. Im Mittelpunkt von SDSI steht nicht ein hierarchischer globaler Namensraum, sondern verknüpfte lokale Namensräume.

SEAL (Software-optimized Encryption ALgorithm) Ein von Rogaway und Coppersmith entwickelter schneller Stromchiffriercode für 32-Bit-Rechner.

Selbstunterschriebener Schlüssel Ein öffentlicher Schlüssel, der vom entsprechenden privaten Schlüssel zum Nachweis des Eigentumsrechts unterschrieben wurde.

SEPP (Secure Electronic Payment Protocol) Eine frei zugängliche Spezifikation für sichere Geldkarten-Transaktionen über das Internet. Sie wurde von IBM, Netscape, GTE, Cybercash und MasterCard entwickelt.

SESAME (Secure European System for Applications in a Multi-vendor Environment) Europäisches Forschungs- und Entwicklungsprojekt, das Kerbros durch Hinzufügen von Bevollmächtigungs- und Zugriffsdiensten weiterentwickelt hat.

SET (Secure Electronic Transaction) Dient der sicheren Übertragung von Kreditkartennummern über das Internet.

SHA-1 (Secure Hash Algorithm)
Die 1994 vorgenommene Überarbeitung des vom NIST entwickelten SHA (FIPS 180-1). SHA-1 wird zusammen mit DSS zur Erzeugung eines 160-Bit-Hash verwendet. Es ähnelt dem sehr beliebten und weitverbreiteten MD4.

Sicherer Kanal
Ein Mittel zur Übertragung von Informationen zwischen Terminals, bei der kein Gegner diese Informationen umstellen, löschen, lesen oder andere Informationen einfügen kann (SSL, IPsec, „Ins-Ohr-Flüstern“).

Sitzungsschlüssel
Der geheime (symmetrische) Schlüssel zum Verschlüsseln aller Datensätze auf Transaktionsbasis. Für jede Kommunikationssitzung wird ein anderer Sitzungsschlüssel verwendet.

SKIP (Simple Key for IP)
Eine einfache, von Sun Microsystems, Inc., entwickelte Schlüsselverwaltung für Internet-Protokolle.

Skipjack
Der im Clipper-Chip des NSA enthaltene Verschlüsselungsalgorithmus mit einem 80-Bit-Schlüssel

SKMP (Secure key Management Protocol)
Eine von IBM entworfene Schlüsselwiederherstellungsarchitektur unter Verwendung eines Schlüsselverschlüsselungsverfahrens, der eine Schlüssel- und Nachrichtenwiederherstellung durch einen vertrauenswürdigen Dritten ermöglicht, bei dem der Schlüssel hinterlegt wird.

SNAPI (Secure Network API)
Eine von Netscape zur Verfügung gestellte API für Sicherheitsdienste zum Schutz von Ressourcen vor unbefugten Benutzern, zur Kommunikationsverschlüsselung und -authentisierung sowie zur Verifizierung der Informationsintegrität.

SPKI (Simple Public Key Infrastructure)
IETF-Normentwurf von Ellison, Frantz und Thomas. Format für Zertifikate für öffentliche Schlüssel, zugehörige Unterschrift und andere Formate sowie Schlüsselerfassungsprotokoll. Wurde vor kurzem mit dem SDSI-Entwurf von Ron Rivest zusammengeführt.

SSH (Secure Shell)
Ein vom IETF empfohlenes Protokoll zur Sicherung der Übertragungsebene durch Verschlüsselung, kryptographische Host-Authentisierung und Integritätsschutz.

SSH (Site Security Handbook)
Die Working Group (WG) der IETF arbeitet seit 1994 an der Erstellung von Dokumenten zum Vermitteln von Sicherheitsinformationen an Internet-Nutzer. Das erste Dokument ist eine vollständige Überarbeitung von RFC 1244. Es richtet sich an System- und Netzwerkadministratoren und ist bei der Entscheidungsfindung behilflich (mittlere Führungsebene).

