Verschlüsselung mit PGP

Inhaltsverzeichnis

Vorwort

Im privaten wie im geschäftlichen Bereich wird die Bedeutung von Electronic Mail, oder kurz E-Mail, immer größer. Seine Vorteile gegenüber der konventionellen papiergebundenen Kommunikation sind nicht von der Hand zu weisen: E-Mail ist preisgünstiger, schneller und scheint für eine effiziente Kommunikation wie geschaffen.

Doch wenn es darum geht, vertrauliche Informationen auszutauschen, und dies ist in der geschäftlichen Kommunikation die Regel, sollte man das Medium E-Mail besser nicht einsetzen. Denn im Gegensatz zu den herkömmlichen Postdiensten kennt das Internet kein Postgeheimnis, d.h. vertrauliche Daten sind von Dritten leicht einzusehen - es sei denn, die Kommunikationspartner benutzen bei der Verwendung von E-Mail das zum Standard gewordene Verschlüsselungsprogramm PGP. PGP ist in idealer Weise dafür geeignet, eine vor neugierigen Blicken geschützte, vertrauliche Kommunikation zu ermöglichen, ohne auf die bekannten Vorteile der E-Mail zu verzichten.

Die Literatur rund um das Thema Datenverschlüsselung und PGP ist knapp und meist rein auf das Thema Verschlüsselung oder auf die alte PGP-Version 2.6.3 beschränkt. Dieses Buch stellt daher eine Verbindung her zwischen den PGP zugrunde liegenden Verschlüsselungsverfahren und der Anwendung der aktuellen PGP Version 5.5. Es richtet sich in erster Linie an Anwender, die PGP erstmals in betrieblicher Umgebung einsetzen möchten.

Das Buch basiert auf der Diplomarbeit von Herrn Diplom-Betriebswirt Holger Sandker im Fachbereich Wirtschaft an der Fachhochschule Münster.

Münster, im Mai 1999

1 Einleitung

In diesem Kapitel erfahren Sie:

- die Problemstellung und den Aufbau des Buches,
- unter welcher Zielsetzung das Studium dieses Buches steht,
- die Geschichte des Programms PGP.

1.1 Problemstellung und Aufbau des Buches

Electronic Mail ist einer der ältesten und zugleich einer der wichtigsten Dienste im Internet. Das Internet „boomt“ und mit dem Internet wächst auch das Ausmaß, in dem Nachrichten im geschäftlichen und privaten Bereich per E-Mail ausgetauscht werden.

Die Funktionsweise des Dienstes E-Mail wird oftmals mit der konventionellen Post verglichen. So beginnt Christian Reiser ein entsprechendes Kapitel seines Buches „Internet – die Sicherheitsfragen“ beispielsweise mit dem Satz: „E-Mail ist eine eins zu eins Kommunikation ähnlich einem Brief […].“[1] Dieses aus dem Zusammenhang gerissene Zitat gibt weniger die Vorstellung des genannten Autors wieder, sondern dient vielmehr der Veranschaulichung einer falschen Ansicht vieler Anwender. Mit einem Brief wird eine Nachricht assoziiert, die im verschlossenen Umschlag vor fremden Blicken geschützt ist. Doch der Vergleich einer E-Mail mit einem Brief täuscht eine Vertraulichkeit vor, die in dieser Form bei einer herkömmlichen E-Mail nicht besteht. Denn eine E-Mail wird über das Internet im Klartext versendet und dies macht sie anfällig für Datenspionage, Datenmanipulation und Datenfälschung. Um beim Einführungsbeispiel zu bleiben: Eine E-Mail ist eher mit einer Postkarte als mit einem Brief zu vergleichen. In ihrer bekannten, d.h. unverschlüsselten und vor fremden Blicken ungeschützten Form ist eine E-Mail somit für eine auf Vertraulichkeit basierende geschäftliche Kommunikation denkbar ungeeignet.

Als Ausgangspunkt wird daher in Kapitel 2 zunächst die grundlegende Datenübertragungstechnik des Internets dargestellt, anhand derer sich sicherheitskritische Eigenschaften der E-Mail erklären, aber auch Sicherheitsziele ableiten lassen.

---

[1] Christian Reiser, Internet – die Sicherheitsfragen, 1998, S. 149.

Zur Lösung des Sicherheitsproblems im Internet eignen sich Verschlüsselungsverfahren, die von der mathematischen Disziplin der Kryptographie, der „Lehre von den Geheimschriften und Verschlüsselungssystemen“,[2] geliefert werden. Dabei erweisen sich insbesondere moderne Public-Key-Verschlüsselungsverfahren als praktikabel. Mit ihrer Hilfe lässt sich nicht nur Vertraulichkeit der Information erreichen, sie eignen sich auch zur Kontrolle, ob eine Nachricht den Empfänger in unveränderter Form erreicht (Überprüfbarkeit der Datenintegrität) und zur Prüfung der Absenderangaben (Authentifikation des Absenders).

Mit der wachsenden Sensibilität für die Sicherheitsrisiken steigt das Bedürfnis der „Internetgemeinde“ nach Sicherheit – und mit ihr steigt der Stellenwert der Kryptographie. Dieser Entwicklung trägt eine Beschreibung kryptographischer Grundlagen in Kapitel 3 Rechnung. Gleichzeitig bildet dieses Kapitel die Basis zum Verständnis der Funktionsweise des Verschlüsselungsprogramms Pretty Good Privacy, das besser unter dem Namen PGP bekannt ist.

Nachdem Kryptographie in der Vergangenheit ihre Anwendung lediglich im militärischen, diplomatischen oder geheimdienstlichen Bereich fand, entwickelte sich mit der fortschreitenden Entwicklung der Computertechnik ein Massenmarkt für Kryptographie und mit PGP eine Programm, das fortan „Encryption for the masses“ – die „Verschlüsselung für jedermann“ – ermöglichte.[3]

Im privaten Bereich hat sich PGP nach der Veröffentlichung der ersten Version im Jahre 1991 mittlerweile zum Standard für die Verschlüsselung von E-Mails entwickelt. In seiner aktuellen Version 5.5 ist die Software als „PGP for Business Security“ auch für den geschäftlichen Einsatz erhältlich. In Kapitel 4 werden Installation und die Anwendung dieser Programmversion beschrieben.

Zum Abschluss akzentuiert Kapitel 5 einige Sachverhalte aus dem vorangehenden Kapitel und beleuchtet einige abschließende Fragen, die im Hinblick auf die Einführung der Programms PGP in einer Organisation auftauchen werden.

---

[2] Hagen Hagemann u.a.: Kryptologie – Interaktives Training, 1997, auf CD-ROM, Kap. 1.1.2.

[3] Vgl. Guido Schröder, Kryptographie – Schlüssel zur Informationsgesellschaft, 1997, S. 19.

1.2 Zielsetzung des Buches

Dieses Buch hat zum Ziel, den Leser als den potentiellen Anwender PGPs

1. für die Sicherheitsrisiken bei der Kommunikation per E-Mail zu sensibilisieren,
2. mit grundlegenden kryptographischen Verfahren im Allgemeinen und der Verschlüsselungstechnik von PGP im Speziellen vertraut zu machen,
3. in eine korrekte, sicherheitsbewußte Anwendung von PGP als Administrator und/oder Nutzer einzuweisen, und
4. eine erfolgreiche Einführung PGPs bei einer Organisation anhand dieses Buches zu ermöglichen,

wobei „erfolgreich“ gleichzusetzen ist mit der Erfüllung der ersten drei Teilziele. D.h. PGP kann nur dort in effizienter Weise eingesetzt werden, wo sich der Anwender eingehend mit dem Thema „Verschlüsselung mit PGP“ auseinandergesetzt hat.

Da die Einführung der Software PGP wiederum unter der Zielsetzung steht, eine vertrauliche E-Mail-Kommunikation zu erhalten, kann auch das oberste Ziel dieses Buches lauten:

Ermöglichung einer auf Vertraulichkeit basierenden geschäftlichen Kommunikation per E-Mail.

1.3 Hintergrund: PGP

Das Programm PGP wurde von dem US-Amerikaner Phil Zimmermann entwickelt und wird seit der ersten Version aus dem Jahr 1991 als Freeware kostenlos im Internet für den privaten Gebrauch zur Verfügung gestellt. Seit der Version 2.4 ist PGP gegen Lizenzgebühren auch für den kommerziellen Einsatz erhältlich.[4]

Absicht der Erstveröffentlichung war, einem Gesetz[5] des amerikanischen Senates zuvorzukommen, das das Ab- bzw. Mithören jeder Art moderner Kommunikation durch Regierungsstellen erheblich vereinfachen sollte. Somit wären z.B. Hersteller kryptographischer Software faktisch gezwungen worden, „Hintertüren“ in ihre Produkte einzubauen, um dem amerikanischen Staat Zugriff auch auf verschlüsselte Informationen zu ermögli-

---

[4] Vgl. Simson Garfinkel, PGP: Pretty Good Privacy, 1996, S. 118f.

[5] Das Gesetz gegen Kriminalität „S. 266“, vgl. Simson Garfinkel, PGP: Pretty Good Privacy, 1996, S. 110.

chen. Die Entwicklung von Pretty Good Privacy hatte hingegen zum Ziel, die Privatsphäre zumindest bei der Kommunikation mit E-Mail zu schützen. So wurde durch die Veröffentlichung ein Faktum geschaffen, infolgedessen sich der Anwender bei der Kommunikation per E-Mail vor staatlichen, aber auch vor anderen fremden Blicken schützen konnte.[6]

Der umstrittene Passus des Gesetzes wurde zwar wieder gestrichen, trotzdem blieb PGP zunächst ein nicht legales „Untergrundprogramm", denn innerhalb der USA verstieß PGP gegen ein bestehendes Patent bezüglich des benutzten Verschlüsselungsalgorithmus RSA. Außerhalb der USA bestanden diese Patentrechte zwar nicht, doch behandelten und behandeln US-amerikanische Ausfuhrbestimmungen bestimmte kryptographische Technologien wie Kriegswaffen und verbieten daher auch den Export von PGP.[7]

Das erste Problem wurde ab der PGP Version 2.4 für den Einsatz im kommerziellen Bereich und ab der Version 2.6 auch für den privaten Gebrauch durch Lizenzabkommen zur Nutzung des Verschlüsselungsalgorithmus RSA gelöst.

Das zweite Problem wird bei jeder neuen Version PGPs auf eine abstrus wirkende Weise umgangen: Der Quellcode PGPs wird ausgedruckt, als Buch exportiert und im Ausland wieder eingelesen, denn Bücher sind von den angesprochenen Ausfuhrbestimmungen ausgeschlossen.[8] Der Einsatz dieser PGP-Versionen unterliegt, wie auch der Einsatz von Verschlüsselungsverfahren allgemein, in Deutschland keiner rechtlichen Beschränkung.[9]

Aufgrund der kostenlosen Distribution und der nach Expertenmeinung sehr hohen Verschlüsselungsqualität[10] entwickelte sich PGP im Laufe der Jahre mit mittlerweile 4 Millionen Anwendern zum De-facto-Standard der Verschlüsselung von E-Mail.[11]

Mit dem „Sprung" der Versionsnummer von 2.6 auf 5.0 übernahm Network Associates die Vermarktung des Programms für gewerbliche Anwender[12]

---

6 Vgl. Simson Garfinkel, PGP: Pretty Good Privacy, 1996, S. 110ff.

7 Vgl. FoeBuD e.V. Bielefeld, PGP-Dokumentation, Teil II, Kapitel .5.

8 Diesen Umstand erkennen Anwender der Freeware Versionen an dem Zusatz „i" oder „ui", mit dem die „internationale" oder auch „inoffizielle (unofficial) internationale" Version des Programmes gekennzeichnet wird.

9 Vgl. Wolfgang Kopp, Rechtsfragen der Kryptographie und der digitalen Signatur, 1998, Kapitel C, Nr. I.2a.

10 Vgl. Hagen Hagemann u.a.: Kryptologie – Interaktives Training, 1997, Handbuch S. 47.

11 Vgl. Achim Born in: Gateway, Mai 1998, S.34.

12 Für Privatanwender ist die entsprechende Version PGP 5.5i nach wie vor Freeware.

und integrierte PGP in ihr Sicherheitskonzept für Netzwerkumgebungen „Total Network Security“. In diesem Buch wird PGP allerdings separat betrachtet.

Diesem Buch ist die Version „PGP for Business Security 5.5.3“ [13] für den gewerblichen Anwendungsbereich zugrunde gelegt.

1.4 Typographische Konventionen des Buches

Dieses Buch enthält viele Fachtermini, die teilweise aus dem Gebiet der Informatik und der Kryptographie bzw. Kryptologie stammen oder aber nur im Gebrauch mit dem Programm PGP verwendet werden. Als Hilfestellung für den Leser sind entsprechende Wörter bei ihrer erstmaligen Verwendung *kursiv* gedruckt und im Glossar ab Seite 109 kurz erklärt.

Um die Übersichtlichkeit zu erhöhen, wird darüber hinaus an einigen Stellen ein besonderer Zeichensatz verwendet:

- Wichtige Sachverhalte erscheinen **fett** gedruckt,
- Dateinamen werden in GROßBUCHSTABEN dargestellt,
- Funktionen und Menüpunkte werden durch KAPITÄLCHEN hervorgehoben,
- Modulnamen PGPs erscheinen in der Schriftart Arial,
- Beispiele sind in der `Schriftart Courier New` gedruckt.

[13] Die Versionsnummern „5.5.3“ und „5.5“ werden oft gleichbedeutend verwendet. Selbst die Dokumentation bleibt nicht bei einer einheitlichen Versionnummer.

2 Ausgangsproblem und Zielsetzung

In diesem Kapitel erfahren Sie:

- wie Nachrichten per E-Mail übertragen werden,
- welchen Gefahren Nachrichten bei der Übertragung ausgesetzt sind,
- welche Sicherheitsrisiken sich aus unverschlüsselter Kommunikation per E-Mail ergeben,
- welche Sicherheitsziele sich mit Verschlüsselung erreichen lassen.

Warum sollte eine Person oder Organisation Nachrichten verschlüsseln, die sie per *E-Mail* über das Internet verschickt? Nimmt man diese Frage als Ausgangspunkt dieses Kapitels, so liegt die Antwort in der Betrachtung des grundlegenden Aufbaus des Internets. Die Kenntnis darüber, wie elektronische Nachrichten ihren Weg vom Sender zum Empfänger nehmen, führt zum Erkennen der mit der Datenübertragungstechnik des Internets verbundenen Sicherheitsrisiken. Hieraus lassen sich Sicherheitsziele ableiten, die auch als Anforderungen an die Verschlüsselungstechnik verstanden werden können.

2.1 Ursprung des Internets und seiner Datenübertragungstechnik

Die Ursprünge des heute unter dem Namen *Internet* bekannten weltumspannenden Computernetzwerks sind Ende der 60er Jahre in den USA zu finden. Dort unterstützte die dem amerikanischen Verteidigungsministerium unterstellte *ARPA (Advanced Research Projects Agency)* die Entwicklung im Bereich der Computervernetzung.[14] Das Ziel dieser Bemühungen war, einen Verbund verschiedenartiger militärischer und wissenschaftlicher Hostrechner zu schaffen, „der auch bei Teilausfällen (z.B. durch militärische Zerstörung) in der Lage ist, verlässliche Kommunikation zwischen den einzelnen Standorten zu ermöglichen.“[15]

[14] Vgl. Martin Scheller u.a.: Internet: Werkzeuge und Dienste, 1994, S. 5.

[15] Gerhard Lienemann, TCP/IP-Grundlagen, 1996, S. 16.

Die erste Sitzung im November 1969 markiert die Entstehung des fortan *Arpanet* genannten Computernetzwerkes mit zunächst zwei Diensten:

- *Telnet*: ermöglicht die Durchführung von Sitzungen auf entfernten Rechnern,
- *ftp:* erlaubt den Transfer von Dateien zwischen zwei entfernten Rechnern.

1971 kam der Dienst Electronic Mail, die Möglichkeit des Austausches von elektronischen Nachrichten zwischen zwei Personen, hinzu.

Zunächst kommunizierten die verschiedenen Hostrechner über ihnen eigens zugeordnete kleine Rechner, sog. IMPs (Interface Message Processor). Diese benutzten untereinander das Übertragungsprotokoll NCP (Network Control Protocol) und bildeten somit das eigentliche Netzwerk. Die Weiterentwicklung des NCP zum bis heute im Internet als Übertragungsprotokoll verwendeten *TCP/IP (Transmission Control Protocol / Internet Protocol)* ermöglichte es schließlich, auf die IMPs zu verzichten, so dass nun verschiedene Rechnerarchitekturen direkt miteinander verbunden werden können. Die Umstellung zwischen 1978 und 1983 kennzeichnet auch die Zeit, in der sich der Begriff Internet für das auf TCP/IP basierende Arpanet durchsetzte.[16]

In den Folgejahren wurden weitere Rechner und bislang eigenständige Computernetzwerke eingebunden. Neue auf TCP/IP basierende Dienste, insbesondere Anfang der 90er Jahre das *WWW (World Wide Web),* kamen hinzu und machten das Internet zu einem vielfältig genutzten Informationspool. Insbesondere E-Mail hat sich in den letzten Jahren als Kommunikationsform etabliert und ist neben dem WWW der meist genutzte Internetdienst.

2.2 Sicherheitsrisiken beim Versenden von E-Mail über das Internet

Sprach man bei der Entwicklung des Computernetzwerks von verlässlicher Kommunikation, so war damit eine „stabile“ Verbindung gemeint, d.h. eine vor Ausfall sichere Datenübertragung zwischen Sender und Empfänger.

[16] Vgl. Martin Scheller u.a.: Internet: Werkzeuge und Dienste, 1994. S. 6ff.

Heute gilt die Sorge um eine verlässliche Kommunikation eher der Sicherheit der Daten. Elektronische Nachrichten können Ziele eines **Angriffs** Dritter werden, d.h. die Daten können

- kopiert,
- gestohlen,
- verändert oder
- gefälscht werden.

Im Folgenden soll untersucht werden, inwiefern diese Sorge begründet ist. Zunächst wird in kurzer Form dargestellt, wie eine Nachrichtenübertragung per E-Mail zwischen Sender und Empfänger erfolgt:

Sender und Empfänger einer E-Mail arbeiten i.Allg. an Rechnern, die keinen permanenten Anschluss an das Internet haben und somit auch nicht Teil des Internets im engeren Sinne sind. Der Austausch der E-Mails erfolgt daher über Mail-Server, die Nachrichten weiterleiten, empfangen, zwischenspeichern und einen permanenten Anschluss an das Internet haben.

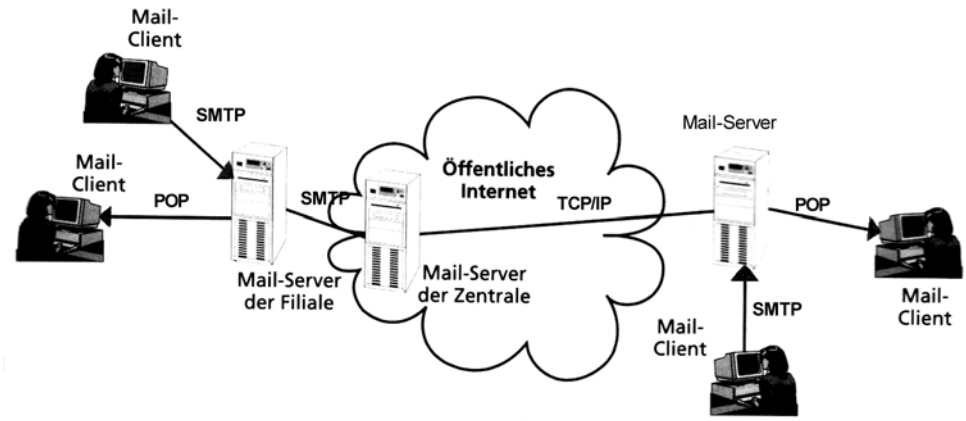


Abbildung 1: Mail-Server und -Clients[17]

Abbildung 1 macht den Sende- und Empfangsvorgang anschaulich: Der Arbeitsplatzrechner des Senders wird in diesem Fall zum Mail-Client; seine Mail-Software baut über den Mail-Server des lokalen Netzwerkes eine Verbindung zum Mail-Server des Empfängers auf. Dabei kommt auf der Anwendungsebene das *SMTP-Protokoll (Simple Mail Transfer Protocol)* zum

[17] Vgl. Abb. in: Richard E. Smith, Internet-Kryptographie, 1998, S. 281.

Einsatz.[18] Dieses Protokoll beinhaltet die nötigen Direktiven, um Sender, Empfänger sowie den Text der Nachricht festzulegen.

Wenn es sich um einen Nachrichtenaustausch innerhalb des lokalen Netzes handelt, stellt der Mail-Server die Nachricht sofort zu, andernfalls gelangt die Mail über das Internet mittels TCP/IP als Übertragungsprotokoll zum Mail-Server des Empfängers.

Treffen die Nachrichten dort ein, werden die Daten zunächst in die physisch auf dem Mail-Server liegende Mailbox des Adressaten eingestellt. Hier bleiben sie solange zwischengespeichert, bis der Empfänger sie mit Hilfe seiner Mail-Anwendung abholt. Die Zugangsmöglichkeit wird ihm über das zwischen Server und Client benutzte Anwendungsprotokoll *POP (Post Office Protocol*) verschafft.[19]

2.2.1 Angriffspunkte

Bei den angesprochenen Anwendungs- und Übertragungsprotokollen handelt es sich um Klartextprotokolle, d.h. die Datenübertragung erfolgt unverschlüsselt. Diese Gegebenheit begründet zusammen mit weiteren Eigenschaften der einzelnen Protokolle die Sicherheitsrisiken. Insbesondere kommt dieser Gesichtspunkt an drei markanten Stellen des Kommunikationsweges zu tragen. Abbildung 2 zeigt diese **Angriffspunkte**, an denen sich für einen Dritten Möglichkeiten zu einer Störung der Kommunikation bieten.

---

[18] Die darunter liegenden Protokolle der Transportebene sind in der Praxis unterschiedlich und sehr vielfältig. LANs verwenden herstellerspezifische Transportprotokolle, private Internet-Nutzer wiederum bauen eine Verbindung zu ihrem Internet-Zugangsanbieter i.A. über SLIP oder PPP auf. Eine nähere Betrachtung dieser Protokolle ist im Rahmen dieser Arbeit jedoch nicht notwendig.

[19] Vgl. Stefan Nusser, Sicherheitskonzepte im WWW, 1998, S. 38ff.

Abbildung 2: Angriffspunkte zur Störung der E-Mail-Kommunikation[20]

Die Angriffspunkte werden nachfolgend im Detail betrachtet:

2.2.1.1 Angriffspunkt Übertragung

Die unten stehende Abbildung 3 zeigt einen Zusammenschluss verschiedener Rechner mittels TCP/IP und gibt damit modellhaft einen Ausschnitt aus dem Internet wieder. Die Abbildung 3 ist, wenn man so will, eine Vergrößerung der „Wolke“ aus Abbildung 2. Als Beispiel sei der Versand bestimmter Daten von Workstation B zur Workstation C auf der Ebene des Übertragungsprotokolls TCP/IP betrachtet.

Die Nachricht wird zunächst durch das TCP-Protokoll der Workstation B in Datenpakete zerteilt. Da sich der Zielrechner nicht im gleichen Netz befindet, werden die Pakete zu einem Grenzrechner an der Schnittstelle zweier Netze, dem sog. *Router*, geschickt. Dieser entscheidet anhand der bekannten *IP-Adresse* des Empfängerrechners, wohin er die Datenpakete routen, d.h. weiterreichen soll. Von Workstation B beispielsweise geht der Weg also über den als Router dienenden Server D weiter zu Router B und abschließend zu Workstation C, die mittels TCP die Datenpakete wieder zusammensetzt.

---

[20] Vgl. Abb. in: Simson Garfinkel, PGP: Pretty Good Privacy, 1996, S. 7.

Abbildung 3: Modellhafter Internet-Ausschnitt[21]

Aufgrund dieser Protokollarchitektur ergibt sich für die Untersuchung ein bedeutsamer Aspekt: Der Vorgang des Routens kann sich im realen Fall etliche Male wiederholen, eine E-Mail „hangelt" sich so von Router zu Router, bis sie schließlich beim Empfänger ankommt. Der Weg eines jeden Datenpaketes lässt sich dabei nicht eindeutig bestimmen, denn jeder Router kennt mehrere Routingprotokolle, um stark frequentierte Teile des Netzes umgehen zu können. Dies ist noch eine Folge der militärischen Forderung nach Kommunikationsfähigkeit auch bei Teilausfällen des Netzes. **Die Datenpakete nehmen folglich je nach aktueller Netzlast verschiedene, unvorhersehbare Wege und passieren damit Rechner unbekannter Dritter.**[22]

Dieser Vorgang lässt sich sehr leicht durch die Funktion Traceroute veranschaulichen, die im MS-DOS-Fenster durch die Eingabe des Befehls TRACERT und eines Domänennamens oder IP-Adresse aufgerufen werden kann, Beispiel:

```
TRACERT WWW.SANDKER.DE
```

Die Funktion Traceroute sendet eine Serie von kleinen Datenpaketen an den Empfängerrechner und listet dabei alle Router auf, die von diesen Paketen auf ihren Wege zum Empfänger passiert werden.

---

[21] Vgl. Abb. in: Richard E. Smith, Internet-Kryptographie, 1998, S. 30.

[22] Vgl. Richard E. Smith, Internet-Kryptographie, 1998, S. 29ff.

