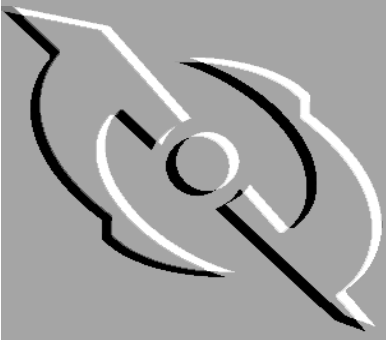

Einführung in die Kryptographie

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.

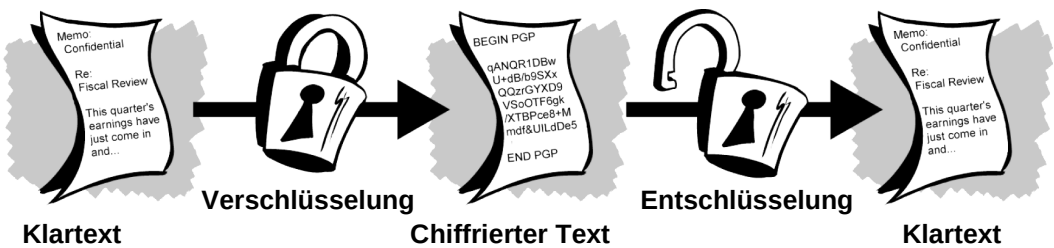

Abbildung 1-1. Verschlüsselung und Entschlüsselung

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.

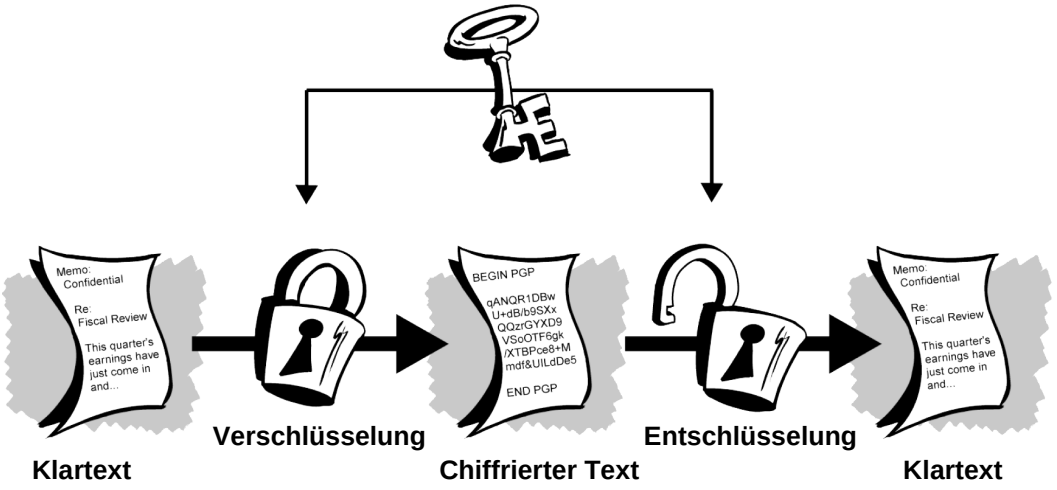

Abbildung 1-2. Konventionelle Verschlüsselung

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.