SSL (Secure Socket Layer)

Wurde von Netscape zur Gewährleistung von Sicherheit und zur Geheimhaltung im Internet entwickelt. SSL unterstützt die Server- und Client-Authentisierung und gewährleistet die Sicherheit und Integrität des Übertragungskanals. Wirkt auf der Übertragungsebene und dient als „Socket-Bibliothek", wodurch eine anwendungsunabhängige Wirkungsweise ermöglicht wird. Verschlüsselt den gesamten Kommunikationskanal und unterstützt keine digitalen Unterschriften auf Nachrichtenebene.

STT (Secure Transaction Technology)

Ein von Microsoft und Visa entwickeltes sicheres Zahlungsprotokoll als Begleitprodukt zum PCT-Protokoll.

Stromchiffriercode

Eine Klasse der symmetrischen Schlüsselverschlüsselung, bei der die Umwandlung für jedes zu verschlüsselnde Symbol des Klartextes geändert werden kann. Wird für Umgebungen mit geringer Speicherkapazität zum Puffern von Daten empfohlen.

STU-III (Secure Telephone Unit)

Ein vom NSA entwickeltes Telefon für sichere Sprach- und langsame Datenübertragungen für das US-Verteidigungsministerium und seine Vertragsnehmer.

Symmetrischer Algorithmus

Wird auch als konventioneller, geheimer Schlüssel- oder Einzelschlüsselalgorithmus bezeichnet. Der Verschlüsselungsschlüssel ist entweder mit dem Entschlüsselungsschlüssel identisch, oder ein Schlüssel kann aus dem anderen abgeleitet werden. Es gibt zwei Unterkategorien – Block und Strom.

TACACS+ (Terminal Access Controller Access Control System)

Ein Protokoll zur Authentisierung von entfernten Zugriffen, zur Bevollmächtigung und für zugehörige Konto- und Anmeldedienste. Wird von Cisco Systems verwendet.

TLS (Transport Layer Security)

Ein IETF-Entwurf. Version 1 basiert auf Version 3.0 des SSL-Protokolls (Secure Sockets Layer; SSL) und dient zur Wahrung der Privatsphäre bei der Kommunikation über das Internet.

TLSP (Transport Layer Security Protocol)

ISO 10736, Entwurf des internationalen Standards.

Transpositionschiffriercode

Der Klartext bleibt erhalten, lediglich die Reihenfolge der Buchstaben wird verändert.

Triple-DES

Eine Verschlüsselungskonfiguration, in der der DES-Algorithmus dreimal mit drei unterschiedlichen Schlüsseln verwendet wird.

TTP (Trust Third-Party)
Eine verantwortungsbewußte Gruppe, in der alle Mitglieder im voraus vereinbaren, einen Dienst anzubieten oder eine Funktion zu erfüllen, wie beispielsweise die Zertifizierung durch Zuordnen eines öffentlichen Schlüssels zu einem Benutzer / einer Benutzergruppe, das Setzen von Zeitmarkierungen oder die Schlüsselhinterlegung.

UEPS (Universal a Electronic Payment System)
Ein für Südafrika entwickeltes Banking-Programm auf der Basis der Smart-Card (einer sicheren Geldkarte), da in Südafrika wegen der schlechten Telefonqualität keine Online-Verifizierung möglich ist.

Unverschlüsselter Text (oder Klartext)
Daten oder Nachrichten in einer für den Menschen lesbaren Form vor dem Verschlüsseln.

Urheberrechtsnachweis
Verhindert die Verweigerung von früheren Verpflichtungen oder Leugnung von Handlungen.

Verifizierung
Dient zur Authentisierung bzw. zur Bestätigung der Genauigkeit.

Verschlüsselung
Das Verfahren zum Verschlüsseln einer Nachricht, so daß deren Inhalt verhüllt bleibt.

Verschlüsselungssystem
Ein System, das aus kryptographischen Algorithmen, beliebigem Klartext, chiffriertem Text und Schlüsseln besteht.

Vertrauen
Die feste Überzeugung von der Ehrlichkeit, Integrität, Rechtschaffenheit und / oder Zuverlässigkeit einer Person, einer Firma oder einer anderen Personengruppe.

Vertrauenshierarchie
Benutzer auf verschiedenen Ebenen, die Vertrauen auf organisierte Weise verteilen. Häufig in ANSI X. 509 zum Verteilen von Zertifizierungsinstanzen verwendet.