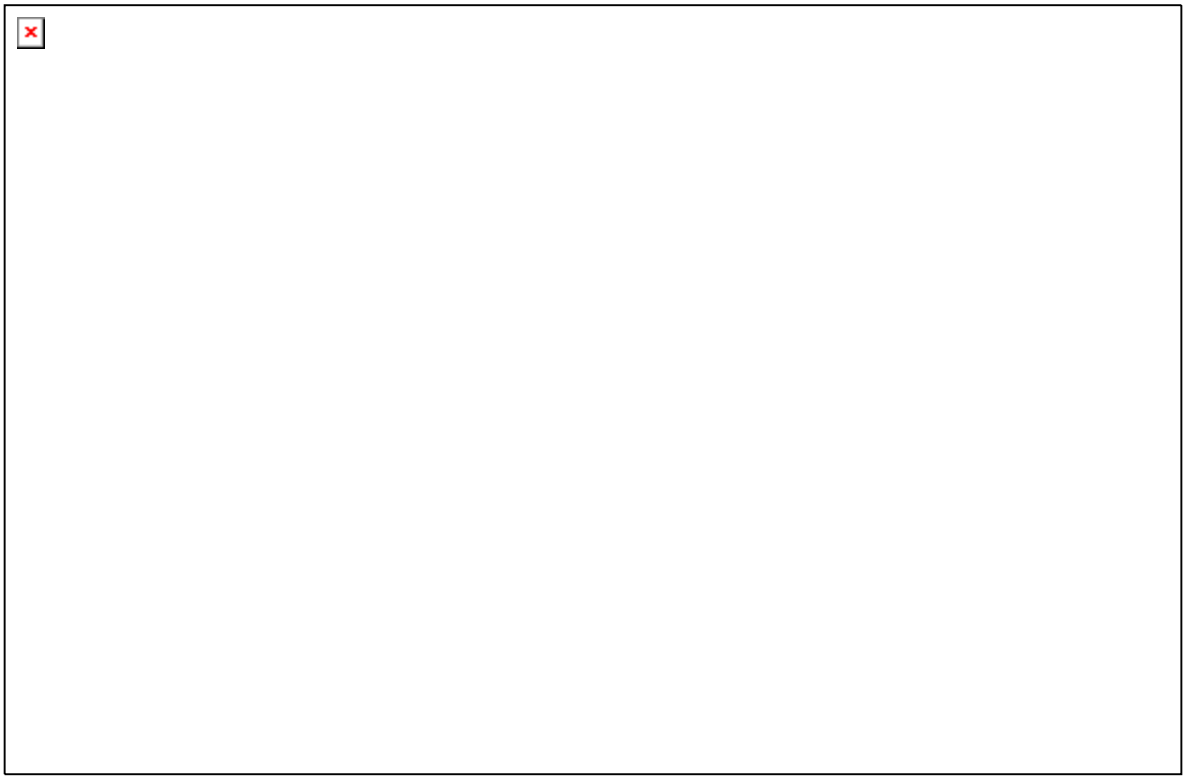


Abbildung 4: Verfolgung der Datenweges mit Traceroute

Durch den Vorgang des Routens ergeben sich erhebliche Risiken für die Datensicherheit, denn Informationen, die das Internet passieren, können auf ihrem langen Weg vom Sender zum Empfänger angegriffen werden. Als Beispiel seien hier sog. „Packet-Sniffer“ genannt, die, auf einem Router oder einem angeschlossenen Netzrechner installiert, alle vom Router weitergereichten Datenpakete kopieren und auf bestimmte Stichwörter hin auswerten können.[23]

2.2.1.2 Angriffspunkt Mail-Server

Empfangene Mitteilungen bleiben nun auf dem Mail-Server so lange gespeichert, bis der Empfänger sie abruft. Hier bietet sich ein Angriffsmoment.

[23] Vgl. Michael Tischer in PC-Online, 10/98, S. 52.

Angriffe von außen auf den Mail-Server können zwar durch *Firewalls* bis auf ein gewisses (nicht messbares) Restrisiko abgewehrt werden,[24] vor den Augen anderer Mitarbeiter sind auf dem Mail-Server lagernde E-Mails i.d.R. schlecht geschützt:

Der Zugang zum Mail-Server erfolgt i.Allg. über die Benutzerkennung und ein Kennwort. Die Benutzerkennung ist meistens der Name des Anwenders und daher jedem Mitarbeiter bekannt, das Kennwort lässt sich u.U. mit ein wenig Aufwand herausfinden. Für fast alle Mail-Systeme sind Programme verfügbar, die fremde Kennwörter ermitteln, indem sie z.B. Wortlisten durchlaufen.[25] Oftmals ist dieser Aufwand nicht einmal notwendig, weil das Kennwort leicht zu erraten ist oder gar am Arbeitsplatz für jedermann sichtbar notiert wurde.

Ist der Angreifer erst einmal in den Besitz eines fremden Kennwortes gekommen, so kann er nicht nur die E-Mails des Benutzers lesen, sondern auch manipulieren oder E-Mails in dessen Namen versenden.

2.2.1.3 Angriffspunkt Mail-Client

E-Mails bleiben i.d.R. nach Abruf vom Mail-Server auf dem als Mail-Client dienenden Arbeitsplatzrechner gespeichert. Für einen internen Angriff auf den Mail-Client gilt daher im entsprechenden Sinne grundsätzlich das Gleiche wie für den Mail-Server.

Arbeitsplatzrechner genießen darüber hinaus nur höchst selten auch physischen Schutz. D.h. Arbeitsplatzrechner werden oftmals unbeaufsichtigt gelassen, was ein Angreifer für seine Zwecke missbrauchen kann.

2.2.2 Angriffsformen

Ein Angriff auf die Kommunikationsbeziehung wurde bereits definiert als Kopieren, Stehlen, Verändern oder Fälschen.[26] Eine genauere Betrachtung wird im Folgenden als Beschreibung der **Angriffsformen** dargestellt, die von einem Angreifer an jedem Angriffspunkt ausgeführt werden können.

---

[24] Ein bekanntes Beispiel dafür, wie Firewalls zu umgehen sind, ist das so genannte „Internet Address Spoofing“: Der Angreifer täuscht mittels geeigneter Software eine falsche IP-Adresse mit der Absicht vor, sich als ein Rechner innerhalb des von dem Firewall geschützten Bereiches auszugeben und somit Zugriff auf den Mail-Server zu bekommen. Vgl. Stefan Nusser, Sicherheitskonzepte im WWW, 1998, S. 23.

[25] Zu finden auf der CD-ROM Hacker's Best Friend, Utech-Verlag, Oldenburg, 1998.

[26] Angriffe auf die Kommunikationsbeziehung sind nicht zu verwechseln mit Attacken auf kryptographische Systeme, siehe Seite 28.

2.2.2.1 Datenspionage

Den grundlegenden Fall, das unbefugte Lesen kopierter oder gestohlener Nachrichten, bezeichnet man in seiner vorsätzlichen Angriffsform auch als Datenspionage. Die Motive des Angreifers können dabei völlig unterschiedlicher Natur sein und reichen von einfacher Neugier bis hin zum Erlangen von Wettbewerbsvorteilen.

Beispielsweise hat dieser Fall für eine Bank eine besondere Bedeutung, da aus ihrer Geschäftsbeziehung zu einem Kunden das Bankgeheimnis erwächst, definiert als „Pflicht der Bank, über Vermögensverhältnisse des Kunden, die ihr aus der Geschäftsverbindung bekannt werden, Dritten gegenüber Stillschweigen zu bewahren".[27]

Somit ist das Bankgeheimnis die elementare Grundlage der Geschäftsbeziehung zwischen Kunde und Bank. Das Bekanntwerden eines Falles, in dem die unverschlüsselte Kommunikation zwischen Bank und Kunden belauscht worden wäre, würde einen erheblichen Vertrauensverlust zur Folge haben und wäre geschäftsschädigend.

Wie gezeigt wurde, ist Vertraulichkeit bei einer gewöhnlichen Kommunikation per E-Mail über das Internet nicht gegeben. D.h. die Kommunikationspartner müssen sich der Tatsache bewusst sein, dass die ausgetauschten Nachrichten von Dritten gelesen werden können.

Hinter dem unbefugten Lesen braucht jedoch nicht immer die böse Absicht der Datenspionage stehen: Bereits das versehentliche Einsetzen eines falschen Adressaten oder das „Vertippen" (z.B. M**A**IER@DOMAIN.DE statt M**E**IER@DOMAIN.DE) führt zur einer ungewollten Zustellung der E-Mail an einen Dritten und dieser wird eine Klartextnachricht wahrscheinlich auch lesen.

2.2.2.2 Datenmanipulation

Der nächste denkbare Schritt ist die Manipulation von Nachrichten, d.h. eine Nachricht wird abgefangen und der Inhalt bewusst durch Streichungen, Änderungen oder Hinzufügungen manipuliert. Die Angaben über Sender und Empfänger können dabei unberührt bleiben.

Ein kurzes Beispiel: Ein Kunde schickt einen Überweisungsauftrag per E-Mail an die Bank. Die E-Mail wird abgefangen und an die Stelle der ur-

---

[27] Def. aus: Gabler Wirtschafts-Lexikon auf CD-ROM, 1993.

sprünglich begünstigten Kontonummer der Überweisung setzt der Angreifer die eigene ein.

Bei einer normalen E-Mail gibt es somit keine Garantie auf Datenintegrität. Dies bedeutet, weder Sender noch Empfänger können und dürfen sich darauf verlassen, dass die Nachricht in der ursprünglichen Form und mit demselben Inhalt ankommt, mit dem sie auch abgeschickt wurde.

2.2.2.3 Datenfälschung

Bei der Datenfälschung handelt es sich um die Konstruktion von frei erdachten Nachrichten unter Angabe eines falschen Namens. Geeignete Programme, wie z.B. Win95 Anonymail[28] nutzen die Tatsache aus, dass das SMTP-Protokoll die Adressangaben des Absenders einer E-Mail nicht überprüft. Sie täuschen dem Mail-Server des Empfängers sowohl eine falsche E-Mail-Adresse als auch IP-Nummer des Absenders vor und sind so einfach zu bedienen, dass selbst Laien zu Datenfälschern werden können. Der Empfänger bemerkt die Täuschung i.Allg. nicht. Für ein Unternehmen entsteht daraus eine doppelte Gefahr:

1. Datenfälscher können sich als Kunden ausgeben und z.B. bei einer Bank eine gefälschte Überweisung per E-Mail einreichen.
2. Datenfälscher benutzen die E-Mail-Adresse eines Unternehmensangestellten für ihre Zwecke.

Das Problem: Der Absender einer E-Mail kann nicht zweifelsfrei nachgewiesen (authentifiziert) werden. Eine gewöhnliche E-Mail ist somit für die Durchführung rechtsverbindlicher Geschäfte wie z.B. Bestellungen oder Überweisungen denkbar ungeeignet.

2.3 Sicherheitsziele

Wie gezeigt wurde, sind die Gefahren, die von der Datenspionage, der Datenmanipulation und der Datenfälschung ausgehen so groß, dass bei Nachrichten mit sensiblen oder vertraulichen Inhalten eine geschäftliche Kommunikation auf Basis unverschlüsselter E-Mails als nicht praktikabel gelten kann.

Eine Lösung dieses Sicherheitsproblems bietet sich aus dem Bereich der *Kryptographie* an. Mit ihr ist es möglich, die beschriebenen Angriffsformen

---

[28] Zu finden auf der CD-ROM Hacker's Best Friend, Utech-Verlag, Oldenburg, 1998.

an sämtlichen Angriffspunkten auszuschalten. Die Unterpunkte des Kapitels beschreiben, welche Ziele mit der Verschlüsselung erreicht werden sollen:

2.3.1 Vertraulichkeit der Nachrichten

Die Nachrichten müssen vor dem Senden so stark verschlüsselt werden, dass ein Dritter im Falle der Datenspionage lediglich in den Besitz unverständlicher Daten kommen kann, die er auch unter höchstem Aufwand nicht zu entschlüsseln vermag. Der Angreifer darf auch selbst dann keine Rückschlüsse auf die Nachricht ziehen können, wenn er dasselbe kryptographische System benutzt.[29] Ziel ist eine vertrauliche Nachrichtenübermittlung zwischen Sender und Empfänger.

Mit der Verschlüsselung kann zwar das Kopieren oder Stehlen der Daten nicht verhindert werden. Eine wirkungsvolle Verschlüsselung macht die Nachricht für einen Dritten jedoch wertlos, weil ihm der Inhalt unbekannt bleibt.

2.3.2 Integrität der Nachrichten

Integrität der Nachricht bedeutet: Der Sender muss die Sicherheit haben, dass die zu übermittelnden Daten nicht ohne seine Einwilligung verändert werden können.[30] Umgekehrt muss dem Empfänger die Möglichkeit der Überprüfung gegeben sein, ob die Nachricht unverfälscht, d.h. authentisch angekommen ist.[31]

2.3.3 Authentifikation des Absenders

Der Empfänger muss zuverlässig feststellen können, dass die empfangene Nachricht auch von der Person kommt, von der sie zu stammen vorgibt. Für den Sender bedeutet dies, Urheberschaftsrechte zu besitzen bzw. nicht leugnen zu können. [32] Die E-Mail benötigt eine so genannte *digitale (elektronische) Signatur*.

---

[29] Vgl. Richard E. Smith, Internet-Kryptographie, 1996, S. 23. Dieser Sachverhalt ist auch unter der "Maxime von Kerckhoffs" bekannt: Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung des Algorithmus, sondern ausschließlich von der Geheimhaltung des Schlüssels abhängen.

[30] Vgl. Simson Garfinkel, PGP: Pretty Good Privacy, 1996, S. 6.

[31] Vgl. Hagen Hagemann u.a.: Kryptologie – Interaktives Training, 1997, auf CD-ROM, Kap. 1.1.2.

[32] Vgl. Richard E. Smith, Internet-Kryptographie, 1996, S 77.

Zusammen mit einem Integritätsbeweis der Nachricht könnte diese elektronische Unterschrift es ermöglichen, per E-Mail verbindliche Rechtsgeschäfte abzuschließen.

2.4 Fazit

Die Übertragungstechnik des Internets macht das Kommunikationsmittel E-Mail preiswerter und schneller als herkömmliche Postdienste und aufgrund der weiten Verbreitung in der Bevölkerung müsste sich dieser neue Dienst mittlerweile bestens dafür eignen, eine Verbindung mit Kunden, Lieferanten und Mitarbeitern herzustellen.[33] Doch gerade die Übertragungstechnik ist Ursache der beschriebenen Sicherheitsrisiken und u.a. ein Grund dafür, dass nach wie vor Papier die vorwiegende Basis geschäftlicher Dokumente ist.

Die Einführung eines Public-Key-Verschlüsselungsverfahrens minimiert diese Sicherheitsrisiken und insbesondere der Einsatz einer digitalen Unterschrift bietet dem Einsatz von E-Mail neue Möglichkeiten. So schreibt Guido Schröder in einem Diskussionspapier der Universität Münster:[34]

„Die sich mit der digitalen Unterschrift bietenden Möglichkeiten sind vielfältig. [...] Viele Anwendungsgebiete liegen in den Bereichen des täglichen Lebens, die gegenwärtig noch die Übertragung papiergebundener Information voraussetzen. Hierzu zählen beispielsweise rechtsverbindliche Geschäfte wie Bestellungen, Überweisungen und Bürgschaften. Möglich werden aber auch elektronisch gestellte Anträge bei Behörden, z.B. Steuererklärungen, ebenso notarielle Beglaubigungen – von Gesellschaftsverträgen bis zu Testamenten – wie fälschungssichere Ausweise – Reisepässe und Führerscheine."

---

[33] Vgl. Jens Christophers und Jürgen Nonhoff: Going online – going public, 1997, S. 37.

[34] Guido Schröder, Kryptographie – Schlüssel zur Informationsgesellschaft, 1997, S. 24.

3 Kryptographische Grundlagen

In diesem Kapitel erfahren Sie:

- den Unterschied zwischen symmetrischer und asymmetrischer Verschlüsselung und deren jeweiligen Vor- und Nachteile,
- in welcher Weise die verschiedenen kryptographischen Algorithmen in PGP ihre Anwendung finden,
- wozu Schlüssel dienen und was digitale Signaturen sind,
- wie sicher PGP ist,
- was man unter dem „Web of Trust“, dem Vertrauensmodell von PGP, versteht,
- wozu „Key Server“ und „Trustcenter“ dienen.

Die Formulierung der Sicherheitsziele deutete bereits an, welche Leistungen der Gebrauch eines *kryptographischen Systems (Kryptosystem)* bieten muss.

Ein kryptographisches System umfasst mindestens einen *kryptographischen Algorithmus* und die Gesamtheit aller möglichen *Schlüssel*. Das Zusammenspiel der beiden Komponenten *chiffriert* oder *dechiffriert* Nachrichten. Die Sicherheit des Chiffretextes ist abhängig von der Stärke des zugrunde liegenden Algorithmus und der Gewährleistung der Geheimhaltung des Schlüssels. Um also zu erkennen, was ein kryptographisches System wie das zu besprechende PGP zu leisten vermag, ist eine eingehende Betrachtung der Komponenten Algorithmus und Schlüssel notwendig.

Wie sich zeigen wird, kombiniert PGP intern eine Reihe kryptographischer Algorithmen sowohl symmetrischer als auch asymmetrischer Natur. PGP stellt also strenggenommen ein hybrides Kryptosystem[35] dar. Aus Anwendersicht ist PGP jedoch ein typischer Vertreter der Verschlüsselung mittels eines *Public-Key-Verschlüsselungsverfahrens*.

Eine nähere Betrachtung des mathematischen Hintergrundes sämtlicher Algorithmen und der sehr komplexen Verschlüsselungsvorgänge würde den gegebenen Rahmen dieses Buches sprengen. Der Einblick sollte je-

[35] Vgl. Network Associates, Dokumentation zu PGP 6.0 Freeware, Intro to Crypto, 1998, S. 16.

doch ausreichen, um eine gute Vorstellung der Funktionsweise von PGP und einen Einstieg in die Arbeit mit PGP zu erhalten. In Verbindung mit dem Unterkapitel über Attacken auf kryptographische Systeme soll auch eine Einschätzung der kryptographischen Stärke von PGP möglich sein.

3.1 Einfache Kryptographie

Im Sinne dieses Buches[36] ist mit *Kryptographie* die wissenschaftliche Disziplin gemeint, „die sich damit beschäftigt, wie man den Inhalt von Nachrichten verheimlicht, sie also vor unbefugter Kenntnisnahme absichert.“[37] Ein Beispiel für ein einfaches Chiffrierverfahren ist die Vigenère-Chiffre.[38] Grundlage dieses klassischen Verschlüsselungsverfahrens bildet das unten abgebildete Vigenère-Quadrat. Es besteht aus 26 untereinander geschriebenen Alphabeten. Sie sind so angeordnet, dass die erste Zeile das gewöhnliche Alphabet darstellt. Das Alphabet in der zweiten Zeile ist um einen Buchstaben nach links verschobenen, das dritte Alphabet um zwei Buchstaben usw.

[36] Die Begriffe Kryptographie und Kryptologie werden im Gegensatz zu dieser Arbeit in vielen Publikationen gleichbedeutend verwendet, vgl. dazu Albrecht Beutelspacher, Kryptologie, 3. Auflage, 1993, S. 10.

[37] Wolfgang Kopp, Rechtsfragen der Kryptographie und der digitalen Signatur, 1998, Kapitel B, Nr. I.1. Vgl. auch Friedrich L. Bauer, Kryptologie, 2. Auflage, 1994, S. 5.

[38] Vgl. Referat von Prof. Dr. Albrecht Beutelspacher in: Hamm, Rainer; Möller, Klaus Peter: Datenschutz durch Kryptographie: ein Sicherheitsrisiko? 1998, S. 16 ff.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	**R**	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Abbildung 5: Das Vigenère-Quadrat

Die Verschlüsselung eines Textes, im folgenden Beispiel „DIESISTGEHEIM“, geschieht mit Hilfe einer als Schlüssel dienenden beliebigen Buchstabenfolge, z.B. das Wort „Ostern“.

Beispiel:

Klartext: **DIESISTGEHEIM**
Schlüssel: **OSTERN**OSTERNO
Chiffrierter Text: **RAXWZFHYXLVVA**

Die obere Zeile des Quadrates dient als „Schlüsselzeile“, die linke Spalte als „Klartextspalte“. Der erste Buchstabe des chiffrierten Textes entsteht aus dem Buchstaben, der im Schnittpunkt der Zeile und Spalte steht, die jeweils durch den ersten Buchstaben des Schlüssels und des Klartextes bestimmt wird. Dies ist für das Beispiel bereits in der Tabelle angedeutet. Der Vorgang wiederholt sich, der nächste Chiffretextbuchstabe „errechnet“

sich aus dem nächsten Klartextbuchstaben und dem nächsten Schlüsselbuchstaben usw. Der Schlüssel wird periodisch verwendet, d.h. nach dem letzten Schlüsselwortbuchstaben wird wieder mit dem ersten fortgefahren usf. bis der gesamte Text verschlüsselt ist.

Anmerkung: Schlüsselzeile und Klartextspalte werden in den Verschlüsselungsvorgang mit einbezogen: Ist der Schlüsselbuchstabe ein „A“, so wird die erste Spalte links zur Verschlüsselung benutzt, der Klartextbuchstabe bleibt demzufolge unverändert. Entsprechendes gilt für den Fall, wenn der Klartext auf ein „A“ trifft. Dann wird der Schlüsselbuchstabe zum Buchstaben im Chiffretext.

Das Beispiel lässt die 4 Elemente eines jeden Chiffrierverfahrens gut erkennen:

1. Die **zu kodierende Information**, hier: der Klartext „DIESISTGEHEIM“.
2. Die **chiffrierte Information**, hier: „RAXWZFHYXLVVA“.
3. Der **Kodieralgorithmus** (auch Chiffrier- oder Verschlüsselungsalgorithmus), hier: Vigenère-Verfahren.
4. Der **Schlüssel**, der vom Kodieralgorithmus verwendet wird, hier: „OSTERN“.

Das Beispiel wird ein wenig verändert: Computer verarbeiten Informationen als Binärcode, d.h. die Daten liegen dem Rechner lediglich als „0“ oder „1“ vor. Stellt man das Vigenère-Quadrat bitweise dar, so liefert es eine erste Vorstellung davon, wie ein einfacher Verschlüsselungsalgorithmus in einem Rechner umgesetzt wird:

0	**1**
1	0

Abbildung 6: Bitweise dargestelltes Vigenère-Quadrat

Beispiel:

Klartext:	**1001 0101 1001**
Schlüssel:	**0110** 0110 0110
Chiffrierter Text:	**1111 0011 1111**

Die Verschlüsselung erfolgt analog zu dem klassischen Vigenère-Verfahren. Die Anwendung des gleichen Schlüssels auf den Chiffretext führt den Anwender wieder zum Klartext.

Diese Verschlüsselungsfunktion wird auch als „Addition modulo 2“ bezeichnet, die einer bitweisen Addition ohne Übertrag entspricht. In der Informatik ist dies die logische Operation XOR, die mathematische Schreibweise ist ⊕:

$$0 \oplus 0 = 0$$
$$0 \oplus 1 = 1 \oplus 0 = 1$$
$$1 \oplus 1 = 0$$

Doch auch jemand, der den Schlüssel nicht kennt, könnte den Klartext ermitteln. Das Gegenstück zur Kryptographie, die als *Kryptoanalyse*[39] bezeichnete „Lehre von der [unbefugten] Entschlüsselung von Geheimschriften“,[40] nutzt zwei Methoden, um eine Verschlüsselung zu brechen und so den geheimen Inhalt einer abgesicherten Nachricht für Unbefugte lesbar zu machen:

1. Ausprobieren aller möglichen Schlüssel.
2. Analytische Suche nach Schwachpunkten im Verschlüsselungsalgorithmus.

Der erste Fall wird im Englischen auch als *Brute-Force-Attack* bezeichnet, die zweite Methode wird im folgenden *Analytische Attacke* genannt.[41]

Der Schlüssel des Beispiels (0110) besitzt eine Länge von 4 Bit. Eine Brute-Force-Attack wäre hier schnell durchgeführt. Ein Außenstehender bräuchte höchstens $2^4 = 16$ mögliche Schlüssel auszuprobieren,[42] um den Klartext zu erhalten. Verlängert man den Schlüssel des Beispiels aber um ein Bit auf 5 Bit, so wären im Höchstfall bereits doppelt so viele, also $2^5 = 32$ Versuche notwendig. Grundsätzlich gilt: **Der Aufwand für eine Brute-Force-Attack erhöht sich mit der Schlüssellänge.**

Die analytische Attacke sucht nach Schwachpunkten im verwendeten Algorithmus. Diese äußern sich z.B. in Gesetzmäßigkeiten des Chiffretextes. So werden zwei identische Bitfolgen im Klartext (die z.B. den gleichen Buchstaben repräsentieren) in der Regel als verschiedene Chiffrebitfolgen ausfallen. Treffen diese übereinstimmenden Teile der Klartextbitfolge je-

---

[39] Kryptoanalyse und Kryptographie sind die beiden Teilgebiete, die zusammengenommen die *Kryptologie* bilden.

[40] Hagen Hagemann u.a.: Kryptologie – Interaktives Training, 1997, auf CD-ROM.

[41] Um Verwechslungen mit den Angriffen auf die unverschlüsselte Kommunikationsbeziehung (siehe Kapitel 2) zu vermeiden, bezeichnet „Attacke“ einen Angriff auf verschlüsselte Nachrichten bzw. auf die zugrunde liegenden Verschlüsselungssysteme oder -algorithmen.