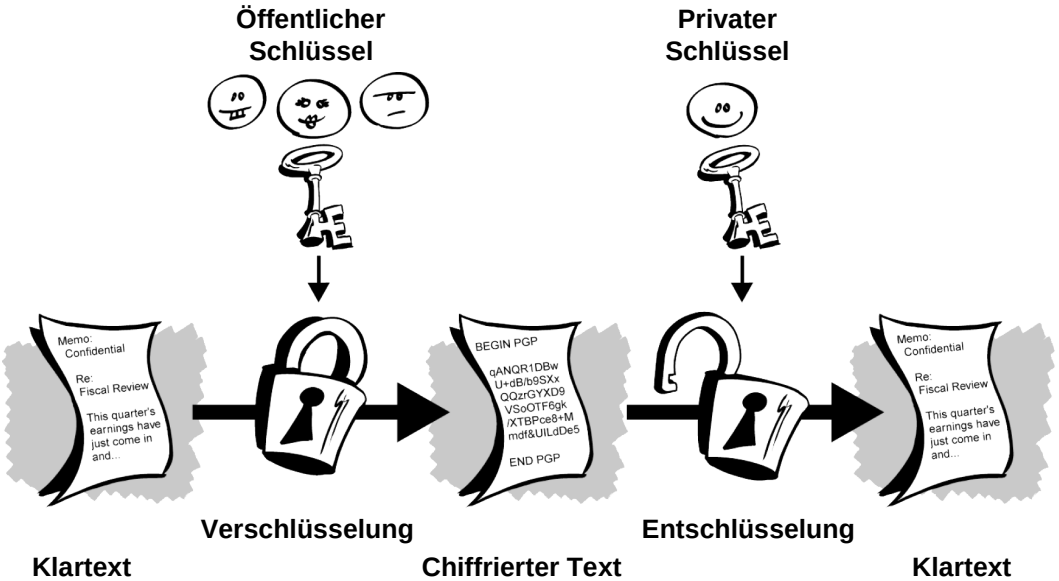

Abbildung 1-3. Verschlüsselung mit öffentlichen Schlüsseln

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.

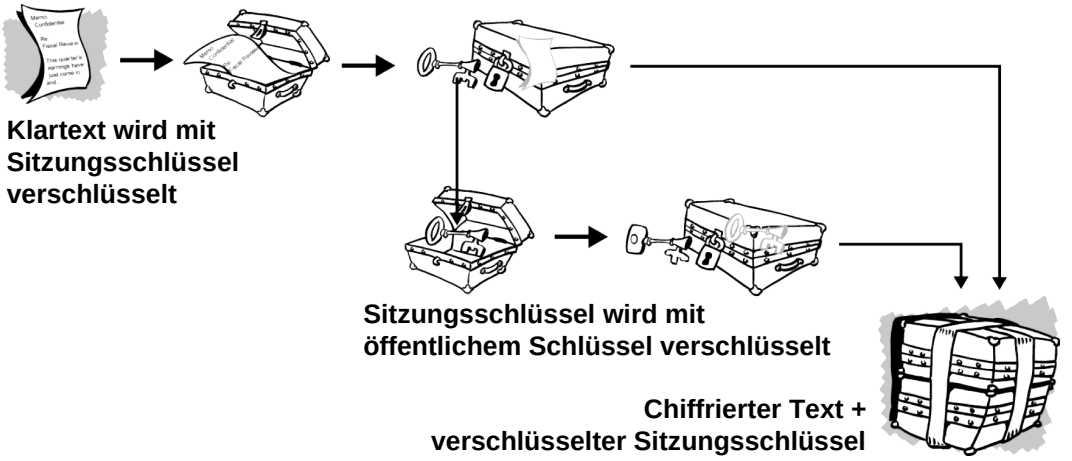

Abbildung 1-4. Funktionsweise der PGP-Verschlüsselung

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.

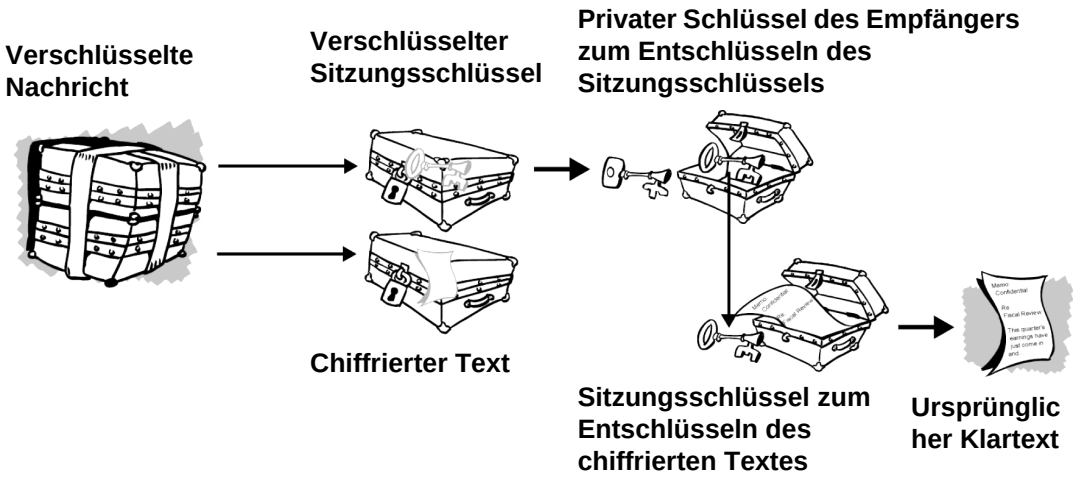

Abbildung 1-5. Funktionsweise der PGP-Entschlüsselung

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.