Vertraulichkeit
Das Geheimhalten von Informationen vor allen unbefugten Personen mit Ausnahme der Personen, die entsprechend autorisiert sind.

Vollmachtszertifikat
Ein elektronisches Dokument, das als Bestätigung des Vorhandenseins von Zugriffsrechten sowie der angeblichen Identität von Benutzern dient.

VPN (Virtual Private Network)
Ermöglicht die Ausdehnung von privaten Netzwerken vom Endbenutzer über ein öffentliches Netzwerk (Internet) direkt bis zum Home-Gateway Ihrer Wahl, wie beispielsweise zum Intranet Ihrer Firma.

W3C (World Wide Web Consortium)
Ein 1994 gegründetes internationales Industriekonsortium zur Entwicklung von einheitlichen Protokollen für die Weiterentwicklung des World Wide Web.

WAKE (Word Auto Key Encryption)
Erzeugt einen Strom aus 32-Bit-Worten, der durch Anwendung des XOR-Operators mit Klartextstrom in eine Entweder-Oder-Beziehung gesetzt werden kann, so daß chiffrierter Text erzeugt wird. Wurde von David Wheeler erfunden.

Web of Trust
Ein Modell des verteilten Vertrauens, mit dem PGP den Eigentümer eines öffentlichen Schlüssels bestimmt. Der Grad des Vertrauens ist kumulativ und basiert auf der Kenntnis einer Person über die „Schlüsselverwalter".

Wörterbuchangriff
Berechneter schwerer Angriff zum Entschlüsseln eines Paßworts durch Testen von offensichtlichen und logischen Wortkombinationen.

X. 509v3
Ein digitales ITU-T-Zertifikat, bei dem es sich um ein international anerkanntes elektronisches Dokument zur Prüfung der Identität und der Eigentümer von öffentlichen Schlüsseln in einem Kommunikationsnetzwerk handelt. Es enthält den Namen des Absenders, Informationen zur Identifizierung des Benutzers und die digitale Unterschrift des Absenders sowie andere mögliche Erweiterungen in Version 3.

X9. 17
Eine ANSI-Spezifikation mit Details über die Verfahrensweise zum Erzeugen von Zufalls- und Pseudo-Zufallszahlen.

XOR
Abkürzung für „Exclusive-Or Operation" („Entweder-Oder-Operation"). Dient zur mathematischen Darstellung von Unterschieden.

Zeitangaben
Aufzeichnen der Erstellungszeit oder der Zeit des Vorhandenseins von Informationen.

Zertifikat (digitales Zertifikat)
Ein von einem vertrauenswürdigen Dritten mit einem öffentlichen Schlüssel verbundenes elektronisches Dokument, das beweist, daß der öffentliche Schlüssel einem rechtmäßigen Eigentümer gehört und nicht verfälscht wurde.

Zertifizierung Bestätigung von Informationen durch einen vertrauenswürdigen Benutzer.

Zufallszahl Ein wichtiger Aspekt für viele Verschlüsselungssysteme sowie ein notwendiges Element beim Erzeugen von eindeutigen Schlüsseln, die für Gegner nicht berechenbar sind. Echte Zufallszahlen werden normalerweise aus analogen Quellen abgeleitet und erfordern in der Regel den Einsatz von besonderer Hardware.

Zugriffssteuerung Ein Verfahren für die Zugriffsbeschränkung auf Ressourcen. Der Zugriff wird nur bestimmten Benutzern gewährt.

Zurücknahme Widerrufen von Zertifizierungen oder Bevollmächtigungen.

Zusätzlicher vom Empfänger angeforderter Schlüssel Ein spezieller Schlüssel, bei dessen Vorhandensein alle mit dem zugehörigen Basisschlüssel verschlüsselte Nachrichten automatisch ebenfalls mit diesem Schlüssel verschlüsselt werden müssen. Dieser Schlüssel wird gelegentlich auch als Zusätzlicher Entschlüsselungs-Schlüssel (Additional Decryption Key, ADK) bezeichnet.

Index

G

H

I

K

L

N

O

P

R

S

T

U

V

W

X

Z