[42] Im Durchschnitt aller Fälle ist er bei der Hälfte der möglichen Schlüsselanzahl am Ziel, also nach 8 Schlüsseln.

doch mehrere Male auf das gleiche Schlüsselstück, z.B. auf die ersten Bit des Schlüssels, sind die Chiffrebitfolgen identisch.[43] Mit analytischem Geschick ist somit die Schlüssellänge schnell ermittelt. In weiteren Analyseschritten können z.B. Häufigkeitsverteilungen benutzt werden, um an den Schlüssel zu gelangen. Bei einem verschlüsselten deutschsprachigen Text etwa wird die Bitfolge am häufigsten auftreten, die das „e“ repräsentiert.[44]

Heutige Verschlüsselungsalgorithmen versuchen diese Gesetzmäßigkeiten zu verwischen und analytischen Attacken standzuhalten, indem sie sowohl Zeichen durch andere ersetzen (*Substitution*) als auch die Reihenfolge der Zeichen vertauschen (*Transposition*).[45] Das ganze geschieht oftmals hintereinander in mehreren Verschlüsselungsläufen, sog. *Iterationen*. Die einzelnen Algorithmen unterscheiden sich dabei in der Gestaltung der einzelnen Iterationen voneinander und dies führt je nach Algorithmus zu qualitativ unterschiedlichen Ergebnissen. Allgemein gilt: **Die Stärke des Kryptosystems wird entscheidend von dem verwendeten Verschlüsselungsalgorithmus beeinflusst.**

Moderne kryptographische Verfahren müssen darüber hinaus den bereits in Kapitel 2 angesprochenen Grundsatz erfüllen, dass nicht allein schon die Benutzung des gleichen kryptographischen Systems einen Rückschluss von chiffrierter Nachricht auf den Ursprungstext zulassen darf. Selbst wenn der Verschlüsselungsalgorithmus ausreichend bekannt und erforscht ist, muss die Sicherheit der Verschlüsselung gewährleistet sein. Im Umkehrschluss heißt dies, die **Sicherheit der Verschlüsselung darf ausschließlich von der Geheimhaltung des Schlüssels abhängen**.

3.1.1 Symmetrische Verschlüsselung

Die in der Einführung verwendeten Verschlüsselungsverfahren sind Beispiele für die konventionelle, symmetrische Verschlüsselung. Verfahren dieser Art finden ihre Anwendung schon seit Jahrhunderten. Sie werden deshalb als symmetrisch bezeichnet, weil Sender und Empfänger sowohl zur Chiffrierung als auch Dechiffrierung mit dem gleichen Schlüssel arbeiten. Mit einem anderen Schlüssel kann die Nachricht nicht dechiffriert werden, wie Abbildung 7 zeigt.

---

[43] Entsprechendes ist bereits im ersten Beispiel zu erkennen: Das erste und das zweite „E“ im Klartext „DIESISTGEHEIM“ fallen zufällig beide auf das „T“ des Schlüsselwortes „OSTERN“; beide werden im Chiffretext zum „X“. Bei einer Analyse des Chiffretextes wären die aufeinanderfolgenden „X“ ein erstes Indiz für die Schlüssellänge von 6 Buchstaben.

[44] Vgl. DOS, Kryptologie-Special, April 1997, S. 250.

[45] Vgl. Bruce Schneier, Angewandte Kryptographie, 1996, S. 11.

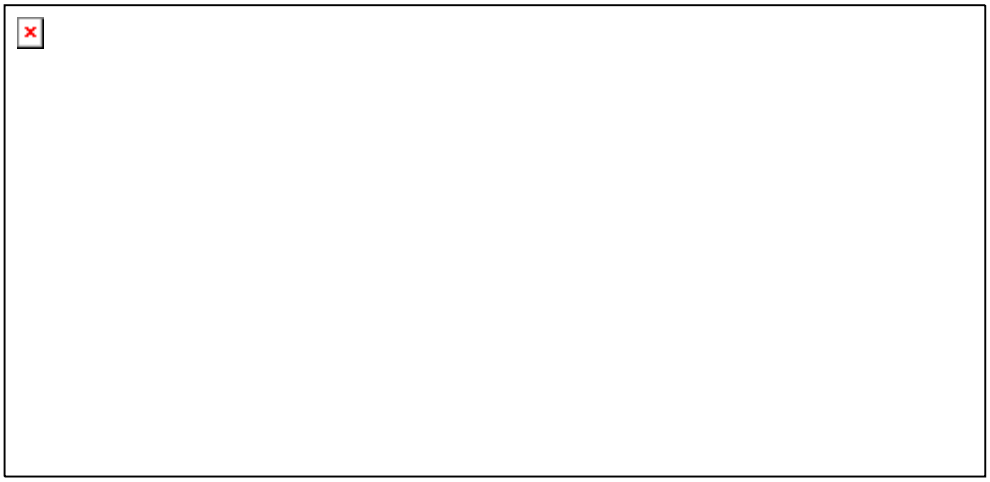


Abbildung 7: Symmetrische Verschlüsselung[46]

Symmetrische Verschlüsselung wird auch *Kryptographie mit geheimen (privaten) Schlüsseln* genannt, weil der Schlüssel nur dem Sender und dem Empfänger bekannt sein darf und folglich geheim gehalten werden muss. Gerät der Schlüssel in die Hände eines Dritten, so ist auch dieser in der Lage, die chiffrierte Nachricht zu entschlüsseln.

Haben sich Sender und Empfänger auf ein symmetrisches Verschlüsselungsverfahren geeinigt, muss als nächster Schritt dem Kommunikationspartner der Schlüssel mitgeteilt werden. Und hier steckt das Problem: Ein Medium wie das Internet kommt hierfür aufgrund der bekannten Sicherheitsrisiken nicht in Frage, der Schlüssel könnte *kompromittiert* werden. Akzeptabel wäre der Vorschlag, einen zuverlässigen Kurier mit der Schlüsselübergabe zu vertrauen, eine sichere Lösung bleibt allerdings nur die persönliche Übergabe.

Das Problem verschärft sich, je mehr Parteien miteinander auf Basis symmetrischer Verschlüsselung kommunizieren möchten. Bereits bei 5 Beteiligten müssen insgesamt 10 Schlüssel ausgetauscht werden. Bei 10 Parteien sind bereits 45 Schlüssel notwendig, bevor jeder mit jedem chiffrierte Nachrichten austauschen kann. Die Anzahl der Schlüssel steigt mit der Zunahme der Kommunikationspartner überproportional an. Allgemein betrachtet verhält sich dieser Zusammenhang folgendermaßen: [47]

Schlüsselanzahl = [n*(n-1)]/2,

---

[46] Abb aus: Richard E. Smith, Internet-Kryptographie, 1996, S. 23.

[47] Vgl. Simson Garfinkel, PGP: Pretty Good Privacy, 1996, S. 51.

wobei n die Anzahl der Kommunikationsparteien darstellt. Ein Unternehmen mit 2000 Mitarbeitern müsste also 1.999.000 Schlüssel generieren und austauschen, bevor eine uneingeschränkte verschlüsselte Kommunikation möglich wäre. Dies wäre sehr zeit- und kostenintensiv.

3.1.2 Asymmetrische Verschlüsselung

Das Problem der Schlüsselverteilung wird gelöst durch asymmetrische Verschlüsselungsverfahren. Die erstmalige Beschreibung eines solchen Verfahrens wurde 1976 von Whitfield Diffie und Martin Hellman veröffentlicht.[48] Die Asymmetrie besteht darin, dass zur Ver- und Entschlüsselung nicht mehr der gleiche Schlüssel benutzt wird, sondern ein Schlüsselpaar, bestehend aus *öffentlichem Schlüssel (public key)* zur Chiffrierung und *privatem Schlüssel (private key)* zur Dechiffrierung. Aufgrund des Gebrauchs eines öffentlichen Schlüssels werden solche Verfahren auch Public-Key-Verschlüsselungsverfahren genannt.

Der entscheidende Punkt des Verschlüsselungsverfahrens: Man kann den privaten Schlüssel nicht aus dem öffentlichen Schlüssel ableiten. Daraus resultiert der Vorteil, dass der zur Chiffrierung benutzte öffentliche Schlüssel nicht der Geheimhaltung unterliegt und jedermann bekannt gegeben werden darf. Ein aufwendiger geheimer Schlüsselaustausch ist nicht notwendig und kann durch jede andere Mitteilungsform ersetzt werden, die Sicherheit einer chiffrierten Nachricht wird dadurch in keiner Weise beeinträchtigt. Denn **die Dechiffrierung ist nur mit dem privaten Schlüssel möglich**, nur dieser muss geheim gehalten werden.

[48] Whitfield Diffie; Martin E. Hellman: New Directions in Cryptography, in: IEEE Transactions on Information Theory 1976, Vol. IT-22, S. 644 – 654 (lt. Bruce Schneier, Angewandte Kryptographie).

Der Sender einer Nachricht nutzt folglich den **öffentlichen Schlüssel des Empfängers, um eine Nachricht zu verschlüsseln.** Nur der Empfänger kann die Nachricht wieder mit Hilfe seines privaten Schlüssels entschlüsseln. Die Abbildung 8 zeigt dieses Prinzip.

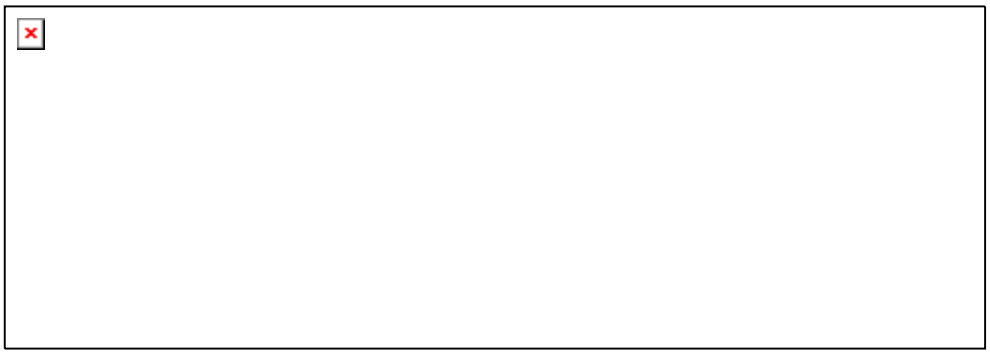


Abbildung 8: Prinzip der Public-Key-Kryptographie[49]

Asymmetrische Verschlüsselungsverfahren erlauben es dem Anwender aber auch, Daten mit dem privaten Schlüssel zu chiffrieren. Diese kann jedermann wieder mit Hilfe des öffentlichen Schlüssels dechiffrieren. Dadurch soll keine Vertraulichkeit erreicht werden, sondern vielmehr stellt dieses Verfahren sicher, dass die kryptographische Operation vom Inhaber des bestimmten privaten Schlüssels durchgeführt wurde.[50] Der Empfänger kann nunmehr sicher sein, dass der Sender die Nachricht verschickt hat – die Chiffrierung entspricht somit der digitalen Unterschrift. Kapitel 3.2.2.2 beschreibt, wie ein solches Verfahren in PGP die Implementierung digitaler Unterschriften/Signaturen ermöglicht.

3.2 Kryptographische Algorithmen in PGP

Der Vorteil des einfachen Schlüsselaustausches wird jedoch dadurch relativiert, dass in Computerprogrammen verwendete asymmetrische Verschlüsselungsalgorithmen im Vergleich zu symmetrischen Algorithmen wesentlich rechenintensiver und daher bis um den Faktor 1000 langsamer sind.[51] Um dieses Problem zu umgehen, geht PGP in zwei Schritten vor. Zunächst wird der Klartext mit einem symmetrischen Schlüssel chiffriert. Nur dieser auch Sitzungsschlüssel genannte Schlüssel wird anschließend mit einem asymmetrischen Verschlüsselungsalgorithmus verschlüsselt. Der symmetrisch verschlüsselte Text und der asymmetrisch verschlüsselte

---

[49] Abb. aus: Homepage von Jens Kirchner, http://www.fto.de/fthp/kirchner/d_index.htm. Stand 12.11.1998

[50] Vgl. Richard E. Smith, Internet-Kryptographie, 1996, S. 217.

[51] Vgl. Network Associates, Dokumentation zu PGP 6.0 Freeware, Intro to Crypto, 1998, S. 17.

Sitzungsschlüssel werden dann an den Empfänger übertragen. Auf diese Weise kombiniert PGP die Vorteile beider Verfahren, die Abbildung 9 veranschaulicht den Vorgang.

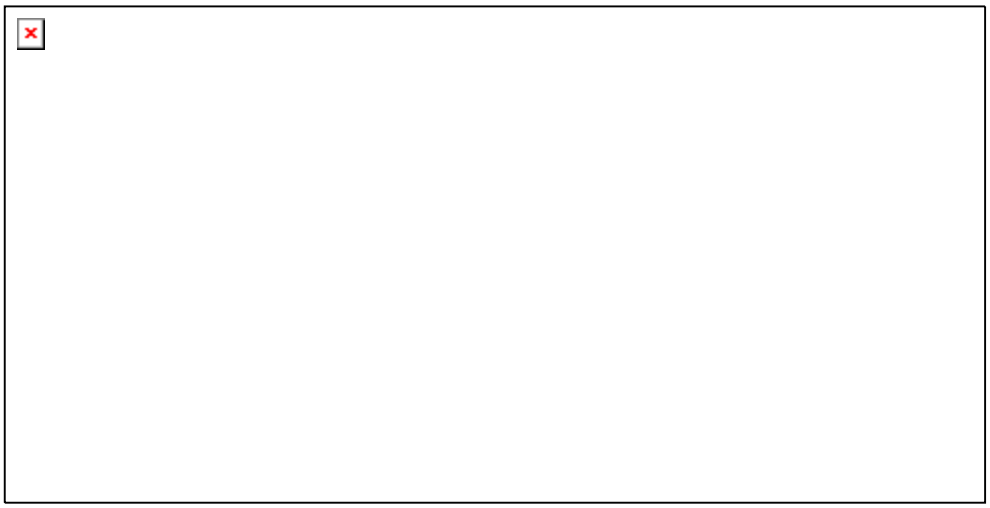


Abbildung 9: Symmetrische und asymmetrische Verschlüsselungsalgorithmen in PGP[52]

Die Dechiffrierung ist entsprechend spiegelbildlich zu sehen. Das PGP-Programm des Empfängers dechiffriert zunächst den Sitzungsschlüssel und mit dem Sitzungsschlüssel entschlüsselt es anschließend den Text.

3.2.1 Symmetrische Verschlüsselungsalgorithmen

PGP nutzt seit der Version 5.0 zur Verschlüsselung des Klartextes optional drei Verschlüsselungsalgorithmen:[53]

- **IDEA,**
  International Data Encryption Algorithm,
- **Triple-DES,**
  eine dreifache Anwendung des Data Encryption Standard (DES) und
- **CAST,**
  benannt nach den Erfindern Carlisle Adams und Stafford Tavares.

Diese Algorithmen sind *Blockchiffren*. Im Gegensatz zum Einführungsbeispiel wird nicht ein Strom binärer Daten verschlüsselt (sog. *Stromchiffre*), sondern es werden mehrere Bits zu einer Gruppe zusammengefasst und gemeinsam verschlüsselt. Klartextblöcke und Chiffretextblöcke weisen

---

[52] Vgl. Network Associates, Dokumentation zu PGP 6.0 Freeware, Intro to Crypto, 1998, S. 16.

[53] PGP 2.x-Versionen benutzen ausschließlich IDEA als symmetrischen Verschlüsselungsalgorithmus.

Längen von jeweils 64 Bit auf. Die Schlüssellänge beträgt bei CAST und IDEA 128 Bit, bei Triple-DES 164 Bit.[54] Aus Platzgründen ist eine genaue Beschreibung der Arbeitsweise am Beispiel des Chiffrieralgorithmus IDEA im Anhang zu finden, siehe Seite 102.

Die Algorithmen werden von PGP im *Cipher-Feedback-Modus (CFB)* angewendet. In diesem Modus wird ein Chiffrieralgorithmus nicht direkt zur Verschlüsselung der Daten, sondern zur Erzeugung eines temporären Schlüssels benutzt, wie die folgende Abbildung veranschaulicht:

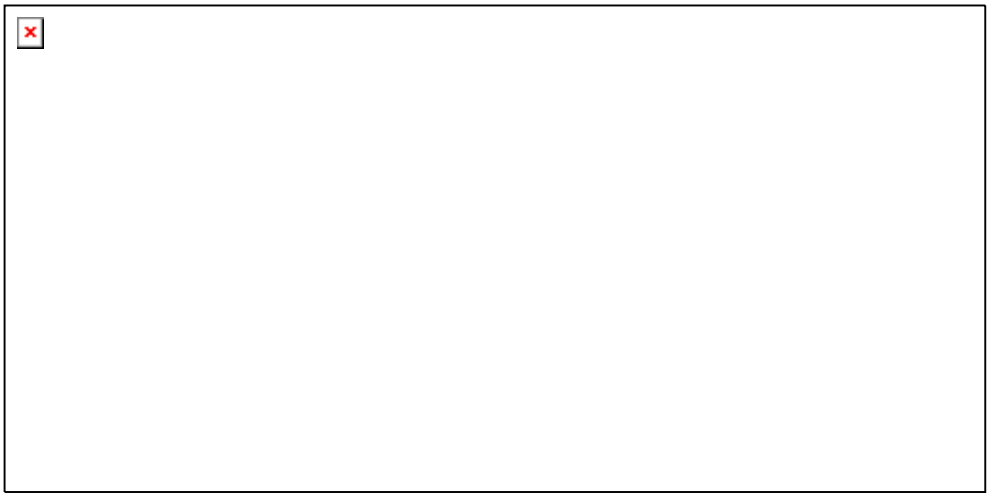


Abbildung 10: Vorgang der symmetr. Verschlüsselung im Cipher-Feedback-Modus

Der Verschlüsselungsvorgang beginnt mit der Erzeugung einer zufälligen Bitfolge, in der Abbildung als *Initialisierungsvektor* bezeichnet. Diese Bitfolge wird nun durch den symmetrischen Blockchiffrieralgorithmus (in der Abbildung: IDEA) unter Verwendung des geheimen und ebenfalls durch Zufallsroutinen erzeugten Sitzungsschlüssels chiffriert. Dadurch wird ein temporärer Schlüssel erzeugt, der durch eine einfache XOR Verknüpfung den Klartext in Chiffretext umwandelt. Dieser Chiffretext dient wieder als Ausgangspunkt zur Erzeugung des nächsten temporären Schlüssels usw.[55]

Die Verschlüsselung im CFB-Modus bewirkt, dass gleiche Klartextblöcke nicht in zwei identische, sondern in verschiedene Chiffretextblöcke umgewandelt werden, siehe Abbildung 10.

---

[54] Die effektive Schlüssellänge für den Fall einer Brute-Force-Attack ist jedoch lediglich 112 Bit. Siehe Alexandra und Hubert Weikert, Kryptographie mit dem Computer, 1997, S. 16.

[55] Vgl. Richard E. Smith, Internet-Kryptographie, 1996, S. 57f; Abb. S. 58.

3.2.2 Asymmetrische Verschlüsselungsalgorithmen

Die in PGP implementierten asymmetrischen Verschlüsselungsverfahren[56] werden in zweifacher Hinsicht genutzt:

1. Verschlüsselung des Sitzungsschlüssels,
2. Erzeugung digitaler Signaturen.

3.2.2.1 Verschlüsselung

PGP verwendet zwei asymmetrische Verschlüsselungsalgorithmen, zwischen denen der Anwender bei der Generierung des eigenen öffentlichen Schlüssels (siehe Kapitel 0) wählen kann.[57]

- **Algorithmus nach Rivest, Shamir und Adleman (RSA)**

  Der RSA-Algorithmus wurde 1978 veröffentlicht und nach seinen Erfindern benannt. Er macht sich das mathematische Problem zunutze, dass es relativ einfach ist, große Primzahlen (100 Dezimalstellen und mehr) zu finden und miteinander zu multiplizieren, es aber selbst für Großrechner nicht in angemessener Zeit möglich ist, das Ergebnis wieder in seine Primfaktoren zu zerlegen.[58]

  Sowohl öffentlicher als auch privater Schlüssel bestehen aus einem Zahlenpaar. Die zweite Hälfte des Zahlenpaares ist in beiden Schlüsseln das Ergebnis der Multiplikation zweier Primzahlen. Die erste Schlüsselhälfte wird jeweils aus einem der zuvor genutzten Primfaktoren abgeleitet.[59] Im Anhang findet sich eine Erklärung des Prinzips der Schlüsselfindung, siehe Seite 103.

  Folgendes Beispiel[60] zeigt den Chiffriervorgang anhand kleiner Schlüssel, errechnet aus den Primzahlen 7 und 17.

---

[56] PGP 2.x-Versionen benutzen ausschließlich RSA als asymmetrischen Verschlüsselungsalgorithmus.

[57] Ob auch in folgenden PGP-Versionen beide Algorithmen zum Einsatz kommen, ist fraglich. Zur Zeit liegt die Version 6.0 Freeware vor, die aufgrund US-patentrechtlicher Bestimmungen lediglich das Public-Key-Verfahren nach Diffie und Hellman benutzt..

[58] Vgl. Hagen Hagemann u.a.: Kryptologie – Interaktives Training, 1997, auf CD-ROM, Kap. 2.2.2.

[59] Vgl. Hagen Hagemann u.a.: Kryptologie – Interaktives Training, 1997, auf CD-ROM, Kap. 2.2.2.

[60] Bsp. aus: William Stallings, Datensicherheit mit PGP, 1995, S. 241.

Öffentlicher Schlüssel:	**5** und **119**
Privater Schlüssel:	**77** und **119**
Ausgangstext:	*19*
Verschlüsselung:	$19^{5} = 2476099$ 2476099 / **119** = 20807 Rest 66
Chiffrierter Text:	*66*
Entschlüsselung:	$66^{77} = 1{,}27 * 10^{140}$ $(1{,}27 * 10^{140}) /$ **119** $= 1{,}06 * 10^{138}$ Rest 19
Ausgangstext:	*19*

Abbildung 11: Beispiel zur RSA-Chiffrierung

- **Algorithmus nach Diffie und Hellman (DH)**

  Der Algorithmus nach Diffie und Hellman beruht darauf, dass die Berechnung diskreter Logarithmen im Gegensatz zur Potenzierung sehr schwierig ist. Eine genauere Erläuterung der Schlüsselfindung und des Chiffrierprozesses erfordert einen umfangreichen zahlentheoretischen Hintergrund, hier sei auf ausführlicher gehaltene Literatur verwiesen.[61]

3.2.2.2 Digitale Signaturen

Digitale Signaturen stellen das Prinzip der Public-Key-Verschlüsselung „auf den Kopf“: Der Anwender verschlüsselt Daten mit dem eigenen privaten Schlüssel, folglich kann jeder, der im Besitz seines öffentlichen Schlüssels ist, diese Daten auch wieder entschlüsseln. Dem Absender geht es hier jedoch weniger um die Geheimhaltung seiner Nachricht. Dahinter steckt die Idee, dass ein öffentlicher Schlüssel nur solche Daten entschlüsseln kann, die mit dem dazugehörigen privaten Schlüssel chiffriert wurden.[62] Und da der private Schlüssel lediglich in der Hand einer Person ist, kann nur diese Person die Nachricht abgeschickt haben. Der Empfänger authentifiziert mit dem öffentlichen Schlüssel den Absender und erhält so Antwort auf die Frage, ob die Nachricht auch tatsächlich von dem angegebenen Absender stammt.

---

[61] Reinhard Wobst, Abenteuer Kryptologie, enthält auf S. 169f eine Abhandlung über die PGP zugrunde liegende Variante des DH-Verfahrens ElGamal.

[62] Strenggenommen findet bei einer Signatur mit dem privaten Schlüssel die mathematische Funktion der Dechiffrierung der Daten statt, die durch den öffentlichen Schlüssel wieder chiffriert werden. Vgl. Reinhard Wobst, Abenteuer Kryptologie, S 261.

Doch auch hier tritt wieder das Problem auf, das die Verschlüsselung des ganzen Textes auf Basis eines asymmetrischen Verschlüsselungsalgorithmus zu aufwendig ist.

PGP stellt der digitalen Signatur daher eine *Einweg-Hashfunktion* voraus. Eine Hashfunktion ist ein sehr kompliziert aufgebauter Algorithmus, der aus einem beliebig langen Klartext ein immer gleich langes Komprimat, den *Message Digest* errechnet. Dieser stellt in Form eines Zahlenwertes einen individuellen digitalen „Fingerabdruck" des Dokumentes her. Da es sich um eine Einwegfunktion handelt, ist es praktisch unmöglich, aus dem Message Digest den Ursprungstext zu rekonstruieren. Andererseits erlaubt es der Message Digest aufgrund seiner Individualität, für jedes Dokument festzustellen, ob eine Nachricht auf dem Kommunikationswege evtl. verändert wurde. Veränderungen im Ursprungstext, und sei es nur das Hinzufügen eines Leerzeichens, führen zu einem anderen „Fingerabdruck" des Dokuments. Aufgrund der Komplexität eines Hash-Algorithmus würde eine genaue Beschreibung der zugrunde liegenden Algorithmen an dieser Stelle zu weit führen. Am Beispiel des MD5-Verfahrens wird dies im Anhang auf Seite 103 nachgeholt.

Die Signatur entsteht nun durch die Verschlüsselung des Message Digest mit dem privaten Schlüssel des Senders. Der Empfänger kann mit der *Verifizierung* genannten Prüfung der Signatur folglich zwei Dinge prüfen:

1. **Die Authentizität des Absenders,**
   wenn die Entschlüsselung des Message Digest mit dem öffentlichen Schlüssel des Absenders erfolgreich ist, und

2. **die Integrität der Nachricht,**
   indem PGP erneut einen Message Digest der Nachricht erzeugt und diesen mit dem entschlüsselten Message Digest vergleicht. Bei Übereinstimmung steht fest, dass die Nachricht unverändert angekommen ist.

PGP nutzt zwei einander sehr ähnliche[63] Hashfunktionen, abhängig von dem benutzten asymmetrischen Verschlüsselungsalgorithmus:

[63] Vgl. William Stallings, Sicherheit im Datennetz, 1995, S. 351.

- **MD5 (Message Digest 5)** erzeugt in Verbindung mit RSA einen Message Digest von 128 Bit Länge,
- **SHA-1 (Secure Hash Algorithm)** ist Bestandteil des vom DH-Algorithmus verwendeten **DSS (Digital Signature Standard)**, der Message Digest hat hier eine Länge von 160 Bit.

Die nächste Abbildung stellt die Erzeugung der digitalen Unterschrift und die Verifizierung bildlich dar:[64]

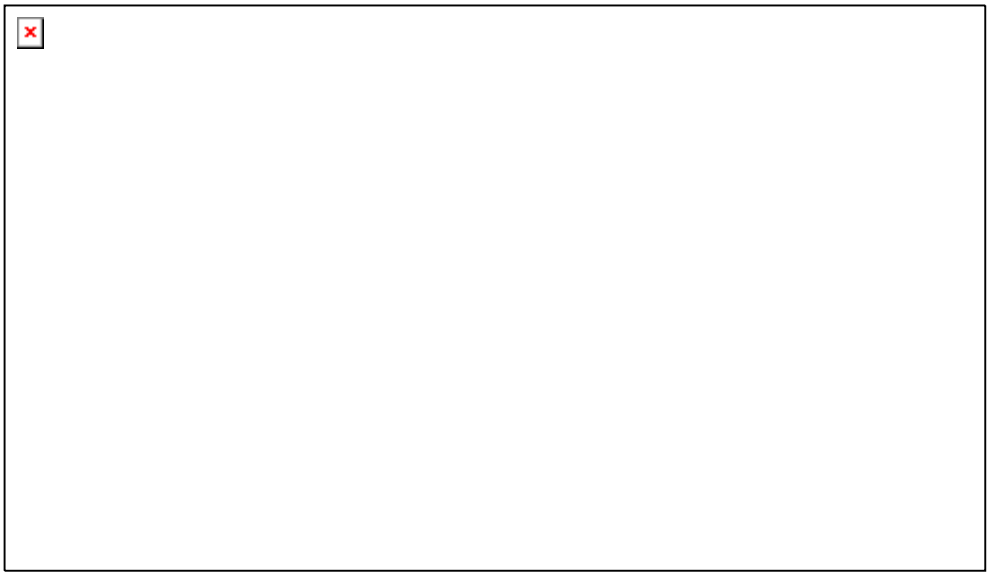


Abbildung 12: Hashfunktion und digitale Unterschrift

3.2.3 Die Verschlüsselung mit PGP in der Übersicht

Um eine Übersicht über die Funktionsweise PGPs zu bekommen, wird der Prozess der Datenverschlüsselung und Signatur im Folgenden zusammengefasst und mit einigen Ergänzungen, die noch nicht beschrieben wurden, Schritt für Schritt dargestellt. Anzumerken ist, dass PGP nicht nur Texte, sondern auf dieselbe Weise ganze Dateien beliebigen Formates verarbeiten kann. Chiffrierung und Signierung können sowohl einzeln als auch zusammen benutzt werden.

---

[64] Abb. aus: William Stallings, Datensicherheit mit PGP, 1995, S. 33.

3.2.3.1 Chiffrierung und Signierung

1. **Erzeugung der Signatur**
   Wenn der Absender eine digitale Unterschrift benötigt, erzeugt PGP mittels einer Hashfunktion (MD5 bzw. SHA-1/DSS) den Message Digest der Datei.

   Der Message Digest wird mit dem persönlichen Schlüssel des Absenders durch den RSA- bzw. DH-Algorithmus chiffriert. Der chiffrierte Message Digest stellt die Signatur dar.

2. **Komprimierung**
   Im nächsten Schritt komprimiert PGP den Text und die Signatur zu einem kompakten Datenblock. Das Programm benutzt die *ZIP-Komprimierungsroutinen*, wie sie auch aus dem Komprimierungsprogramm PKZIP bekannt sind. Sinn der Komprimierung: Die Komprimierung beseitigt Datenredundanzen, die andernfalls Ausgangspunkt einer Kryptoanalyse sein könnte. Zudem spart das kleinere Datenvolumen Übertragungszeit.

3. **Chiffrierung**
   Zur Chiffrierung erzeugt PGP zunächst einen zufälligen einmaligen Sitzungsschlüssel. Dieser Schlüssel dient einem symmetrischen Verschlüsselungsalgorithmus (IDEA, CAST oder Triple-DES) zur Chiffrierung von Text und Signatur.

   Der Sitzungsschlüssel wiederum wird mit dem öffentlichen Schlüssel des Empfängers mittels RSA- oder DH-Verfahren chiffriert.

4. **Umwandlung in das ASCII-Format**
   Der durch die Verschlüsselung entstandene binäre Datenblock wird in das druckfähige ASCII-Format umgewandelt. Die so entstandenen druckfähigen Zeichen können durch jedes E-Mail-System problemlos verarbeitet werden.[65]

3.2.3.2 Dechiffrierung und Verifizierung

1. **Rückumwandlung in binäre Daten**
   Die ASCII-Zeichen werden wieder in binäre Daten umgeformt.

---

[65] Die Umwandlung von verschlüsselten **Dateien** in druckfähige ASCII-Zeichen ist i.A. nicht erforderlich, weil Dateien von MIME-fähigen E-Mail-Programmen als Attachment in ihrem ursprünglichem Dateiformat verschickt werden können. Die Umwandlung erfolgt daher optional.

2. **Dechiffrierung**
   Zunächst wird der Sitzungsschlüssel mit dem privaten Schlüssel des Empfängers dechiffriert.

   Der Sitzungsschlüssel kann nun zur Dechiffrierung der Daten genutzt werden.

3. **Dekomprimierung**
   Text und Signatur werden wieder dekomprimiert

4. **Prüfung der Signatur**
   Text und Signatur werden getrennt, der Text liegt nun wieder in seiner Ausgangsform als Klartext vor.

   Der Message Digest wird mit dem öffentlichen Schlüssel des Senders dechiffriert.

   PGP errechnet erneut einen Message Digest aus dem Klartext und vergleicht diesen mit dem entschlüsselten Message Digest, um so die Signatur auf Echtheit zu prüfen.[66]

Im Anhang auf Seite **Fehler! Textmarke nicht definiert.** finden sich die beschriebenen Vorgänge in einer bildlichen Darstellung wieder.

3.3 Einschätzung der Sicherheit von PGP

In Kapitel 3.1 wurde bereits auf die Kryptoanalyse hingewiesen. Um die Sicherheit von PGP beurteilen zu können, wird kurz auf die Anwendung kryptoanalytischer Attacken auf PGP eingegangen.

3.3.1 Analytische Attacken

Der Quellcode von PGP ist frei erhältlich und folglich sind auch die in PGP benutzen Algorithmen von Kryptoanalytikern gut erforscht. In der Literatur[67] finden sich daher auch unterschiedliche Ansätze, die verwendeten Algorithmen analytisch zu „knacken“. Bei diesen Ansätzen jedoch blieb es, keiner führte zu einem Erfolg. Da man nur vermuten kann, ob jemals eine analytische Attacke auf PGP gelingen wird, nutzt man die Angaben über

---

[66] Vgl. William Stallings, Datensicherheit mit PGP, 1995, S. 38ff.

[67] Insbesondere bei Reinhard Wobst, Abenteuer Kryptologie.

die Zeitdauer des Durchprobierens aller Schlüssel, um eine Vorstellung von der Sicherheit PGPs zu erhalten.

3.3.2 Brute-Force-Attacke

Die Dauer einer Brute-Force-Attacke wird in erster Linie von zwei Faktoren bestimmt:

- Länge des Schlüssels,
- Rechengeschwindigkeit des Computers, der die Schlüssel prüft.

Beispielrechnungen und Tabellen zu dieser Thematik finden sich in nahezu allen Büchern zur Kryptologie. Beispielhaft steht hier eine Zahl von Richard E. Smith,[68] der für einen 128 Bit IDEA-Schlüssel eine mittlere Suchzeit von $2*10^{18}$ Jahren veranschlagt. Diese Zeit würde ein Rechner brauchen, dessen Leistungsfähigkeit die eines gewöhnlichen PC um ein Vielfaches übertrifft und $3*10^9$ Schlüssel in der Sekunde testet. Für die Faktorisierung eines Public-Key-Schlüssels der Länge von 1024 Bit wird bei gleicher Rechenleistung ungefähr dieselbe Zeitdauer veranschlagt,[69] wobei diese Zeit nicht unbedingt zur Faktorisierung eines PGP-Schlüssels ausreichen würde, denn PGP generiert Public-Keys bis zu 4096 Bit Länge.

Fazit: Für den Anwender sind dies nur Gedankenspielereien, deren weitere Erläuterung sich im Rahmen dieses Buches erübrigt. An gegebenen Stellen in den folgenden Kapiteln wird wiederholt darauf hingewiesen, dass sich Gefahren für verschlüsselte Daten weniger durch kryptoanalytische Attaken als durch Fehler in der Handhabung von PGP ergeben können.

Darüber hinaus sind Gefahren aufgrund gefälschter öffentlicher Schlüssel denkbar. Eine Absicherung gegen gefälschte Schlüssel stellt das *Web of Trust*, (Netz des Vertrauens) dar, das im Folgenden kurz vorgestellt wird.

---

[68] Richard E. Smith, Internet-Kryptographie, 1996, S. 67.

[69] Vgl. Referat von Prof. Dr. Albrecht Beutelspacher in Hamm, Rainer; Möller, Klaus Peter: Datenschutz durch Kryptographie: ein Sicherheitsrisiko? 1998, S. 35.

3.4 Das Web of Trust

Als Voraussetzung einer sicheren Kommunikation auf Basis eines asymmetrischen Verschlüsselungssystems muss sich der Anwender darauf verlassen können, dass der öffentliche Schlüssel eines Kommunikationspartners

1. echt ist, d.h. auch tatsächlich zu der bestimmten Person gehört und nicht von einem Dritten generiert wurde,
2. auf dem Wege der Übermittlung nicht gefälscht wurde.

PGP versieht jeden öffentlichen Schlüssel mit einem *Fingerabdruck (Fingerprint)*, wie er schon aus Kapitel 3.2.2.2 von der digitalen Signatur her bekannt ist. Der Fingerabdruck wird im Falle eines RSA-Schlüssels durch das oben angesprochene MD5-Verfahren erzeugt. Der 128 Bit lange Fingerabdruck ist in 16 Hexadezimalzahlen[70] angeordnet, jede Zahl genau ein Byte (=8 Bit) lang.

Ein Beispiel für einen Fingerabdruck eines RSA-Schlüssels ist diese Zahlenfolge:

93 C3 71 AC 32 66 87 84 42 62 E6 00 FF CE BB 0D

Der Fingerabdruck eines Diffie-Hellman-Schlüssels hat dagegen eine Länge von 160 Bit, weil er durch das SHA-1 Verfahren erzeugt wird. Folglich wird dieser durch 20 Hexadezimalzahlen[71] von je ein Byte Länge dargestellt, Beispiel:

4B BB BC DF F6 CA A4 08 4F8E 57 18 CF 96 1C B1 91 A4 9D 54

So wie der Message Digest einer Nachricht ist auch der Fingerabdruck eines jeden Schlüssels einzigartig. Eine Änderung des Schlüssels würde auch eine Änderung des Fingerabdrucks bewirken – der Fingerabdruck eignet sich daher dafür, die Echtheit eines Schlüssels zweifelsfrei zu prüfen.

Der Fingerabdruck des Schlüssels, den der Anwender erhalten hat, kann mit dem Fingerabdruck verglichen werden, den der Kommunikationspartner angibt. Dies kann z.B. telefonisch geschehen, oftmals wird der Fingerabdruck aber auch auf Visitenkarten abgedruckt oder unter jede E-Mail angefügt.

---

[70] Jede Zahl besteht aus 2 Ziffern, insgesamt besteht der RSA-Fingerabdruck also aus 32 Hexadezimalziffern.

[71] Bzw. 40 Hexadezimalziffern.

Stimmt der Fingerabdruck des Schlüssels mit den Angaben des Schlüsselinhabers überein, kann sich der Anwender der Echtheit und Unverfälschtheit des öffentlichen Schlüssels sicher sein. Er bezeugt dies, indem er diesen öffentlichen Schlüssel signiert. Damit erhält der Schlüssel für den Anwender *Validity*, zu deutsch *Gültigkeit*.

Nur ein gültiger Schlüssel kann von dem Anwender anschließend eine weitere Eigenschaft erhalten: *Trust*, zu deutsch *Vertrauen*. Hiermit wird der betreffende Schlüsselbesitzer eingeschätzt von „untrusted = nicht vertrauenswürdig“ über „marginal = begrenzt vertrauenswürdig“ bis hin zu „complete = voll vertrauenswürdig“.

Hat der Anwender einen Schlüsselbesitzer als voll vertrauenswürdig eingestuft, so erhält jeder fremde Schlüssel, den dieser Schlüsselbesitzer signiert hat, auch für den Anwender volle Gültigkeit. Folglich braucht der Anwender sich nicht mehr um die Echtheit dieser fremden Schlüssel zu sorgen, denn die Echtheit hat ja bereits sein vertrauenswürdiger Kommunikationspartner bestätigt. In der Abbildung 13 genießt B das volle Vertrauen von A. Person B signiert den Schlüssel von C. Dieser Schlüssel hat nun auch Gültigkeit für A.

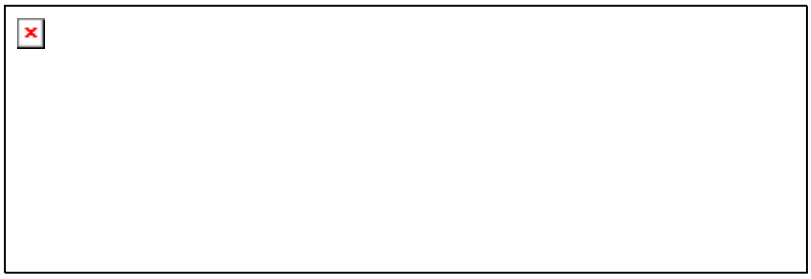


Abbildung 13: Web of Trust

Darüber hinaus hat A die Möglichkeit, B als *Meta-Introducer* zu deklarieren. Signiert dieser den Schlüssel von C mit dem Zusatz *Trusted Introducer*, so ist der Schlüssel von C für A nicht nur gültig, sondern C ist für A auch vertrauenswürdig: Schlüssel weiterer Personen, die von C signiert wurden, werden auch für A gültig, wie Abbildung 14 zeigt.

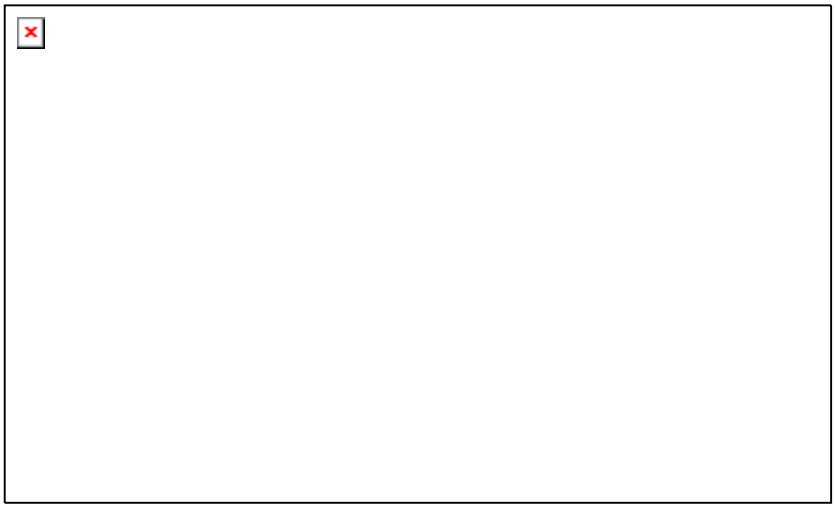


Abbildung 14: Web of Trust mit Meta-Introducer

Man kann nun die Beispiele weiterführen und sich ein weites Netz an Verflechtungen denken. Ein solches Netz wird auch als Web of Trust bezeichnet, das Netz des Vertrauens.

3.5 Key Server und Trustcenter

Im Internet existieren eine Reihe von Datenbanken, die öffentliche Schlüssel sammeln und auf Anfrage zur Verfügung stellen. Diese Datenbanken werden *Key Server* genannt und erleichtern die Schlüsselverteilung erheblich. PGP 5.5.3 bietet dazu eine komfortable Schnittstelle an (siehe Kapitel 4.2.2 Funktion SEARCH), mit der eigene Schlüssel an einen Key Server übermittelt und fremde Schlüssel anhand bestimmter Kriterien gesucht werden können.

Die Key Server des „pgp.net“ (zu erkennen an der Endung, z.B. bei http://wwwkeys.de.pgp.net, dies ist der deutsche Key Server des pgp.net) und einige weitere Key Server bilden ein Netzwerk, indem sie die Schlüssel untereinander austauschen und somit ihren Bestand ständig aktualisieren.[72] Für den Anwender ist es daher lediglich erforderlich, seinen Schlüssel nur an einen Key Server zu schicken und nur auf einem Key Server nach weiteren Schlüsseln zu suchen.

Ein *Trustcenter*, zu deutsch „Zentrum des Vertrauens“, ist ein Key Server, der über die Funktion des Schlüsselverteilers hinaus als *Zertifizierungsstelle* dient. Gegen Entrichtung einer Gebühr zertifiziert das Trustcenter

[72] Vgl. Michael Uplawski, Deutsche Übersetzung der comp.security.pgp FAQ, Version 1.5, Kapitel 8.1. URL: http://www.iks-jena.de/mitarb/lutz/security/pgpfaq.html. Stand 14.12.1998.

mittels seiner Signatur den öffentlichen Schlüssel des Antragstellers. Damit bestätigt das Trustcenter, dass zu dem signierten öffentlichen PGP-Schlüssel auch eine genau bestimmte Person gehört.[73] Vorher stellt das Trustcenter sicher, dass der Schlüsselinhaber auch der ist, der er vorgibt zu sein, etwa durch Kontrolle des Personalausweises.

Ein Dritter kann nun allein anhand des Fingerprints des Trustcenters feststellen, ob der zertifizierte Schlüssel echt ist. Der Fingerprint ist bei dem Trustcenter zu erfahren, z.B. über eine Website. Eine andere Möglichkeit ist die Überprüfung des Zertifikats anhand einer öffentlichen Zertifikatsdatenbank, in der Kopien sämtlicher Zertifikate, die das Trustcenter ausgegeben (oder auch zurückgezogen) hat, gespeichert sind.

Ein Trustcenter wird auch Zertifizierungsstelle genannt, oftmals wird die englische Bezeichnung *Certificate Authority (CA)* oder *Public Certification Authority (PCA)* gewählt.

Eine besondere Rolle werden in Zukunft Zertifizierungsstellen einnehmen, die von staatlicher Stelle nach strengen Vorschriften geprüft werden und eine Genehmigung von der Regulierungsbehörde Telekommunikation und Post (RegTP) erhalten. Sie können öffentliche Schlüssel gemäß des Signaturgesetzes zertifizieren, wodurch Signaturen mit dem dazugehörigen privaten Schlüssel Beweiskraft vor Gericht erhalten, siehe Kapitel 5.4.

Im Anhang auf Seite 106ff findet sich ein Verzeichnis über Adressen von Key Servern und Trustcentern.

---

[73] Vgl. DOS, Kryptologie-Special, April 1997, S. 228.

4 Die Anwendung der Software PGP

In diesem Kapitel erfahren Sie:

- wie PGP sowohl auf dem Rechner des Administrators als auch auf den Clients installiert wird,
- wie PGP-Schlüssel generiert und verwaltet werden,
- wie PGP-Schlüssel mit Hilfe einer Passphrase, dem sog. „Mantra“, vor fremden Zugriff geschützt werden,
- wie E-Mails und andere Daten verschlüsselt, signiert, entschlüsselt und verifiziert werden,
- welche Optionen sich bei dem Programm PGP 5.5 einstellen lassen, wie man sie einstellen sollte und weitere Einzelheiten zur Anwendung von PGP.

Die Herstellerfirma Network Associates gibt für Computer, auf denen PGP Version 5.5 for Business Security ausgeführt werden soll, folgende **Systemanforderungen** an:[74]

- Windows 95, 98 oder NT mit 8 MB RAM und 15 MB freiem Festplattenspeicher oder
- Macintosh System 7.5.3 oder höher mit 68030er Prozessor oder höher, mit 8 MB RAM und 10 MB freiem Festplattenspeicher oder
- UNIX System mit Sun Solaris 2.5.1 oder höher, HP-UX 9.0 oder höher, IBM AIX 3.2.5 oder höher, SGI IRIX 5.2 oder höher oder Linux 1.2.13 oder höher, mit 8 MB RAM und 8 MB freiem Plattenspeicher.

Die folgenden Beispiele und Abbildungen beziehen sich ausschließlich auf die vorliegende Windows-Version von PGP.

4.1 Administration

Unter Administration wird in diesem Kapitel zunächst die Einrichtung PGPs in einem Netzwerk verstanden. PGP for Business Security Version 5.5.3 bietet mit dem Administration Wizard ein Tool an, das die Installation

[74] Network Associates, Infoblatt zu PGP for Business Security 5.5.

PGPs auf den Rechnern eines Netzwerkes vorbereitet, indem für die Clients unternehmensindividuelle Setup-Dateien erstellt werden.

Die Einrichtung PGPs in einem Netzwerk durchläuft drei Schritte:

1. Installation und Generierung eines oder mehrerer Schlüsselpaare auf dem Rechner des Administrators.
2. Konfigurierung des Client-Setup durch den Administrator mittels Administration Wizard.
3. Installation auf den Clients, Generierung der Schlüsselpaare der Mitarbeiter.

Um die Übersichtlichkeit zu erhöhen, wird der erste Schritt in die Kapitel „Installation“ und „Schlüsselgenerierung“ unterteilt.

4.1.1 Installation

Die erste Installation erfolgt auf dem Rechner des Administrators. Die Installations-CD-ROM startet automatisch. Ein Klick auf den Menüpunkt INSTALL PGP 5.5 öffnet den Installationsassistenten. Sollte die CD-ROM nicht automatisch starten: Die Datei SETUP.EXE findet sich im Verzeichnis PGP55.

Der Installationsassistent führt den Administrator durch die Installation. Zunächst wird das Zielverzeichnis bestimmt, in das PGP kopiert werden soll. Darauf folgt der Bildschirm zur Auswahl der Systemkomponenten.

Als Defaultwerte sind alle Komponenten ausgewählt:

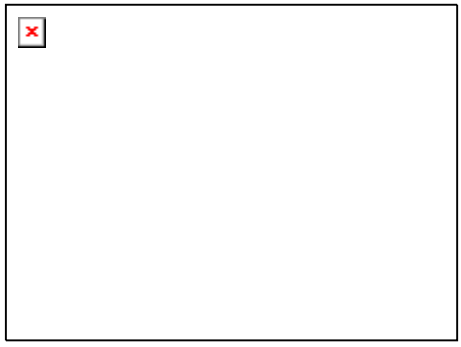


Abbildung 15: Auswahl der zu installierenden Komponenten

- **PGP 5.5 Program Files**
  Die PGP Programmdateien. Sie sind auf jeden Fall erforderlich.

- **PGP 5.5 Eudora Plugin und PGP 5.5 MS Exchange/Outlook Plugin**
  Plug-Ins integrieren bestimmte Funktionen PGPs in den Funktionsumfang der aufgeführten E-Mail-Programme. Wird keines der beiden aufgeführten E-Mail-Programme benutzt, kann die Auswahl der Plug-Ins deaktiviert werden. Die Funktionalität von PGP bleibt trotzdem im vollen Umfang nutzbar.

- **PGP 5.5 User's Manual**
  Das Bedienungshandbuch in englischer Sprache liegt im Adobe Acrobat-Format vor. Der Adobe Acrobat Reader kann gegebenenfalls von der CD installiert werden.

- **Unconfigured PGP 5.5 Client Install**
  Dateien zur Client-Installation von PGP im Netzwerk. Sie werden später durch den Administration Wizard konfiguriert. Der Administrator sollte diese Auswahl nicht deaktivieren, da ohne diese Dateien eine netzwerkweite Installation nicht möglich ist.

Im nächsten Installationsschritt werden die ausgewählten Dateien in das vom Administrator angegebene Verzeichnis kopiert. Anschließend fragt der Installationsassistent, ob bereits *Schlüsselbunde,* d.h. Dateien mit öffentlichen oder privaten Schlüsseln bestehen.

Bei einer Erstinstallation wird die Antwort in der Regel „Nein" lauten.

Die Frage sollte dagegen mit „Ja" beantwortet werden, wenn bereits öffentliche oder private Schlüssel vorhanden sind, z.B. weil vorher eine ältere Version von PGP genutzt wurde. In diesem Fall wird der Benutzer im nächsten Installationsschritt aufgefordert den Verzeichnispfad anzugeben, in dem sich der öffentliche und der private Schlüsselbund befinden. Mit dem Folgebildschirm ist der erste Teil der Installation abgeschlossen:

Abbildung 16: Frage nach bestehenden Schlüsselbunden

Mit der Auswahl des Punktes YES, I WANT TO RUN PGPKEYS gelangt der Benutzer in das Modul PGPkeys zur Schlüsselverwaltung. Der erstmalige Aufruf dieses Moduls startet automatisch die Schlüsselgenerierung. Dies gilt auch für den Fall, wenn PGPkeys erst später zum ersten Mal aufgerufen wird.

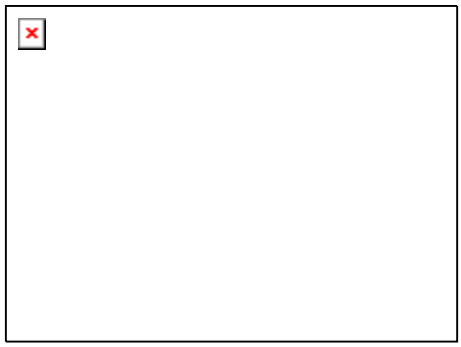


Abbildung 17: Abschluss des ersten Teils der Installation

Tipp - Download und Installation von PGP 5.5.3i für Privatanwender

Der Privatanwender kann PGP aus dem Internet u.a. von folgenden Seiten kostenlos beziehen:

- ftp://ftp.uni-mainz.de/pub/internet/security/pgp/pgpi
- ftp://ftp.cert.dfn.de/pub/tools/crypt/pgp/pgpi

Beide Server bieten mehrere PGP-Versionen, jeweils auch für verschiedene Betriebssysteme, zum Download an. Wir empfehlen die in diesem Buch beschriebenen Version 5.5 zu wählen. Von der Version 6.0 ist aufgrund eines Bugs abzuraten.[75]

Der Name der Datei für Windows 95 und Windows NT ist „pgp553i-win95nt.exe“ . Die Datei hat eine Größe von 2.229 KB. Nach dem Download kann durch einen Doppelklick mit der Installation des Programmes begonnen werden.

Installation und Handhabung unterscheiden sich kaum von der hier beschriebenen PGP Version 5.5.3 for Business Security. Wesentlicher Unterschied ist die fehlende Möglichkeit zur Client-Installation im Netzwerk. Demzufolge sind auch die Kapitel 4.1.3 und 4.1.4 für die Freeware-Version 5.5.3i nicht relevant. Bei der Schlüsselgenerierung kann der Anwender wie im Folgenden beschrieben vorgehen, jedoch braucht er die Angaben zum „Corporate Signing Key“ und „Additional Decryption Key“ (siehe Seiten 55 bis 56) nicht zu beachten.

4.1.2 Schlüsselgenerierung

Bevor PGP vollständig eingesetzt werden kann, muss ein Schlüsselpaar generiert werden, bestehend aus öffentlichem und privatem Schlüssel. Auch hier erleichtert ein Assistent die Arbeit.

Die Schlüsselgenerierung spielt eine zentrale Rolle für die Arbeit mit PGP, zur Orientierung wird im Folgenden jeder einzelne Schritt als Screenshot abgebildet und erläutert:

[75] Lt. mündlicher Auskunft von Michael Rudrich, NAI München, am 26.02.1999.

- **Angabe des Namens und der E-Mail-Adresse**
  Aus diesen Angaben setzt sich später die *Benutzer-ID (User-ID)* des Schlüsselpaares zusammen.
  Gegebenenfalls sind Formvorschriften zu beachten. Die Zertifizierungsstelle TC Trustcenter beispielsweise verlangt für Schlüssel, die zertifiziert werden sollen, einen Aufbau der Benutzer-ID nach folgendem Muster, dessen Eingabe im Screenshot zu sehen ist.[76]

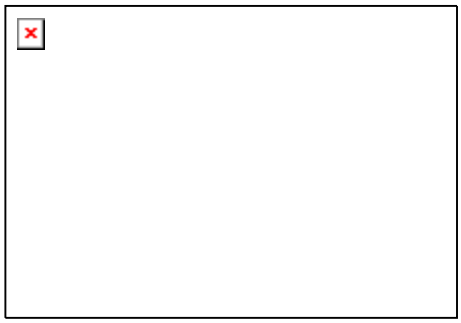


Abbildung 18: Schlüsselgenerierung: Bestimmung der User-ID

```
Firmenname lt. HR, Sitz des Unternehmens, Name Schlüsselinhaber <E-Mail>.
```

  Die Benutzer-ID des Beispiels wird später im Modul zur Schlüsselverwaltung in folgender Form angezeigt:

```
Musterfirma GmbH, Musterstadt, M. Mustermann <mm@musterfirma.de>.
```

  Das erste Schlüsselpaar ist das des Administrators. Später können weitere Schlüssel generiert werden, die spezielle Funktionen übernehmen, siehe auch die Beschreibung am Endes des Kapitels auf Seite 55.

- **Wahl zwischen den Schlüsseltypen DH/DSS und RSA**
  PGP empfiehlt die Generierung eines DH/DSS-Schlüssels.

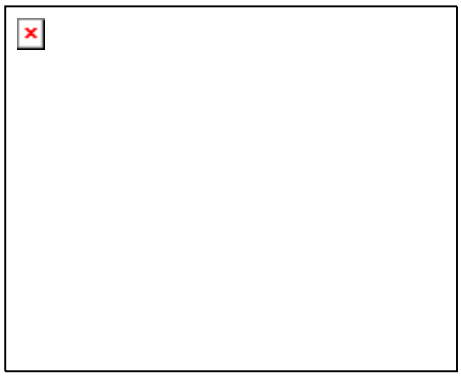


Abbildung 19: Schlüsselgenerierung: Auswahl des Schlüsseltyps

  RSA- und DH-Keys bieten ein in etwa gleich hohes Sicherheitsniveau. Die heute noch vielfach benutzte Vorgängerversion 2.6 arbeitet lediglich mit RSA-Schlüsseln, die Version PGP 6.0 Freeware verwendet jedoch nur DH/DSS-Schlüssel. Der Benutzer der älteren PGP-Version kann somit nicht mit dem öffentlichen DH-Schlüssel eines PGP 5.5–Anwenders verschlüsseln und für die Verschlüsselung mit der Version 6.0 ist ein RSA-Schlüssel nutzlos. Um Kompatibilitätsprobleme zu vermeiden, sollten daher Schlüssel beiden Typs generiert werden. Da pro Durchgang lediglich ein

[76] Vgl. TC Trustcenter, URL: http://www.trustcenter.de/html/zertifikate/654.htm

Schlüsselpaar generiert werden kann, ist im Anschluss an die erste Schlüsselgenerierung eine zweite notwendig.

- **Auswahl der Schlüssellänge**
  Es können RSA-Schlüssel bis zu einer Länge von 2048 Bit erzeugt werden. Bei einem Schlüsselpaar vom Typ DH beträgt die Schlüssellänge bis zu 4096 Bit, der für die Signatur verwendete DSS-Schlüssel ist allerdings auf eine Länge von 1024 Bit begrenzt. Schlüssellängen öffentlicher Schlüssel ab 1024 Bit gelten bereits als absolut sicher.[77]

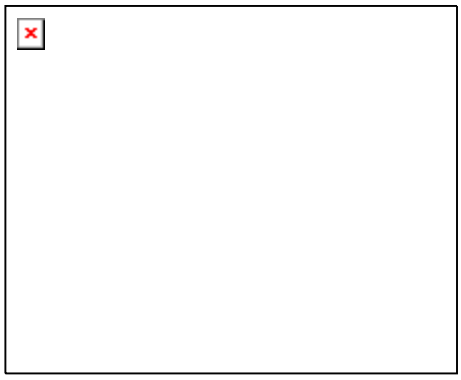


Abbildung 20: Schlüsselgenerierung: Bestimmung der Schlüssellänge

  PGP weist zwar darauf hin, dass längere Schlüssel eine langsamere Verschlüsselung zur Folge haben. Da jedoch lediglich die Chiffrierung des Sitzungsschlüssels und die Signatur mit öffentlichen Verschlüsselungsalgorithmen erfolgen, wird die Gesamtdauer des Verschlüsselungsvorgangs weniger von der Länge des öffentlichen Schlüssels als von der Größe der zu verschlüsselnden Datei beeinflusst. Doch selbst Dateien der Größe von 1000 KB werden von einem Pentium-PC in weniger als 10 Sekunden verschlüsselt, wenn der asymmetrische Schlüssel eine Länge von 2048 Bit besitzt.

- **Verfallsdatum des Schlüssels bestimmen**
  Die unbegrenzte Nutzung des Schlüsselpaares ist als Defaultwert gesetzt und sollte auch beibehalten werden. Bei der Eingabe einer zeitlich begrenzten Nutzungsmöglichkeit eines Schlüssels sollte bedacht werden, dass nach diesem Datum ein neues Schlüsselpaar generiert und verteilt werden muss. Der alte öffentliche Schlüssel kann dann von den Kommunikationspartnern nicht mehr zur Verschlüsselung genutzt werden. Mit dem abgelaufenen privaten Schlüssel lässt sich auch nicht mehr signieren.

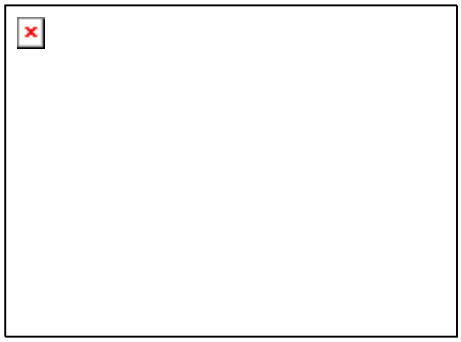


Abbildung 21: Schlüsselgenerierung: Bestimmung des Verfallsdatums

[77] Vgl. William Stallings, Datensicherheit mit PGP, 1995, S. 73.

- **Bestimmung der *Passphrase* („*Mantra*“)**
  Um Unbefugten den Zugriff auf den privaten Schlüssel zu verwehren, wird der private Schlüssel durch die Passphrase, auch Mantra genannt, geschützt.[78] Die Passphrase wird später vor jedem Gebrauch des privaten Schlüssels abgefragt, d.h. vor jeder Signatur und vor jeder Dechiffrierung. Man spricht von einer Passphrase und nicht von einem Passwort, weil die Eingabe beliebig lang sein kann. Dieser Schutz ist insbesondere dann wichtig, wenn der private Schlüssel auf der Festplatte eines Rechners abgespeichert ist, an dem mehrere Personen arbeiten oder auf den sie durch ein Netzwerk Zugriff haben (zum Speicherort der Schlüssel: siehe Kapitel 4.2.6 und 5.1.1). **Die Sicherheit verschlüsselter Daten hängt in diesem Fall unmittelbar von der Qualität des Mantras ab**, d.h. die Passphrase darf für Dritte nicht zu erraten oder auf systematische Weise zu ermitteln sein. Die Qualität des Mantras wird bei der Schlüsselgenerierung durch einen Balken angedeutet, der mit höherer Qualität des Mantras länger wird. In erster Linie wird die Güte des Mantras von der Anzahl der Zeichen bestimmt, auch der wechselnde Gebrauch von Sonderzeichen, Groß- und Kleinbuchstaben machen es sicherer. Gleichzeitig sollte es für den Schlüsseleigentümer leicht zu merken sein, denn: Vergisst er das Mantra, so kann er auch den eigenen privaten Schlüssel nicht mehr nutzen.

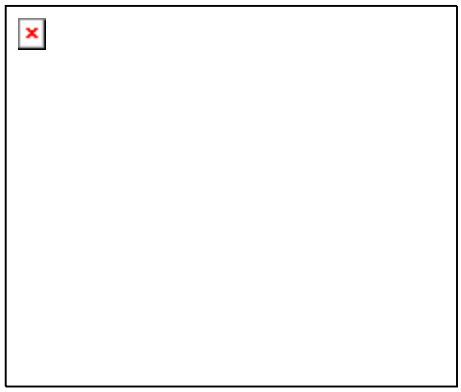
  

  Abbildung 22: Schlüsselgenerierung: Bestimmung des Mantras

  Solange die Option Hide Typing aktiviert ist, wird das Mantra nicht auf den Bildschirm ausgegeben.

  Sollte zu diesem Zeitpunkt noch keine geeignete Passphrase gefunden werden, so kann der Anwender sie an jedem späteren Zeitpunkt wieder ändern, siehe Kapitel 4.2.2 (KEY PROPERTIES). Hilfestellung zur Auswahl des Mantras bietet Kapitel 5.2.

[78] Der private Schlüssel wird strenggenommen nur indirekt durch das Mantra geschützt: Aus dem Mantra wird mittels einer Hashfunktion ein 128 Bit langer Code berechnet. Dieser dient als Schlüssel zur Chiffrierung bzw. Dechiffrierung des privaten Schlüssel mittels eines symmetrischen Chiffrieralgorithmus. Vgl. Simson Garfinkel, PGP: Pretty Good Privacy, 1996, S. 170.

- **Erzeugung von Zufallsdaten**
  PGP sammelt in diesem Schritt Zufallsdaten anhand von Mausbewegungen. Alternativ dazu können auch Tastatureingaben erfolgen. Sowohl die zeitlichen Abstände als auch die tatsächlich gedrückten Tasten werden zur Erzeugung der Zufallsdaten verwendet. Der Fortschritt des Vorgangs wird durch einen Balken angezeigt. Die Zufallsdaten werden zunächst dazu gebraucht, eine zufällige Ausgangsbasis zur Findung der Primzahlen zu erhalten.[79]

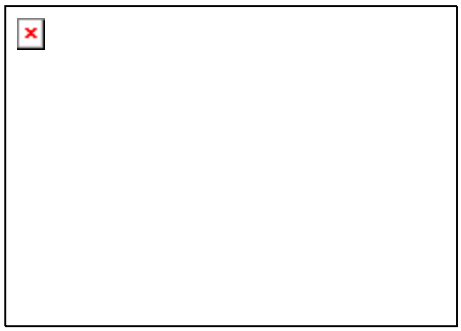


Abbildung 23: Schlüsselgenerierung: Erzeugung von Zufallsdaten

  Darüber hinaus bilden die an dieser Stelle gesammelten Zufallsdaten später die Grundlage zur Erzeugung zufälliger Sitzungsschlüssel. Zu diesem Zweck werden sie in der Datei RANDSEED.BIN gespeichert und nach jedem Aufruf anhand zufälliger Systemdaten verändert.[80] Diese Datei sollte Dritten nicht zugänglich sein, weil aus den Zufallsdaten möglicherweise Rückschlüsse auf generierte Schlüssel möglich sind. Zum Speicherort der Datei siehe Kapitel 4.2.6 und 5.1.1.

- **Ermittlung der Primzahlen**
  DH-Schlüssel benötigen nur eine Primzahl, auch wenn dessen Suche fälschlicherweise mit „generating second prime number“ angezeigt wird, wie in der Abb. zu sehen ist. Bei der Generierung von RSA-Keys werden zwei Primzahlen gesucht.

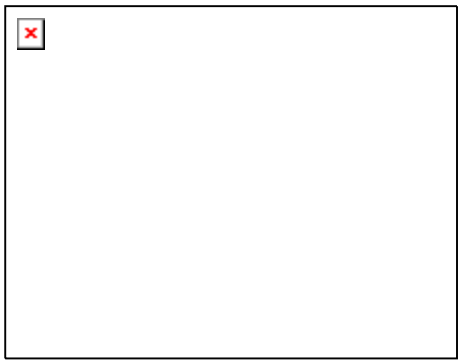


Abbildung 24: Schlüsselgenerierung: Ermittlung der Primzahlen

  Die Primfaktoren eines z.B. 1024 Bit langen RSA-Schlüssels sind jeweils 512 Bit lang. Mit Hilfe der vorher erzeugten Zufallsdaten werden zufällige Zahlen dieser Länge auf ihre Eigenschaft als Primzahl untersucht.[81]

  Dieser Vorgang ist i.d.R. auch bei 2048 Bit-Schlüsseln auf einem Penti-

---

79 Vgl. William Stallings, Datensicherheit mit PGP, 1995, S. 76.

80 Eine genauere Erläuterung zur Bedeutung der gewonnen Zufallsdaten siehe: PGP for Business Security, Windows User's Guide Version 5.5 v, 1997, S. 103.

81 Vgl. Reinhard Wobst, Abenteuer Kryptologie, 1998, S. 164.

um-PC innerhalb einer Minute durchgeführt.

Die Gefahr, dass bei der Schlüsselgenerierung zweier Personen die gleichen Primzahlen benutzt werden, ist außerordentlich gering. Von den Zahlen der Länge 512 Bit, das sind die Zahlen zwischen 2^{512} und 2^{513}, sind lt. einer Rechnung des Mathematikers Reinhard Wobst[82] etwa $7{,}5*10^{151}$ Primzahlen.

- **Möglichkeit, den generierten Schlüssel zu einem Key Server zu senden**
  Wenn eine Verbindung des Rechners zum Internet besteht, kann an diesem Punkt der soeben generierte eigene öffentliche Schlüssel zu einem voreingestellten *Key Server* geschickt werden. Der standardmäßig voreingestellte Key Server hat die Adresse http://wwwkeys.pgp.net, von dort wird der Schlüssel an alle Key Server des „pgp.net“ und einige weitere Servern weitergegeben.

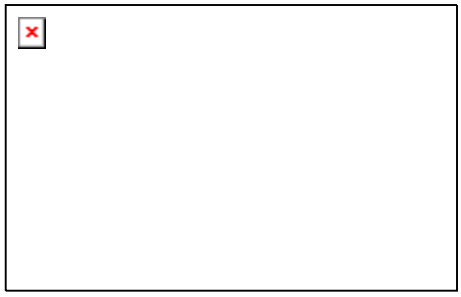


Abbildung 25: Schlüsselgenerierung: Schlüssel zum Key Server senden

Zur Bestimmung der Key Server siehe Kapitel 4.2.6 (Register SERVERS). Ist der Versand des Schlüssels zum jetzigen Zeitpunkt nicht möglich, kann er auch später nachgeholt werden, siehe Kapitel 4.2.2.

- **Abschluss der Schlüsselgenerierung**
  Mit diesem Bild ist die Generierung eines Schlüsselpaares abgeschlossen.

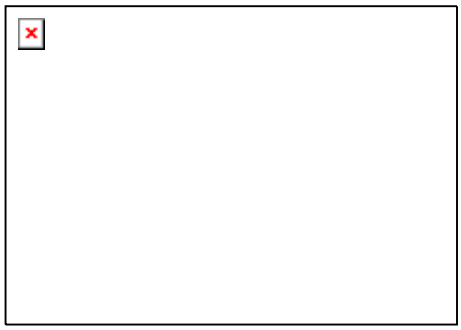


Abbildung 26: Schlüsselgenerierung: Abschluss

Im Anschluss an die Schlüsselgenerierung öffnet sich das Modul PGPkeys, das der Schlüsselverwaltung dient. Es beinhaltet nun das generierte Schlüsselpaar. Darüber hinaus enthält der Schlüsselbund zwei weitere, bereits während der Installation PGPs hinzugefügte öffentliche Schlüssel

---

[82] Vgl. Reinhard Wobst, Abenteuer Kryptologie, 1998, S. 166.

der Herstellerfirma. Eine Erläuterung der Schlüsselverwaltung erfolgt im Kapitel 4.2.2.

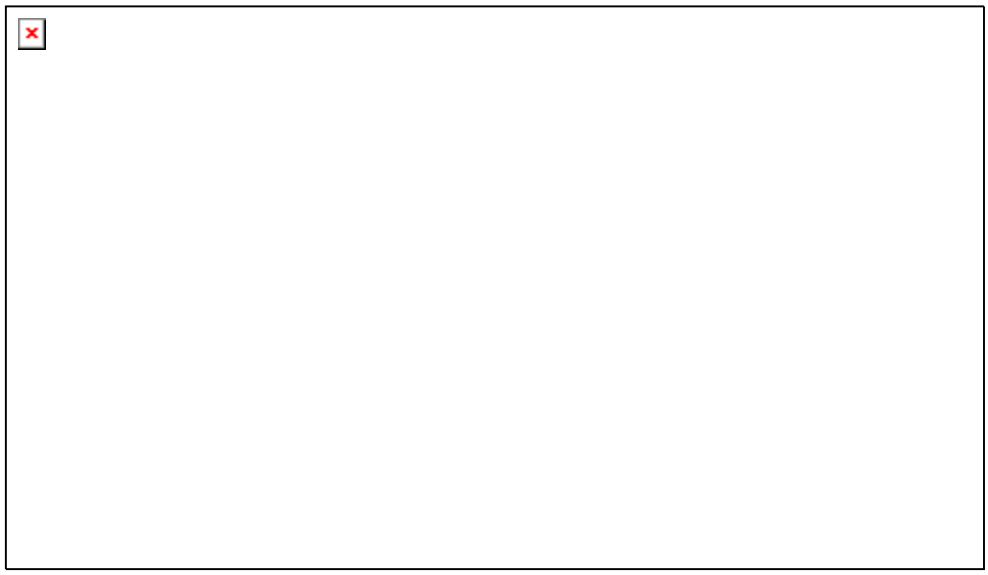


Abbildung 27: Das Modul zur Schlüsselverwaltung: PGPkeys

An dieser Stelle sollten die Schlüsselgenerierung wiederholt und zwei weitere Schlüssel generiert werden:

1. **Der *Corporate Signing Key (CSK)***
2. **Der *Additional Decryption Key (ADK)***

- **Corporate Signing Key (CSK)**

  Unter dem Corporate Signing Key versteht man ein Schlüsselpaar, das automatisch von allen Client-Schlüsseln durch ihre Signatur als gültig und voll vertrauenswürdig anerkannt wird. Dies hat in dem Web of Trust-Modell von PGP die Folge, dass jeder Schlüssel, der später vom privaten Schlüssel des CSK signiert wird, unternehmensweite Gültigkeit erhält. Folglich ist dieses Schlüsselpaar nicht zur Ver- und Entschlüsselung, sondern nur zur Signierung gedacht.[83]

[83] Da der Schlüssel des Administrators in dieser Beschreibung bereits vor dem CSK erzeugt wurde, ist seine Signatur des CSK mit seinem Schlüssel manuell nachzuholen.

- **Additional Decryption Key (ADK)**

  Die wörtliche Übersetzung „zusätzlicher Dechiffrierungsschlüssel“ macht die Aufgabe dieses Schlüssel bereits deutlich. Mit der Generierung eines ADK besitzt der Administrator einen Schlüssel, mit dem

  1. die **für Mitarbeiter bestimmte** chiffrierte Mail entschlüsselt werden kann und
  2. die **von Mitarbeitern verschickte** chiffrierte Mail entschlüsselt werden kann.

  Es besteht auch die Möglichkeit, die Funktionen auf zwei verschiedene ADKs zu verteilen. Im ersten Fall spricht man dann vom *Incoming Additional Decryption Key (IADK)*, im zweiten Fall vom *Outgoing Additional Decryption Key (OADK)*.

  Der Zweck eines ADKs sollte nicht die Kontrolle des Schriftverkehrs der Mitarbeiter sein. Ein solcher Schlüssel ist dafür gedacht, trotz bestimmter Umstände noch die Möglichkeit zu haben, verschlüsselte Nachrichten zu öffnen. Dies kann z.B. der Fall sein, wenn ein Mitarbeiter für längere Zeit abwesend ist und die für ihn eingehenden verschlüsselten Nachrichten bearbeitet werden müssen. Ein anderer Name für den ADK ist auch *Message Recovery Key (MRK)*.[84]

  Aufgrund der Tatsache, dass unter Nutzung des ADKs sämtliche verschlüsselte Nachrichten des Unternehmens dechiffriert werden können, ist der ADK in besonderer Weise vor unbefugtem Zugriff zu schützen. Der ADK muss daher durch eine besonders starke Passphrase geschützt sein. Empfehlenswert ist zudem, den ADK nicht auf der Festplatte zu speichern, sondern den ADK auf einer Diskette an einem vor Diebstahl sicheren Ort zu verwahren.

  Hinweis: Lediglich ein DH/DSS-Schlüssel kann als ein Incoming ADK genutzt werden, während Outgoing ADKs sowohl RSA- als auch DH/DSS-Schlüssel sein können.

Die Benutzer-ID dieser beiden Schlüssel kann folgendermaßen aufgebaut sein:[85]

`Firmenname lt. HR, Sitz des Unternehmens, Schlüsselzweck <E-Mail Administrator>.`

---

[84] Vgl. PGP Security Officer’s Guide Version 5.5, 1997, S. 63.

[85] Um die Übersichtlichkeit zu erhöhen, wurde bei den Schlüsseln in den folgenden Screenshots auf dieses Format verzichtet.

Wenn das Modul zur Schlüsselverwaltung nach der Schlüsselgenerierung vom Anwender erstmals geschlossen wird, erscheint die Aufforderung, ein Backup der Schlüssel zu machen. Diese Aufforderung erfolgt zudem bei jeder Generierung eines neuen Schlüsselpaares und nach der Aufnahme von weiteren öffentlichen Schlüsseln in den Schlüsselbund.

Dieser Rat sollte unbedingt befolgt werden, um einem Verlust der Schlüssel, z.B. durch Festplattencrash, vorzubeugen. Empfehlenswert ist die Speicherung auf einer Diskette, die später an einem sicheren Ort verwahrt werden sollte. Öffentliche und private Schlüssel werden von dem Programm automatisch getrennt in den Dateien PUBRING.PKR bzw. SECRING.SKR gespeichert.

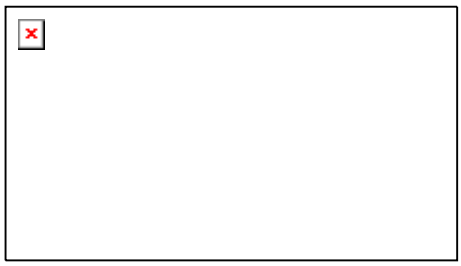


Abbildung 28: Aufforderung zum Backup der Schlüssel

4.1.3 Konfigurierung des Client-Setup

Nachdem PGP auf dem Rechner des Administrators installiert wurde, kann unter Windows über die START-Leiste … PROGRAMME … PRETTY GOOD PRIVACY … PGPADMIN der Administration Wizard aufgerufen werden.

Der Administration Wizard dient der Erzeugung der unternehmensindividuellen Setup-Dateien zu Installation PGPs auf den Clients.

Nach der Eingabe der Lizenznummer und einem Einführungsbildschirm wird dem Administrator eine Information über die Bedeutung des Additional Decryption Key angezeigt. Die darauf folgenden Konfigurierungsschritte werden nachfolgend beschrieben, die Screenshots dienen der Orientierung.

- **Festlegung, ob es einen Incoming ADK geben soll**
  Wenn in der Organisation mit einem IADK gearbeitet werden soll, so ist dies hier anzugeben.

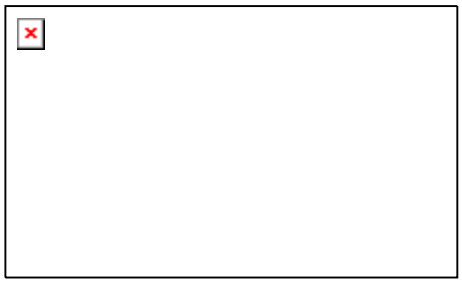


Abbildung 29: Client-Setup-Konfig.: Festlegung, ob es einen ADK geben soll

- **Bestimmung des IADK**
  Wenn im letzten Schritt festgelegt wurde, dass ein IADK benutzt werden soll, so kann hier ein beliebiger DH/DSS-Schlüssel zum IADK bestimmt werden. Dieser Incoming Additional Key wird später den öffentlichen DH/DSS-Schlüsseln der Clients hinzugefügt. Der IADK kann nicht im Zusammenhang mit RSA-Schlüsseln der Clients genutzt werden.

Abbildung 30: Client-Setup-Konfig.: Bestimmung des ADK

- **Festlegung ob es einen Outgoing ADK geben soll**
  In diesem Schritt ist festzulegen, ob in der Organisation ein OADK benutzt werden soll.

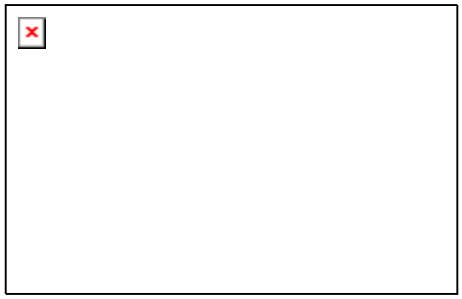


Abbildung 31: Client-Setup-Konfig.: Festlegung, ob es einen OADK geben soll

- **Bestimmung des OADK**
  Der OADK kann sowohl ein DH/DSS-Schlüssel als auch ein RSA-Schlüssel sein. Im Beispiel sind Incoming ADK und Outgoing ADK derselbe Schlüssel.

Abbildung 32: Client-Setup-Konfig.: Bestimmung des OADK

- **Festlegung, ob IADK und OADK generell benutzt werden müssen**
  Ein ADK wird automatisch bei jeder Verschlüsselung genutzt. Der Client kann im Einzelfall die Chiffrierung mit dem ADK abstellen.

  Mit den drei Auswahlmöglichkeiten kann der Administrator die Nutzung des ADK jedoch erzwingen:

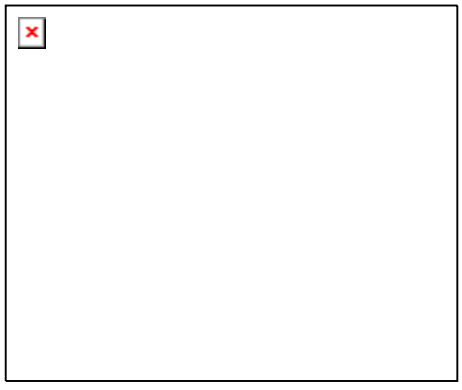


Abbildung 33: Client-Setup-Konfig.: Generelle Nutzung des ADK

1. Die Nutzung des IADK innerhalb der Organisation (ENFORCE INCOMING ADDITONAL DECRYPTION KEY).
2. Die Nutzung des OADK (ENFORCE OUTGOING ADDITONAL DECRYPTION KEY).
3. Die Nutzung der IADKs anderer Organisationen. (ENFORCE REMOTE ADDITONAL DECRYPTION KEY STRICTNESS).
   Punkt 3 gilt nur dann, wenn chiffrierte E-Mails an Mitarbeiter von Organisationen geschickt werden, die die Nutzung des IADK innerhalb der eigenen Organisation vorgeschrieben haben. D.h. sie müssen ihrerseits ein Kreuz bei der ersten Auswahl gemacht haben.

Punkt 3 bedeutet im Umkehrschluss, dass nur dann der eigene IADK von anderen Unternehmen immer zur Verschlüsselung genutzt wird, wenn im eigenen Unternehmen die erste Auswahl getroffen wurde und im anderen Unternehmen Punkt 3 angekreuzt ist.

Grundsätzlich sollte es den Mitarbeitern überlassen werden, ob sie den ADK benutzen oder nicht. Eine erzwungene Nutzung des ADK könnte den Eindruck der Kontrolle erwecken.

- **Bestimmung der Qualität des Mantras der Mitarbeiter**
  Mit der ersten Auswahl kann die Mindestlänge des Mantras der Clients bestimmt werden. Die zweite Auswahl bestimmt das Minimum der Qualität. Unterschreiten die Mantras der Clients später diese Vorgaben, werden sie abgelehnt und PGP fordert zur Eingabe eines neuen Mantras auf. Die Abbildung 34 zeigt, welche Mindestwerte von PGP vorgeschlagen werden. Diese sollten auch nicht unterschritten werden.

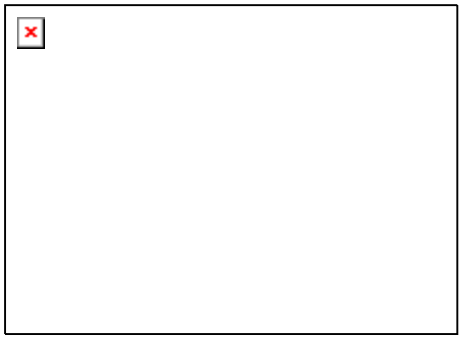


Abbildung 34: Client-Setup-Konfig.: Mantra-Qualität

- **Bestimmung, ob ein Corporate Signing Key (CSK) benutzt werden soll**
  Mit der obersten Auswahl wird bestimmt, ob automatisch jeder Client Key nach seiner Generierung den Corporate Key signieren soll. Diese Auswahl sollte getroffen werden, sie ist später für den Aufbau einer unter nehmensinternen Public Key Infrastruktur notwendig, siehe Kapitel 5.1.3.

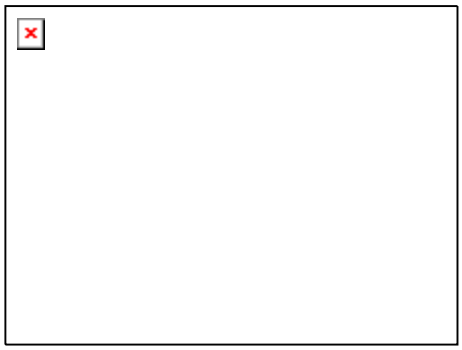


Abbildung 35: Client-Setup-Konfig.: Bestimmung, ob CSK benutzt werden soll

  Wenn diese Auswahl getroffen wird, kann der Corporate Key darüber hinaus als Meta-Introducer fungieren. D.h. alle vom Corporate Key unterzeichneten und mit dem Zusatz Trusted Introducer signierten Schlüssel erhalten für die Client Keys nicht nur Gültigkeit, sondern gleichzeitig auch Vertrauen.

  Die dritte Auswahlmöglichkeit bietet an, vor der Verschlüsselung mit einem öffentlichen Schlüssel, der nicht vom Corporate Key unterzeichnet wurde, eine Warnung auszugeben.

- **Bestimmung des CSK**
  Der CSK kann sowohl ein DH/DSS-Schlüssel als auch ein RSA-Schlüssel sein.

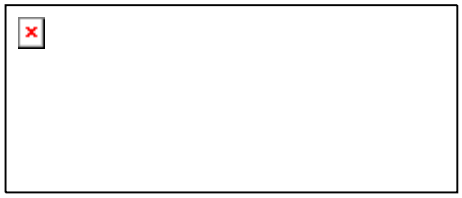


Abbildung 36: Client-Setup-Konfig.: Bestimmung des CSK

- **Optionen zur Schlüsselgenerierung der Clients festlegen**
  An dieser Stelle kann zunächst festgelegt werden, ob die Mitarbeiter ihre eigenen Schlüssel generieren können oder ob dies durch den Administrator zentral erledigt werden soll. Der Assistent gibt zu Bedenken, dass eine zentrale Schlüsselgenerierung in einer größeren Organisation mitunter sehr arbeits- und zeitaufwendig ist. Darüber hinaus muss der Administrator im Falle der zentralen Schlüsselgenerierung einen Weg finden, wie die privaten Schlüssel der Clients verteilt werden. Um diese Probleme zu vermeiden, sollte der Administrator die Schlüsselgenerierung durch die

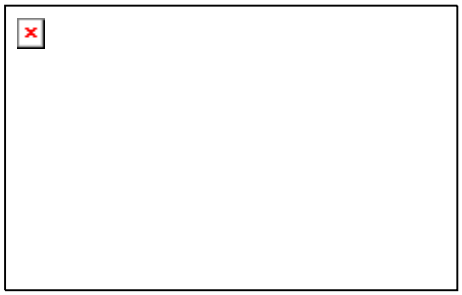


Abbildung 37: Client-Setup-Konfig.: Optionen zur Schlüsselgenerierung

Clients erlauben.

Wenn die Schlüsselgenerierung der Clients freigegeben wird, kann die Generierung von RSA-Schlüsseln unterbunden werden. Einziger Grund zur Unterbindung ist die Tatsache, dass der Incoming ADK nicht im Zusammenhang mit RSA-Schlüsseln genutzt werden kann. Um allerdings die angesprochenen Kompatibilitätsprobleme bzgl. der ausschließlichen Nutzung von DH-Schlüsseln zu umgehen, sollte die Generierung von RSA-Schlüsseln erlaubt werden, indem die entsprechende Option aktiviert wird.

Bei der Bestimmung der minimalen Schlüssellänge sollte auch der Wert für die Clients mindestens 1024 Bit betragen.

- **Schlüsselbund der Clients festlegen**
  Hier können die Schlüssel ausgewählt werden, die später in den anfänglichen Schlüsselbunden der Clients erscheinen. Wenn ADK und CSK genutzt werden sollen, so müssen sie hier ausgewählt werden.

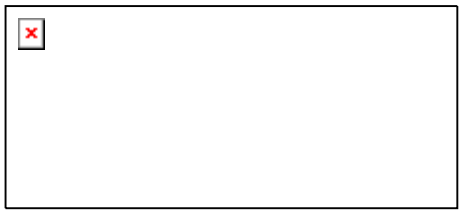


Abbildung 38: Client-Setup-Konfig.: Default-Schlüsselbund festlegen

- **Festlegung, ob konventionelle Chiffrierung erlaubt ist**
  Neben der öffentlichen Verschlüsselungsmethode kann PGP auch auf konventionelle, symmetrische Weise Daten verschlüsseln. Mit der Auswahl wird die konventionelle Verschlüsselung erlaubt, andernfalls wird diese Möglichkeit bei den Clients ausgeschaltet. Des weiteren besteht hier die Möglichkeit, einen Nachrichtenkopf zu bestimmen, der jeder Nachricht hinzugefügt wird.

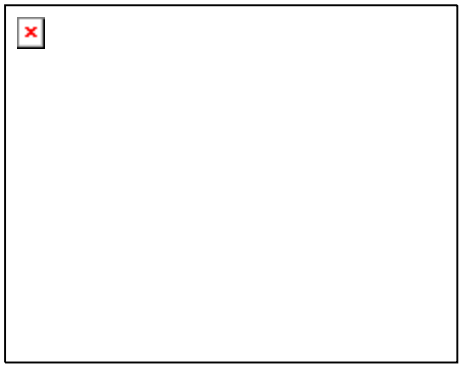


Abbildung 39: Client-Setup-Konfig.: Konventionelle Verschlüsselung erlauben

- **Zusammenfassung**
  Zum Abschluss werden die eingegebenen Daten noch einmal in einer Übersicht angezeigt. Durch Zurückblättern können alle Angaben noch korrigiert werden.

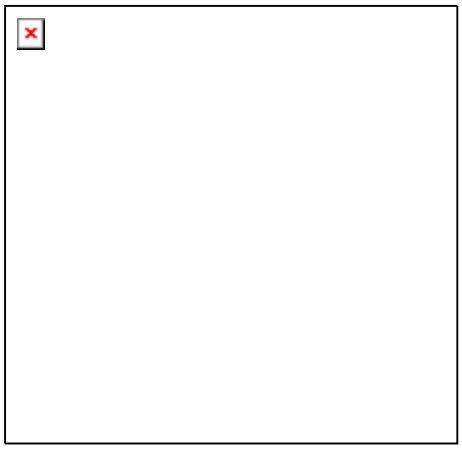


Abbildung 40: Client-Setup-Konfig.: Zusammenfassung

- **Optionen des Administrators übernehmen**
  Die Optionen-Einstellungen des Administrators (PGP PREFERENCES) dienen mit dieser Auswahl als Ausgangswerte für die Einstellungen der Clients. Die Benutzer an den Client-Rechnern können diese Einstellungen später jederzeit nach ihren Wünschen ändern, siehe Kap. 4.2.6.

Abbildung 41: Client-Setup-Konfig.: Optionen übernehmen

- **Verzeichnispfad des Client-Setup festlegen**
  Der Administrator bestimmt das Verzeichnis, in das die Client-Setup-Dateien kopiert werden sollen. PGP richtet dort ein Unterverzeichnis mit dem Namen PGP5.5.3CLIENT INSTALL ein.

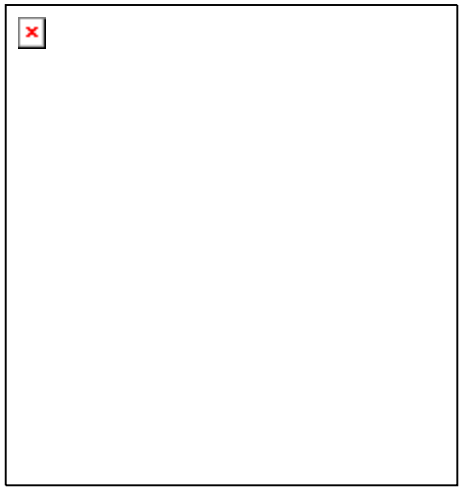


Abbildung 42: Client-Setup-Konfig.: Verzeichnispfad festlegen

- **Abschluss der Konfigurierung**

Abbildung 43: Client-Setup-Konfig.: Abschluss

4.1.4 Installation auf den Clients

Mit dem Abschluss der Konfiguration des Client-Setups wurde von PGP in dem vom Administrator bestimmten Verzeichnis das Unterverzeichnis PGP5.5.3CLIENTINSTALL angelegt. Hier findet der Anwender ein weiteres Unterverzeichnis mit dem Namen DISK1, in dem sich alle notwendigen Dateien zum Setup auf den Clients befinden. Die Installation auf den Clients erfolgt aus diesem Verzeichnis heraus durch Starten der Datei SETUP.EXE.

Der Installationsvorgang entspricht der in Kapitel 4.1 beschriebenen Installation und erfolgt nach den Vorgaben, die der Administrator mit der Konfigurierung des Client-Setup gesetzt hat.

Insofern die Schlüsselgenerierung auf den Clients nicht durch den Administrator eingeschränkt wurde, hat PGP auf den Client-Rechnern grundsätzlich den gleichen Funktionsumfang wie auf dem Rechner des Administrators. Lediglich das Modul PGPadmin kann durch das Client-Setup nicht installiert werden.

4.2 Handhabung

Nach der Installation findet der Anwender im Startmenü über START ... PROGRAMME ... PRETTY GOOD PRIVACY ... 3 Einträge vor:[86]

- PGPkeys
  Dieser Eintrag startet das bereits angesprochene Modul zur Schlüsselverwaltung.

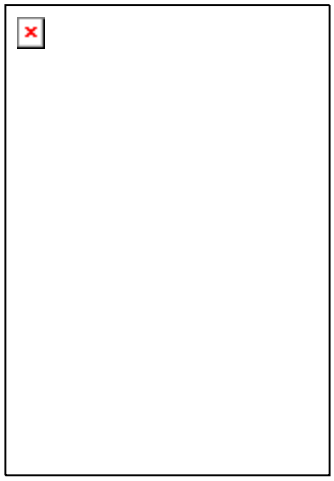
[86] Evtl. kann der Verzeichnisweg auch START ... **PROGRAMS** ... PRETTY GOOD PRIVACY lauten.

- PGPtray
  Der Start dieses Moduls legt PGP als Icon in der Taskleiste ab:

  Abbildung 44: Icon PGPtray

  Von dort kann mit einem Mausklick der volle Funktionsumfang PGPs aufgerufen werden:

  - Chiffrierung des Zwischenspeichers
  - Signierung des Zw.sp.
  - Chiffrierung und Signierung des Zw.sp
  - Dechiffrierung und Verifizierung des Zw.sp.
  - Hinzufügen eines Schlüssels
  - Editieren des Zwischenspeichers
  - Löschen des Zwischenspeichers
  - PGPtools starten
  - PGPkeys starten
  - PGP Optionen
  - Hilfefunktionen aufrufen
  - PGPtray beenden

  Abbildung 45: PGPtray

  Die Verschlüsselungsfunktionen finden bei der Nutzung des PGPtray ihre Anwendung auf den Inhalt des Zwischenspeichers. Dies ist insbesondere dann nützlich, wenn zu der verwendeten E-Mail-Software kein Plug-In verfügbar ist.

  Wenn ein Plug-In installiert wurde, können die E-Mails direkt im E-Mail-Programm durch Anklicken eines Icons chiffriert und signiert bzw. dechiffriert und verifiziert werden.

- PGPtools
  Die Verschlüsselungsfunktionen können auch auf ganze Dateien angewendet werden. Diese Funktionalitäten sind über die PGPtools ausführbar.

Ein Klick auf die gewünschte Funktion öffnet ein Fenster zur Dateiauswahl. Neben den bekannten Funktionen ist es zudem möglich, mit WIPE eine Datei unwiderruflich zu löschen. Darüber hinaus kann über einen Klick auf das PGPkeys-Icon die Schlüsselverwaltung aufgerufen werden.

Abbildung 46: PGPtools

Die Verschlüsselungsfunktionen können auch aus dem Windows Explorer heraus durch Markieren der gewünschten Datei und Klick auf die rechte Maustaste ausgeführt werden.

4.2.1 Schlüsselgenerierung

Auch nach der Installation ist es jederzeit möglich, weitere Schlüsselpaare zu generieren. Die Schlüsselgenerierung erfolgt im Modul PGPkeys:

- Aufruf des Punktes KEYS in der Menüzeile
- Klicken auf NEW KEY... startet den Assistenten zur Schlüsselgenerierung

Die dann folgenden Schritte entsprechen den in Kapitel 0 erläuterten Schritten.

4.2.2 Schlüsselverwaltung mit dem Modul PGPkeys

In Abbildung 27 wurde das Modul PGPkeys zur Schlüsselverwaltung bereits dargestellt. Hier befinden sich die aufgenommenen öffentlichen Schlüssel der Kommunikationspartner und der eigene private Schlüssel. Mit PGPkeys werden Schlüssel erzeugt, exportiert, signiert, ausgeschaltet und importiert.

In der Infospalte werden DH-Schlüssel mit einem goldgelben Schlüsselsymbol dargestellt, Schlüssel des Typs RSA sind blau gezeichnet. Ein doppeltes Schlüsselsymbol stellt ein eigenes Schlüsselpaar dar. Wie in Abbildung 27 zu sehen, kann durch Klick auf das Symbol Φ vor dem Schlüssel die User-ID des Schlüssels angezeigt werden, die jedem Schlüssel zugeordnet ist und sich i.d.R. aus dem Namen des Schlüsselinhabers und seiner E-Mail-Adresse zusammensetzt. Die User-ID kann ebenfalls erweitert werden, darunter sind die Signatur des Schlüsselinhabers und gegebenenfalls weitere Signaturen zu finden.

Mit Auswahl des Menüpunktes KEYS ... SELECT COLUMNS ... kann die Anzeige weiterer Infospalten ermöglicht bzw. ausgeschaltet werden. Folgende Infospalten geben dem Anwender Auskunft über den Schlüssel:

- Validity: Zeigt die Gültigkeit eines Schlüssels an. Ein grüner Punkt bedeutet Gültigkeit, ein grauer Punkt keine Gültigkeit. Der eigene Schlüssel ist automatisch gültig, dies wird durch eine grüne Raute angezeigt.
- Seize: Länge des Schlüssels in Bit.
- Description: Informationen über den Schlüssel.
- Trust: Das Vertrauen wird in den drei Abstufungen „volles", „marginales" und „kein Vertrauen" durch gefüllte, halbgefüllte und leere Balken angezeigt.
- ADK: Beinhaltet ein Schlüssel einen ADK, so wird dies durch einen roten Punkt angezeigt.
- Creation: Erstellungsdatum.
- Expiration: Verfallsdatum.
- Key ID: Identifikationsnummer des Schlüssels, bestehend aus acht hexadezimalen Ziffern und einem vorangestellten `0x`.[87]

  Beispiel: **`0xBD85B7C3`**

  Jede verschlüsselte bzw. signierte Nachricht oder Datei ist mit der Key ID des Schlüssels versehen, mit dem verschlüsselt/signiert wurde. Anhand dieser Key ID sucht PGP den entsprechenden privaten Schlüssel zur Entschlüsselung.[88]

  Eine weitere Aufgabe besteht z.B. darin, einen bestimmten Schlüssel auf einem Key Server schneller aufzufinden.

---

[87] Vgl. Feisthammel, Patrick, Website http://www.rubin.ch/pgp/glossar.de.html. Stand 14.12.1998.

[88] Vgl. Stallings, William, Datensicherheit mit PGP, 1995, S. 141.

Die Funktionen der Menüzeile werden in folgender Übersicht zusammengefasst. Die meisten Funktionen beziehen sich entsprechend auf den oder die markierten Schlüssel:

FILE

EXIT .....PGPkeys verlassen.

EDIT

COPY .....Schlüssel kopieren.

PASTE .....Schlüssel einfügen.

DELETE .....Schlüssel löschen.

SELECT ALL.....Alle Schlüssel auswählen.

COLLAPSE ALL .....Schlüsselansicht einschränken, d.h. alle User-IDs und Signaturen ausblenden.

EXPAND ALL.....Ansicht aller Schlüssel auf User-ID und Signaturen ausweiten.

PREFERENCES .....Optionen (Siehe Kapitel **4.2.6**)

KEYS

SIGN .....Signieren des ausgewählten Schlüssels. PGP öffnet daraufhin folgendes Fenster:

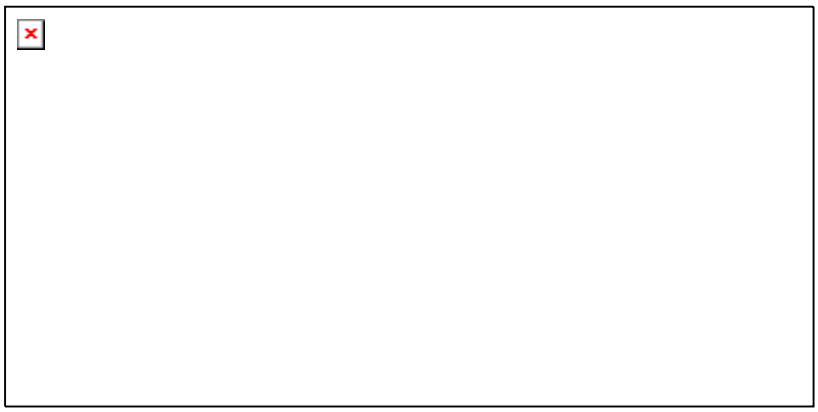


Abbildung 47: Signieren eines Schlüssels

Mit der Aktivierung der Option ALLOW SIGNATURE TO BE EXPORTED wird die Signatur im Fall der Weiterga-

be des Schlüssels zusammen mit dem Schlüssel exportiert, andernfalls gilt die Signatur nur im eigenen Schlüsselbund. Ein Klick auf die Schaltfläche MORE CHOICES erweitert die Signaturfunktion, indem der ausgewählte Schlüssel zum Trusted Introducer bzw. Meta-Introducer deklariert werden kann (siehe Kapitel 3.4).

SET AS DEFAULT KEY..Besitzt der Anwender mehrere eigene Schlüssel, so wird durch diese Auswahl der markierte Schlüssel als Standardschlüssel deklariert. Der Schlüssel erscheint daraufhin fett gedruckt und wird somit standardmäßig zur Signatur genutzt.

Dieser Schlüssel kann optional auch dafür benutzt werden, Nachrichten zusätzlich zum Empfängerschlüssel auch mit diesem Schlüssel zu chiffrieren, siehe Kapitel 4.2.6, Register GENERAL.

ADD NAME .....Ein **eigener** Schlüssel kann durch diese Funktion mit mehreren User-IDs versehen werden. Dies ist z.B. dann sinnvoll, wenn sich mehrere Personen einen Schlüssel teilen.

UPDATE FROM SERVERVon dem voreingestellten Key Server können die im eigenen Schlüsselbund befindlichen öffentlichen Schlüssel aktualisiert werden, z.B. um neue Signaturen oder eine Änderung der User-ID hinzuzufügen. Zur Auswahl der Key Server siehe 4.2.6, Register SERVERS.

SEND KEY TO SERVER.Der ausgewählte Schlüssel wird zu einem ausgewählten Key Server geschickt.

SEARCH.....Im eigenen Schlüsselbund oder auf einem frei wählbaren Key Server kann mittels bestimmter Auswahlkriterien nach einem Schlüssel gesucht werden.

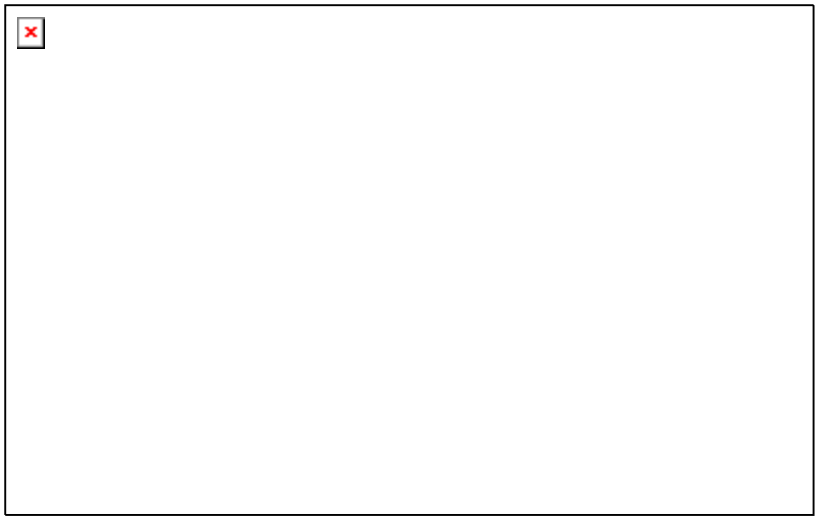


Abbildung 48: Suchen eines Schlüssels auf einem Key Server

Die Abbildung 48 zeigt beispielhaft das Suchergebnis aller Schlüssel auf dem Key Server www.trustcenter.de, deren User-ID den Namen „bank“ beinhaltet.

Der gesuchte Schlüssel kann daraufhin markiert und nach einem Klick auf die rechte Maustaste über die Funktion IMPORT TO LOCAL KEYRING in den Schlüsselbund des Anwenders aufgenommen werden.

NEW KEY .....Startet die Schlüsselgenerierung. Siehe Kapitel 4.1.2.

ENABLE .....Einen deaktivierten Schlüssel aktivieren.

DISABLE .....Den ausgewählten Schlüssel deaktivieren, d.h. dieser Schlüssel wird nicht gelöscht, sondern steht bei der Schlüsselauswahl vor der Verschlüsselung nicht zur Auswahl. In der Schlüsselverwaltung erscheinen sie kursiv. Diese Funktion ist sinnvoll, um große Schlüsselbunde übersichtlich zu halten, indem selten gebrauchte Schlüssel deaktiviert werden.

REVOKE.....Mit der REVOKE-Funktion kann das eigene Schlüsselpaar für ungültig erklärt werden. Von dieser Funktion ist Gebrauch zu machen, wenn der priva-

te Schlüssel unerlaubt kopiert wurde und der Anwender Gefahr läuft, dass Fremde seine Mails lesen können.

Das Schlüsselsymbol erscheint anschließend mit einem roten Querbalken durchgestrichen. Der jetzt ungültige Schlüssel kann nun an einen Key Server geschickt oder mit der EXPORT-Funktion seinen Kommunikationspartnern zugesandt werden. Der ungültige Schlüssel kann fortan nicht mehr benutzt werden.

IMPORT ..... Öffentliche Schlüssel werden i.d.R. als Datei an E-Mails angehängt oder auf Diskette weitergegeben. Hat der Anwender von seinem Kommunikationspartner eine solche Datei erhalten, kann er durch die Import-Funktion den Schlüssel in seinen Schlüsselbund aufnehmen.

EXPORT ..... Der Anwender kann seinen öffentlichen Schlüssel oder auch den ganzen Schlüsselbund mit den öffentlichen Schlüsseln seiner Kommunikationspartner exportieren, d.h. durch diese Funktion in einer Datei speichern. Die Datei kann so z.B. als Attachment an E-Mails angehängt werden.

Private Schlüssel können ebenfalls exportiert werden, dazu ist vom Anwender im Folgebildschirm das Auswahlkästchen EXPORT PRIVAT KEY(S) zu aktivieren.

SELECT COLUMNS ..... Anzeige der Infospalten erweitern bzw. einschränken.

KEY PROPERTIES ..... Zeigt die Eigenschaften des ausgewählten Schlüssels an, wie in der Abbildung unten dargestellt. Bei dem eigenen Schlüssel kann der Anwender das Mantra durch Klick auf die Schaltfläche CHANGE PASSPHRASE ändern.

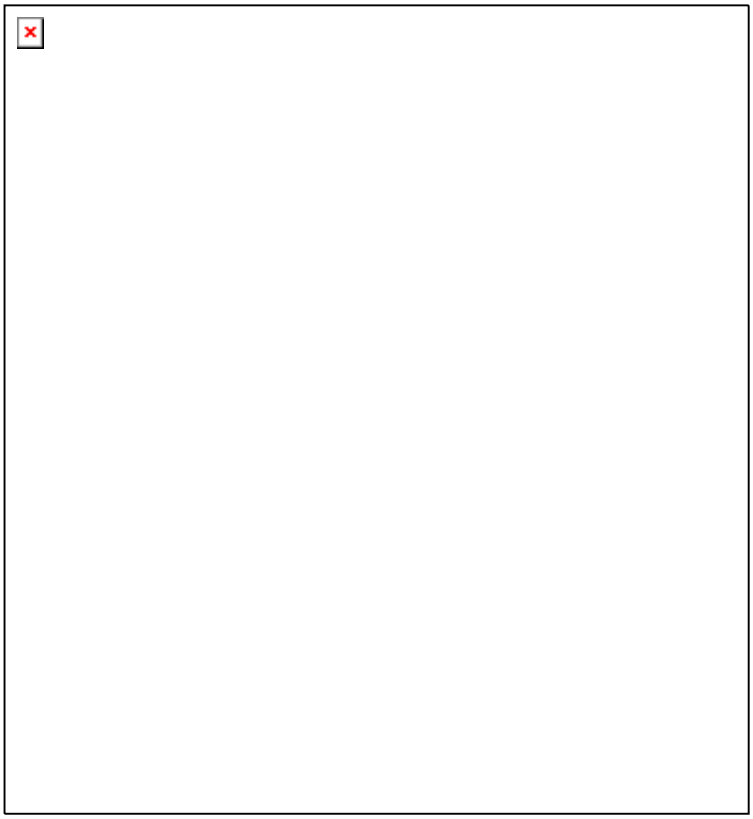


Abbildung 49: Anzeige der Schlüsseleigenschaften

Während die Eigenschaft „Trust“ bei öffentlichen Schlüsseln der Kommunikationspartner lediglich die Werte „untrusted“, „marginal trusted“ oder „complete trusted“ annehmen kann, besitzen eigene Schlüssel automatisch höchstes Vertrauen. Die Standardeigenschaft ist deshalb bei eigenen Schlüsseln „Trust: Ultimate“, wie in der Abbildung 49 zu sehen ist. Deaktiviert der Anwender die Eigenschaft IMPLICIT TRUST, so wird der eigene Schlüssel einem gewöhnlichen Schlüssel gleichgestellt und der Anwender kann wieder zwischen einer der drei bekannten Vertrauensstufen wählen.

Die übrigen Eigenschaften wurden bereits weiter oben beschrieben.

GROUPS

NEW GROUP.....Um ein großes Schlüsselbund übersichtlich zu gestalten, kann man mit dieser Funktion Gruppen bilden, denen dann Schlüssel zugeordnet werden. E-

Mails können später durch Auswahl einer Gruppe mit allen darin enthaltenen Schlüsseln einzeln chiffriert werden. Diese Funktion ist insbesondere bei Rundschreiben interessant.

SHOW GROUP .....Wenn Gruppen gebildet wurden, können sie durch Aktivierung dieser Funktion angezeigt werden. Ein zweiter Klick deaktiviert die Gruppenanzeige wieder.

IMPORT GROUP .....In Dateien abgespeicherte Gruppen können hier dem eigenen Schlüsselbund hinzugefügt werden.

GROUP PROPERTIES....Dient zur Änderung des Gruppennamens bzw. zur Änderung der Gruppenbeschreibung.

HELP

HELP TOPICS .....Aufruf der Hilfethemen

REGISTER ONLINE .....Aufruf der Online-Registrierung

ABOUT PGP .....Informationen zur benutzten PGP-Version: Versionsnummer, Lizenzangaben, Copyrightvermerke, Link zur PGP-Website, Patennummern, Angaben zum Entwicklerteam.

Die Funktionen sind zum Teil auch im Kontextmenü, d.h. durch Markieren eines Schlüssels und Klicken der rechten Maustaste, aufrufbar.

4.2.3 Verschlüsseln und Signieren von E-Mails

PGP ist ein reines Verschlüsselungsprogramm, aber kein Mailprogramm. Zum Empfang und zum Versand verschlüsselter und signierter Nachrichten ist daher immer auch ein Mailprogramm notwendig. PGP kann zusammen mit jedem Mailsystem genutzt werden. Die Funktionen von PGP können in einigen Programmen wie Eudora oder MS Outlook mittlerweile komfortabel über Plug-Ins aufgerufen werden. Andernfalls können die Nachrichten in den Zwischenspeicher kopiert werden, um sie anschließend von PGP bearbeiten zu lassen.

Bevor PGP eine E-Mail chiffrieren oder signieren kann, ist die E-Mail zu erstellen. Dies kann wie gewöhnlich im Editor des benutzten E-Mail-Programms geschehen. Beispielnachricht:

```
Sehr geehrter Herr Dr. Peters,

ihr Kontostand beträgt: DM 4.520,00 (Soll)

Mit freundlichen Grüßen
Musterbank
Abtlg. elektr. Zahlungsverkehr
```

Abbildung 50: Beispielnachricht

4.2.3.1 Verschlüsseln und Signieren mit Hilfe des E-Mail-Plug-Ins

Wenn ein Plug-In installiert wurde, sind in der Symbolleiste des E-Mail-Editors neben dem rechten Icon zur Aktivierung der Schlüsselverwaltung zwei weitere Schaltflächen für die Verschlüsselung bzw. Signierung von E-Mails zu finden:

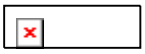


Abbildung 51: Schaltflächen zur Verschlüsselung und Signierung

Die linke Schaltfläche aktiviert die Verschlüsselung, die mittlere die Signierung. Chiffrierung und Signierung können sowohl einzeln als auch zusammen verwendet werden.

Wurden die Schaltflächen zur Chiffrierung und/oder Signierung aktiviert, so wird chiffriert/signiert, wenn die E-Mail durch das E-Mail-Programm zum Versand vorbereitet wird, d.h. nachdem der Anwender bei seinem E-Mail-Programm die Schaltfläche SENDEN oder entsprechendes geklickt hat. Der Sendende bekommt weder die verschlüsselte Nachricht noch die Signatur zu Gesicht.

Die Schlüsselauswahl wird von PGP automatisch vorgenommen, indem es den passenden öffentlichen Schlüssel zu dem im Adressfeld genannten Empfänger heraussucht. Zur Bestätigung des Empfängerschlüssels wird das Schlüsselbund eingeblendet.

Für den Fall, dass zu dem Empfänger im Adressfeld kein passender öffentlicher Schlüssel im Schlüsselbund gefunden werden kann, wird der Anwender auf diese Tatsache hingewiesen. Dazu wird der Schlüsselbund eingeblendet, damit der dazugehörige öffentliche Schlüssel vom Anwender ausgewählt werden kann (Der Vorgang der Schlüsselauswahl ist bei der Verschlüsselung mittels Zwischenspeicher immer notwendig und wird daher im nächsten Kapitel beschrieben.).

Vor der Signatur mit dem eigenen privaten Schlüssel muss der Anwender den Schlüssel durch Eingabe der Passphrase freigeben.

Alternativ zu den Schaltflächen kann auch der Menüpunkt PGP in der Menüzeile angewendet werden. Die Funktionen ENCRYPT ON SEND und SIGN ON SEND entsprechen den hier beschriebenen Schaltflächen. Unter dem Menüpunkt PGP finden sich auch die Befehl ENCRYPT NOW, SIGN NOW und ENCRYPT & SIGN NOW. Diese Befehle bewirken eine sofortige Verschlüsselung und Signierung, schon bevor die Nachricht durch das Mail-Programm für den Versand vorbereitet wird. In diesem Fall wird dem Anwender die verschlüsselte Nachricht bzw. die Signatur angezeigt.

4.2.3.2 Verschlüsseln und Signieren mit Hilfe des Zwischenspeichers

Wenn kein Plug-In installiert wurde, kann der Anwender die E-Mail mit Hilfe des Zwischenspeichers verschlüsseln und/oder signieren.

Eine geschriebene Nachricht wird dazu zunächst markiert und kopiert. Das Kopieren kann sowohl über den entsprechenden Menüpunkt im E-Mail-Programm bzw. im Kontextmenü (rechte Maustaste) oder auch über den Shortcut Strg+C geschehen. Die Nachricht befindet sich somit in dem Zwischenspeicher. Nach einem Mausklick auf das Icon PGPtray in der Taskleiste kann die gewünschte Option ausgewählt werden: ENCRYPT CLIPBOARD (nur verschlüsseln), SIGN CLIPBOARD (nur signieren) oder ENCRYPT & SIGN CLIPBOARD (verschlüsseln und signieren).

Zur Verschlüsselung wird die Liste der zur Verfügung stehenden Schlüssel eingeblendet:

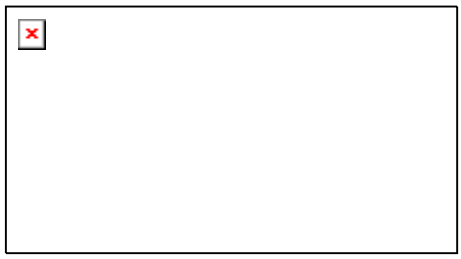


Abbildung 52: Schlüsselauswahl

Durch Ziehen in das unten stehende Empfängerfeld oder durch Doppelklick können ein oder mehrere Schlüssel und sogar ganze Schlüsselgruppen ausgewählt werden. In diesem Fall verschlüsselt die Bank mit dem Empfängerschlüssel von Dr. Peters und gleichzeitig auch mit dem eigenen Schlüssel der Abteilung „Elektr. Zahlungsverkehr“. Die Verschlüsselung mit dem eigenen Schlüssel hat den Zweck, den chiffrierten Text später auch selbst wieder entschlüsseln zu können. Der Text im Zwischenspeicher wird nach Klicken des OK-Buttons mit den ausgewählten Schlüsseln chiffriert.

Zur Signatur gibt die Bank ihren privaten Schlüssel mit Hilfe des Mantras frei.

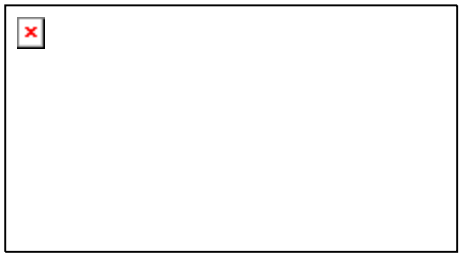


Abbildung 53: Nachricht signieren

Der verschlüsselte und/oder signierte Text befindet sich nun im Zwischenspeicher. Im E-Mail-Programm kann der Anwender nun durch Klicken der rechten Maustaste und Auswahl der Funktion EINFÜGEN den chiffrierten/signierten Text in den Texteditor des E-Mail-Programms einfügen und zum Versand vorbereiten.

4.2.4 Entschlüsseln und Verifizieren verschlüsselter Mail

Der Beispieltext als **unverschlüsselte, aber** (wie hier mit einem DH/DSS-Schlüssel) **signierte** Nachricht hat folgendes Format:

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Sehr geehrter Herr Dr. Peters,

ihr Kontostand beträgt: DM 4.520,00 (Soll)

Mit freundlichen Grüßen
Musterbank
Abtlg. elektr. Zahlungsverkehr

-----BEGIN PGP SIGNATURE-----
Version: PGP for Business Security 5.5.3

iQA/AwUBNpoY2zrwecdRYNP0EQLa/QCfVcRlDM/mq47dzKBvn0+w1K8kwrkAoMrs
Qz8DHQkl+G5lK37qb6NVHidK
=hE4/
-----END PGP SIGNATURE-----
```

Abbildung 54: Signatur unter einer unverschlüsselten Nachricht

Verschlüsselt (wie hier mit einem DH/DSS-Schlüssel)**, aber nicht signiert**, besitzt der Beispieltext folgendes Aussehen:

```
-----BEGIN PGP MESSAGE-----
Version: PGP for Business Security 5.5.3

qANQR1DBwU4Dxjh4AZPSjEUQB/9OhrVjExkr5gFEHCiZzhsaNeTFkmWcI52zQ8Rq
0pj6+neJKGUolXvV5sg+zL4cvSj2PM9demfVXisgptywsN9enehr7/wsclAI8MC3
9D6u4Zq8kMNz4NHrjrxDnMhbcTMBV/Z+OVxQtXsavrWbnweb8CjyZqC0mJgtIVYI
S5xazO20VI//h8Q0NfJVzjiy4cLQu3eDNyJpZ30hb9lx3T+7BH+jH6AaQ/KJlnYd
LI1CGc1toE1JPtDmLqWJ1ANmBb35ljqBkpiG9cQJfRLoUTuPrxX6lrgY5UVphlkE
PA1JzWURlnGtau2ONA83NnnXR2cqh1A91Ya8RNRGSoiYC8aeCADZmtPw8pCRbaEK
+84yHsIaatO8/gN7Ijh85uNA9y3X2SxhWMbFZKe6Vt2MuxjRMX8cAQo+zB7DnRdo
S+CbI1PTqwW7ipOX2OTkgFhzS9Sr5kdP/1OLd/o/n44bRDY65smmRaHxpf6Eg+uI
JPpJIqmNsz/4h7GIFsaoj0k4uzaYZrT9YE33zE8Zy0i84tkwc9OAzjVWuG3GL2M0
/SvUt1Do/wpgF+iQVoeWLn5ks6txWxSVX5LPDyjMsAAy+VBMlmVygTYVjhcKPQKU
6BevXIGB4CHZzsWsUP2STNFJKQ6xwlF0FlZSWmPSdB2jyuyib1zaiL99eJsIYI4t
3H6gHyo9wcFOAzePrKrGZU5+EAf/aUM2HE/hF+yX1I5sr+igsmeZYjjpc+trgEne
/pdwnr+kM3wC4aAQMAHcvf0jrsdaBMauRIXx4wKSgzxcBn0Y44ZWUMWsSstHX8r0
+GGmxHmqvSZf/hHmIzYFBdMJ14vFrnHZxVqhcpCLb38cENSmwwFglsS6M4Bvg7K1
zNPAen83N3swnvM30mR0ojlZE/I/OBKouM670IcAKsTJVt6ohex1Tiz3U/NwSR2y
WJr2VjVBDZPCZVFChvrYoT5uPlM8GQaecHFavOOi9nQhNaMQ+RNyF+7+eF5uqNZq
Eoi3VmQ1gmoyImgugEtBFTaFTzKagh0xm68wznZ/ryeM4rEK5wf+Oh3fj8Lb8VYD
5GXM8h18UkiLY9phtF98oFPJABKMIlmnVdGfcv1NaFWraCRF0oDpFg9+s3deG/wO
FeOR1tUCiIFJ8sjK+bm531g1dafZjkAav+rP5AOJmaNwe+cby4OYAOjvWwQ5LG6F
1bNh1Xn6tZPv/xSg/5N2R2PjYm974V4E8uV8gxMRXKb/6et+vJp6lc/DQwfD9rnd
qQs98WAP7fRfCySV9MK6hlzIxUPGuFt/7JkzTSSnoMDbF8GJ2cge+ClhzIGOjtXE
c6ipVS8aEcpPTJHDDIMPYLuOCMosyWQLUfVe+fB52ofyqGdF1z37K4gO+pNGuq8T
6pX6xcHDMMmjcu6Ws4DeN1JNYuM9SaPETlV9stZp7Qey2ZXvIv0CJLDBLo2VUvSB
elIm/WFB92PcV3/Ym/DbOQcuIZXNrnZri6V36tzYqsImSxR77PixQMlD/lQl5R27
i5BiBSmcQ+z+bNvPN7dFkmGQriBkkI7DOYaJYGhyTeI0LKHtSr4bxwbMhJ/ikq5B
OHIGF1+7jCZGYd32s7YTlgUoD7s68AraJlFWXw==
=d76g
-----END PGP MESSAGE-----
```

Abbildung 55: Verschlüsselte Nachricht

Nachrichten, die (wie hier mit einem DH/DSS-Schlüssel) **verschlüsselt und signiert** sind, haben auf den ersten Blick das gleiche Format wie verschlüsselte und unsignierte Nachrichten. Die Signatur wird ebenfalls verschlüsselt und an den verschlüsselten Text angefügt, aber nicht extra ausgewiesen.

Derselbe verschlüsselte Beispieltext ist inklusive Signatur daher um die entsprechende Zeichenzahl länger:

```
-----BEGIN PGP MESSAGE-----
Version: PGP for Business Security 5.5.3

qANQR1DBwU4Dxjh4AZPSjEUQB/0SRPZQtuso+R2P2/xKPkj26MaA+9GJdMSMefbE
AALBMTnktcTD/kZ1hDbygAds2mJgXnkuUqS7Ww8XrozfbWzzbtzX7OEEGDpLtLfE
kleToTiOXa4ETBzVZAlV/nmoX/69oN07Ye+OjkWDHrnNwOf3XhuKd9v+DHYEnj5c
pc7WdmYh6cODBhyoQzU0KSg4s3aS+ArAIIn+IWGv/buH/VTNAxaZSbMNoiHHveJM
gjM7Hl5/8JjtZNg5XEy1PzROQfMuDM0tNmnKj0heB7q6YiZgoHQICbuUGqrm/+YE
LZz1EDht1LejhJc+Pos+3UjNBuybkmF904idCzy9/jXGhwl8B/4wTG5pSuJTDz/V
jGEaCdbNmgeGabRA7s2pvW/fqbeMAkUuWY8PhDSV5OUgZGFtfQGTnRF3nee3dDhF
/2Vl35i/nyPY5vzy0PKsLJlPLuwNi87arK6D4jzRk3thLvMPZmepB8jIpXIHbH5U
NaxBY1ktbbyldM3GJeGmMuQKuaLqzFVkRHe2vmSolOhMULOFFlSaQFYwTQU3ISs1
o7ys+yQ9KQ+6DJ7Ow67d74/ESOEPp8sqBYvrbA1lnbDDn6aUAqn91rfXh8lxWgtn
N8AiPCTTZXyXMucc9aMlKVSOJIWlgQUHdkEVnfnNsprwOOPdx35n9ZSHkY1o9kO6
mKhWXI3/wcFOAzePrKrGZU5+EAf/RXdokmMC/3tZUaLu5UOr/U+bHA4E/X0xXbsT
yAIlPXbyvST2V94u6pWgQmOBOwV2u9pvDWGx+KmgXIY/0yV1f4QLFgR4HVKSHAV7
4cbgxKQkT/cMcPM8t+mfNxdmiVTy0d2HDzusKFkPxtASo9PCybxaY44FPAg5PHwI
Om74rwcCxiD1wctI+jQPrmprDMWYZyFM1OFrA4cnfayN7F6fKvzUBonEH1NvYqJi
CvR9iVeyYx7/EAKS6CpdX65hrW+AbZrSbFr0aFvjrOhVO7DxvQVISn6gWkTZnIsq
cZEOiKJqxLVA0jsGc0AIvHzSC4N3i4NaP0xdOWtZqFK8RPzj1gf+PfjrRR1mTydT
Ek+WlOCc07up0637Od4JqwpWFYID16MLJo23BcVjpRe8/7j3kZWsWee3s+CMaHFV
fwQMR11VJjCOvwruEuE9TKmrkhNXjwEwOVS2y9GMOXql0Oj+6bcK3TC2GFG3Fk0m
ihJpoC4p3tDcanZpINGZ8RsypGzOJLOixsbZ3BlFQQOviGQGvGY5tfXBtmAgiFRa
AgJ3Eu4Cil3xBe2ZH6bqhxiHWA65/1pxa+PhaL9pGXtUEKFG6fw1hDsRowqLeen2
oWgXT6tHKvUiAjvapt9wVsAhdMzCawdDcZHAxIuhgEWl6mJZsS8dA20p0ifUYDZF
yO/I5L3r4snAMckBu8hyPWj3LxTIynXLDWI950zMc/+MdJZ7f+S6aBRGpDPrTinh
lj+SUbybWZZCY0owggvGcVsOhqScV89ZASJwgFudZWQNixzRF29foFxiVKC8PcNU
RxAEOO1SRIl436GYXKfjlzlK53SQEx0lJjnI8c75gk4i6MHUMt97l+9OenIhrhvq
GH+HbkCBQ3mG4m/tcGUNr11xyzde+KdbeIEItc/EmxwzbideCMyuAJs5k75kGuAW
dxm7Nd8M6o3shhFp0IQN/5oS1ISFt0CPPjxosgwZj+9yHG80l8eBR0W2ZXlA8cez
w7iLe7iTNYbYtg0=
=qi5y
-----END PGP MESSAGE-----
```

Abbildung 56: Verschlüsselte und signierte Nachricht

4.2.4.1 Entschlüsseln und Verifizieren mit Hilfe des E-Mail-Plug-Ins

Wenn ein Plug-In installiert wurde, befinden sich beim Lesen von eingegangenen Nachrichten in der Symbolleiste des E-Mail-Programms neben dem rechten Icon zur Schlüsselverwaltung zwei weitere Schaltflächen:

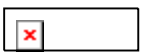


Abbildung 57: Schaltflächen zur Dechiffrierung und Verifizierung

Die linke Schaltfläche dient der gleichzeitigen Dechiffrierung und Verifizierung. Die mittlere Schaltfläche fügt einen öffentlichen Schlüssel dem Schlüsselbund zu, wenn der Schlüssel nicht als Schlüsseldatei, sondern als E-Mail im ASCII-Format geschickt wurde.

Wird die linke Schaltfläche betätigt, so prüft PGP, ob und mit welchem öffentlichen Schlüssel die erhaltene Nachricht chiffriert wurde. Findet PGP den dazugehörigen privaten Schlüssel in dem eigenen Schlüsselbund, so fordert das Programm zur Eingabe der Passphrase auf.

Abbildung 58: Dechiffrierung: Eingabe der Passphrase

Wenn die korrekte Passphrase eingegeben wurde, wird der Text entschlüsselt und in einem Textfenster ausgegeben. Enthält die Nachricht eine Signatur, so wird diese zusammen mit Signaturdatum und -uhrzeit ebenfalls ausgegeben.

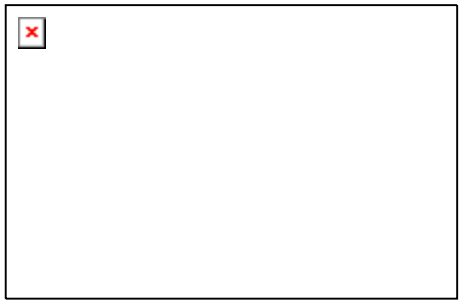


Abbildung 59: Ausgabe des dechiffrierten Textes und der Signatur

Mögliche Fehlermeldungen bei chiffrierten Nachrichten:

Die Änderung einer chiffrierten Nachricht, z.B. durch Hinzufügen eines Zeichens während der Übertragung, zerstört die Nachricht. Sie ist nicht mehr zu entschlüsseln. PGP reagiert darauf mit nebenstehender Meldung.

Abbildung 60: Fehlermeldung bei einer veränderten chiffrierten Nachricht

Wurde mit einem öffentlichen Schlüssel verschlüsselt, zu dem der passende private Schlüssel nicht im Schlüsselbund enthalten ist, so gibt PGP den Hinweis aus, dass der zur Chiffrierung genutzte öffentliche Schlüssel nicht bekannt ist.

Mögliche Fehlermeldungen bei signierten Nachrichten:

Die Warnung „Bad Signature“ kann aus zwei Gründen angezeigt werden:

1. Der Nachrichtentext wurde nach der Signierung geändert.
2. Die Signatur wurde ausgetauscht, d.h. Signatur und Nachricht gehören nicht zusammen.

Abbildung 61: Meldung bei veränderter signierter Klartextnachricht

Ist der zur Signatur gehörige öffentliche Schlüssel des Senders nicht in dem eigenen Schlüsselbund enthalten, so kann PGP die Signatur nicht prüfen und teilt dies mit der nebenstehenden Meldung mit. PGP kann in diesem Fall auch nicht prüfen, ob die Nachricht nach der Signierung verändert wurde oder nicht.

Abbildung 62: Fehlermeldung bei Signatur ohne dazugehörigen öffentl. Schlüssel

4.2.4.2 Entschlüsseln und Verifizieren mit Hilfe des Zwischenspeichers

Auch hier erfolgen Dechiffrierung und Verifizierung in einem Arbeitsschritt. Die empfangene Nachricht wird von dem Empfänger durch ein E-Mail-Programm geöffnet. Der ganze Text wird markiert und anschließend in den Zwischenspeicher kopiert. Ein Klick auf das Icon PGPtray in der Taskleiste und Aktivierung der Funktion DECRYPT/VERIFY CLIPBOARD dechiffriert und verifiziert den Text. Bei verschlüsselten Nachrichten wird der Empfänger aufgefordert, seine Passphrase einzugeben. Bei signierten Nachrichten wird die Signatur über den öffentlichen Schlüssel des Senders geprüft.

Die Eingabe der Passphrase zur Dechiffrierung, die Prüfung der Signatur und die Ausgabe sind gleich den im letzten Kapitel beschriebenen Schritten.

4.2.5 Sonstige Funktionen

4.2.5.1 Konventionelle Verschlüsselung

PGP kann Daten auch konventionell, d.h. lediglich mit einem symmetrischen Verschlüsselungsalgorithmus verschlüsseln. Anstatt den Empfän-

gerschlüssel auszuwählen, aktiviert der Anwender die Option CONVENTIONAL ENCRYPTION (vgl. Abbildung 52 oder Abbildung 63). Das Programm fordert den Anwender daraufhin zur Eingabe einer Passphrase auf.

Wie auch beim Schutz des privaten Schlüssels, wird hier durch eine Hashfunktion aus der Passphrase ein Code berechnet. Dieser dient als Schlüssel zur Chiffrierung bzw. Dechiffrierung mittels eines symmetrischen Chiffrieralgorithmus.

Um die Daten wieder entschlüsseln zu können, benötigt der Empfänger die Passphrase.

4.2.5.2 Verschlüsselung von Dateien

Zu Beginn des Kapitels 4.2 wurden bereits die Funktionen des Moduls PGPtools vorgestellt. Die Handhabung erfolgt analog zu den entsprechenden Funktionen bei der Verarbeitung von Textnachrichten.

Abbildung 63: Optionen bei der Dateiverschlüsselung

Auch für Dateien besteht die Möglichkeit, sie konventionell zu verschlüsseln. Der Benutzer hat zusätzlich die Option, die verschlüsselte Datei in druckfähige ASCII-Zeichen Aktivierung der Option: TEXT OUTPUT, siehe Abbildung) umzuwandeln oder die Datei im binären Format zu belassen. Die Umwandlung ist sinnvoll, wenn das benutzte E-Mail-Programm Dateien nicht als Attachment verschicken kann. Eine in ASCII-Code umgewandelte Datei, man spricht auch vom Format *ASCII-Armor*, kann dagegen von jedem E-Mail-Programm wie eine gewöhnliche Textnachricht versendet werden.

Mit der Option WIPE ORIGINAL kann der Benutzer gleichzeitig zur Verschlüsselung die Originaldatei löschen lassen. Andernfalls bleibt die Originaldatei bestehen. Eine verschlüsselte binäre Datei erhält den Zusatz „PGP Encrypted File“ bzw. „PGP Armored Encrypted File“, wenn sie in ASCII-Code umgewandelt wurde.

Auch die Signatur einer Datei kann in ASCII-Zeichen (Option: Text Output) umgewandelt werden, standardmäßig bleibt sie jedoch eine Datei binärer Daten.

Abbildung 64: Optionen bei Signatur von Dateien

Die zweite Option DETACHED SIGNATURE FILE bewirkt, dass die Signatur separat zur signierten Datei in einer eigenen Datei gespeichert wird. Eine Deaktivierung ist nicht zu empfehlen, denn das Hinzufügen der Signatur zu der Datei hat bei einigen mit Anwendungen verbundenen Dateien zur Folge, dass sie nicht mehr geöffnet werden können.

4.2.6 Optionen

Durch Aufruf des PGPtray in der Taskleiste und Auswahl der Funktion PGP PREFERENCES kann der Anwender in den Registern GENERAL, FILES, EMAIL, SERVERS und ADVANCED eine Vielzahl von Optionen einstellen.

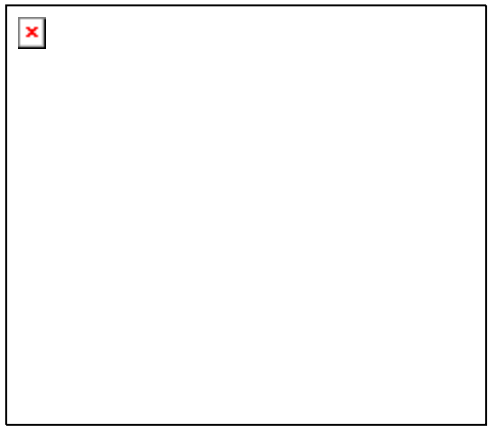


Abbildung 65: Optionen: Register General

Register GENERAL

ALWAYS ENCRYPT TO DEFAULT KEY

Nach Aktivierung der Option erfolgt die Verschlüsselung zusätzlich zum Empfängerschlüssel automatisch auch mit dem öffentlichen Schlüssels des Anwenders. Diese Funktion ist empfehlenswert, da anderenfalls eine verschlüsselte Nachricht nur noch vom Empfänger, nicht aber vom Sender entschlüsselt werden kann. Das würde bedeuten, der Sender hat keine Möglichkeit, seine eigene Nachricht wieder zu dechiffrieren. Ist die Option jedoch aktiviert, kann auch der Sender die Nachricht später wieder lesen und überarbeiten.

CACHE DECRYPTION/SIGNING PASSPHRASE FOR...

Die Passphrase kann durch Aktivierung dieser zwei Optionen für eine bestimmte Zeit im Arbeitsspeicher behalten werden, so dass sie während dieses Zeitraums bei einer weiteren Entschlüsselung oder Signierung die Passphrase automatisch verwendet wird.

Diese Option sollte sehr vorsichtig genutzt werden, denn wenn der Rechner während dieser Zeit unbeaufsichtigt gelassen wird, ist es Unbefugten mit

Zugang zu dem Rechner möglich, Nachrichten des Anwenders zu entschlüsseln... zu signieren.. usw.

COMMENT BLOCK

Der Empfänger legt hier einen Text fest, der im Nachrichtenkopf seiner verschlüsselten Nachrichten erscheinen kann.

FASTER KEY GENERATION

Mit der Aktivierung dieser Option wird bei der Generierung von DH-Schlüsselpaaren eine im voraus berechnete Primzahl benutzt, um die Schlüsselgenerierung zu beschleunigen. Auf diese Option sollte verzichtet werden.

DISPLAY WIPE CONFIRMATION DIALOG

Wird diese Option gesetzt, so warnt PGP, wenn eine Datei mit der Löschfunktion WIPE gelöscht werden soll. Diese Option sollte ausgewählt werden, denn eine Löschung mit der Funktion WIPE ist nicht mehr rückgängig zu machen. Die Warnfunktion schützt insbesondere vor versehentlichem Löschen und beugt einem Datenverlust vor.

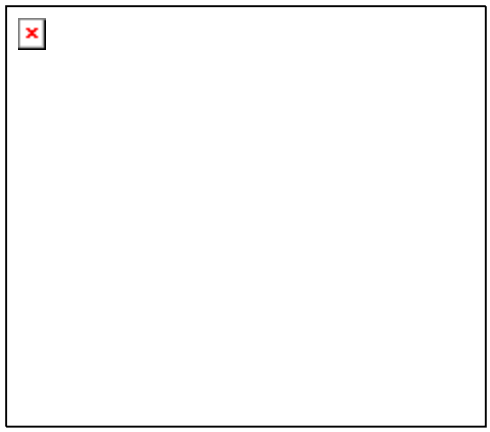


Abbildung 66: Optionen: Register Files

Register FILES

Das Register zeigt die Verzeichnisse an, in denen die Datei PUBRING.PKR mit den öffentlichen Schlüsseln, die Datei SECRING.SKR mit den privaten Schlüsseln und die Datei RANDSEED.BIN mit den Zufallsdaten zu finden sind. Standardmäßig sind diese Dateien im gleichen Verzeichnis gespeichert, in dem auch die PGP Programmdateien zu finden sind.

Wenn entsprechende Dateien aus anderen Verzeichnissen benutzt werden sollen, können diese nach Klicken der Schaltfläche BROWSE gesucht und bestimmt werden.

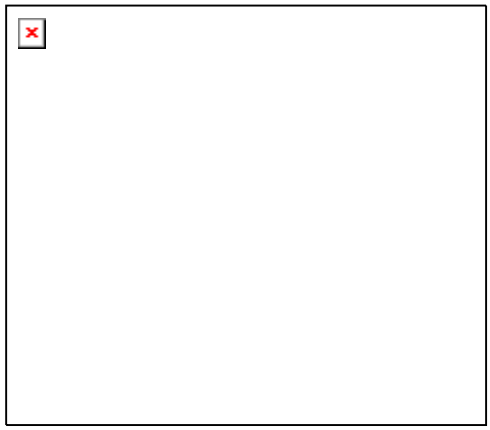


Abbildung 67: Optionen: Register E-Mail

Register EMAIL

USE PGP/MIME WHEN SENDIG EMAIL

PGP/MIME (MIME: Multipurpose Internet Mail Extensions) bezeichnet den Standard für die Integration der PGP-Funktonen in E-Mail-Programme. Sie automatisiert den Austausch von PGP-verschlüsselter E-Mail. Eine Aktivierung bedeutet, dass sämtliche E-Mails und Attachments automatisch beim Sender chiffriert und signiert sowie beim Empfänger dechiffriert und verifiziert werden. Diese Option ist nur sinnvoll, wenn sowohl Sender als auch Empfänger über ein E-Mail Programm verfügen, das PGP/MIME unterstützt.

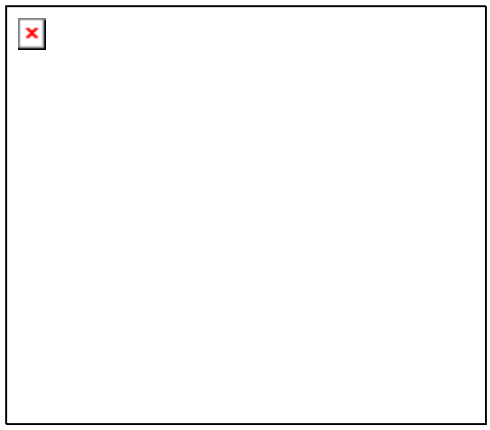


Abbildung 68: Optionen: Register Servers

Register SERVERS

Das Register zeigt die dem System bekannten Key Server an. Mit der Schaltfläche NEW können weitere Key Server hinzugefügt werden. Bestehende können mit REMOVE aus dem Verzeichnis entfernt oder mit SETDEFAULT als Standardserver festgelegt werden. Für ein Verzeichnis verschiedener Key Server siehe Anhang, Seite 105.

ENCRYPTING TO UNKNOWN KEYS

Wenn PGP zu der Empfängeradresse keinen entsprechenden Schlüssel findet, wird auf dem Key Server danach gesucht.

ADDING NAMES TO A KEY

Wenn einem eigenen Schlüssel neue Namen hinzugefügt werden, wird dies automatisch an den Key Server übertragen.

KEY SIGNING

Wird ein öffentlicher Schlüssel vom Anwender unterzeichnet, so wird dieser Schlüssel mit der neuen Signatur an den Key Server geschickt.

REVOCATIONS

Widerruft (Revoke) der Anwender den eigenen Schlüssel, so wird dies dem Key Server mitgeteilt.

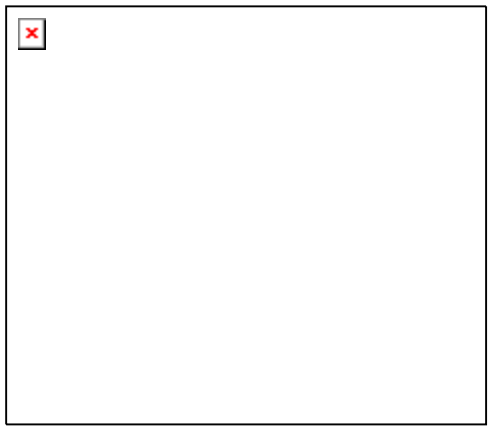


Abbildung 69: Optionen: Register Advanced

Register ADVANCED

ENABLED ALGORITHMS

Legt den bevorzugten symmetrischen Algorithmus fest, der zur Verschlüsselung genutzt werden soll. Dieser Algorithmus wird zum einen dann benutzt, wenn Dateien oder Texte auf konventionelle Weise verschlüsselt werden.

Zum anderen wird bei der Schlüsselgenerierung dem öffentlichen Schlüssel eine Zusatzinformation beigefügt. Hier wird festgelegt, welchen Algorithmus das PGP-Programm des späteren Absenders benutzen soll, wenn es den öffentlichen Schlüssel des Empfängers benutzt.[89] DH-Schlüssel können jeden der drei Algorithmen enthalten, RSA-Schlüssel lediglich den IDEA-Algorithmus.

DISPLAY MARGINAL VALIDITY LEVEL

Zeigt Schlüssel nicht als „gültig“ (grüner Punkt) oder „ungültig“ (grauer Punkt) an, sondern als „voll gültig“ (grauer Balken), „marginal gültig“ (halb gefüllter grauer Balken) und „nicht gültig“ an (leerer Balken) an. Schlüssel sind „marginal gültig“, wenn sie von Personen unterschrieben wurden, deren Vertrauen vom Anwender als „marginal“ eingestuft wurde.

TREAT MARGINALLY VALID KEYS AS INVALID

Warnt den Benutzer, wenn mit einem Schlüssel chiffriert wird, der nicht „voll gültig“ ist.

WARN WHEN ENCRYPTING TO KEYS WITH AN ADK

Warnt den Anwender vor der Chiffrierung, wenn der Empfängerschlüssel mit einem ADK versehen ist. Der Anwender wird somit darauf hingewiesen, dass nicht nur der Empfänger, sondern auch ein Dritter, der Besitzer des ADK, die Nachricht lesen kann.

---

[89] Vgl. Kai Raven, Deutsche Anleitung zu PGP 5.5.x, Kapitel 04. URL: http://home.kamp.net/home/kai.raven-/index.html. Stand 29.10.1998.

5 Hinweise zur Einführung der Software PGP

In diesem Kapitel erfahren Sie:

- das richtige Schlüsselmanagement mit Empfehlungen zum Aufbau einer Public Key Infrastruktur,
- Tipps zur Auswahl des Mantras,
- wie man einem Verlust des Mantras oder des privaten PGP-Schlüssels vorbeugt,
- Anmerkungen zur Rechtskraft der digitalen Signatur.

5.1 Schlüsselmanagement

Der Erfolg des Einsatzes von PGP ist unmittelbar vom richtigen Schlüsselmanagement abhängig. Über die Kenntnis des Moduls zur Schlüsselverwaltung PGPkeys hinaus ist damit der verantwortungsbewußte Umgang mit sämtlichen Schlüsseln sowie eine sinnvolle Schlüsselverteilung gemeint.

5.1.1 Empfehlungen zum Speicherort der Schlüssel

Die Dateien PUBRING.PKR, SECRING.SKR und RANDSEED.BIN sind standardmäßig im gleichen Verzeichnis wie auch die Programmdateien PGPs auf der Festplatte des Rechners installiert. In einigen Fällen ist aus Sicherheitsgründen eine Änderung des Speicherortes empfehlenswert:

- **Öffentliche Schlüssel – die Datei PUBRING.PKR**
  Als Speicherort der Datei PUBRING.PKR kann bedenkenlos das standardmäßige Verzeichnis belassen werden.

- **Geheime Schlüssel – die Datei SECRING.SKR**
  Für den ADK und den CSK sollte die Speicherung auf ein Wechselmedium, z.B. auf einer Diskette, und Verschluss an sicherer Stelle als unbedingt erforderlich angesehen werden. Damit kommt man auch der bildlichen Vorstellung eines Schlüssels sehr nahe, denn jeder Chiffrierungs- und Signiervorgang kann erst nach Einlegen der Diskette erfolgen.

Diese Sicherheitsvorkehrung ist sehr ernst zu nehmen, denn eine Kompromittierung des ADK oder des CSK hätte weitreichende Folgen: Einerseits ist mit dem ADK u.U. die gesamte chiffrierte Firmenpost zu entschlüsseln, andererseits wären die Signaturen des CSK nicht mehr zuverlässig und das unternehmensweite Web of Trust damit hinfällig.

Für die geheimen Schlüssel der Anwender gilt diese Empfehlung grundsätzlich auch, allerdings ist hier zu vermuten, dass sie sich in der betrieblichen Praxis nicht durchsetzen lässt. Wenn der geheime Schlüssel mehrmals am Tage gebraucht wird, wird der ständige Verschluss der Diskette mit dem geheimen Schlüssel schnell störend wirken, mit der Folge, dass die Diskette in einer jedermann zugänglichen Schublade landet oder gar auf die „lästige“ Verschlüsselung verzichtet wird.

Der geheime Schlüssel der Anwender kann daher, durch ein starkes Mantra geschützt, auf der Festplatte gespeichert werden, wobei dazu geraten sei, die Datei SECRING.SKR in ein anderes als das Standardverzeichnis zu verschieben, es im Windows-Explorer mit der Eigenschaft VERSTECKT zu versehen und auch mit einem anderen Namen zu bezeichnen. Der Anwender sollte zudem darauf achten, dass die Datei nicht auf irgendeine Weise, z.B. durch ein systemweites Backup in einem Netzwerk, unbemerkt kopiert und somit für einen Zweiten zugänglich wird.[90]

- **Zufallsdaten – die Datei RANDSEED.BIN**

  Auch wenn die Wahrscheinlichkeit, aufgrund der Zufallsdaten der Datei RANDSEED.BIN auf einen generierten Sitzungsschlüssel zu schließen, rein theoretischer Natur ist, wird dem Anwender im Handbuch[91] empfohlen, diese Datei Zweiten unzugänglich zu machen. Eine Speicherung auf einem Wechselmedium erscheint allerdings unangebracht, da die Datei für jeden Verschlüsselungsvorgang benötigt wird. Als Empfehlung kann daher die Befolgung der gleichen Anweisungen wie auch bei den geheimen Anwenderschlüsseln gelten.

5.1.2 Key-Revokation erzeugen

Mit Key-Revokation ist der Widerruf des eigenen Schlüssels durch den Anwender gemeint, siehe auch Seite 69. Dieser Vorgang sollte bereits früh-

[90] Vgl. PGP Security Officer’s Guide Version 5.5, 1997, S. 23.

[91] Vgl. PGP for Business Security, Windows User’s Guide Version 5.5 v, 1997, S. 103.

zeitig, d.h. kurz nach der Generierung des geheimen Schlüssels erfolgen. Diese zunächst scheinbar widersprüchliche Maßnahme ist sinnvoll, um eine nachteilige Konsequenz der folgenden zwei Fälle vorzubeugen:

1. Durch Diebstahl oder versehentliches Löschen kommt es zu einem Verlust des geheimen Schlüssels und seiner Sicherungskopie.
2. Der Anwender vergisst das Mantra und hat für diesen Fall keine Vorkehrung, wie auf Seite 94 beschrieben, getroffen.

In beiden Fällen ist es nicht mehr möglich, sein Schlüsselpaar über die Revoke-Funktion zu widerrufen, denn hierzu sind der geheime Schlüssel und das Mantra notwendig.

Um diesem Dilemma zu entgehen, sollte direkt nach der Schlüsselgenerierung eine Key-Revokation erzeugt werden. Dazu geht der Anwender folgendermaßen vor:[92]

1. Aufrufen des Moduls PGPkeys
2. Erstellen einer Kopie des öffentlichen und geheimen Schlüssels mittels EXPORT-Funktion (Schaltfläche EXPORT PRIVATE KEY(S) aktivieren!) und Speicherung auf Diskette.
3. Widerruf des eigenen Schlüsselpaares mittels REVOKE-Funktion, anschließend erscheint das Schlüsselpaar durchgestrichen.
4. Die Datei mit dem widerrufenen Schlüsselpaar exportieren (die Schaltfläche EXPORT PRIVATE KEY(S) nicht aktivieren) und unter einem aussagekräftigen Namen, bei einem RSA-Schlüssel z.B. „RSArevoke.asc“, auf Diskette abspeichern. Der Datenträger ist vor unbefugtem Zugriff zu schützen.
5. Das widerrufene Schlüsselpaar im Modul PGPkeys markieren und löschen. Nur so kann das ursprüngliche Schlüsselpaar anschließend wieder importiert werden.
6. Die Kopien des öffentlichen und privaten Schlüssels mittels der IMPORT-Funktion wieder in das Schlüsselbund aufnehmen.

Sollte nun einer der oben beschriebenen Fälle eintreten und eine Key-Revokation nötig sein, so sollte der Anwender für eine schnelle Verbreitung des widerrufenden Schlüssels sorgen, indem

1. die auf der Diskette gespeicherte Datei mit dem widerrufenen Schlüsselpaar wieder importiert und anschließend an einen Key-Server geschickt wird, und

---

[92] Vgl. Michael Uplawski, Deutsche Übersetzung der comp.security.pgp FAQ, Version 1.5, Kapitel 7.1ff.

2. diese Datei direkt an alle Kommunikationspartner gesendet wird.

5.1.3 Aufbau einer unternehmensinternen Public Key Infrastruktur

Unter dieser Überschrift sind einige Punkte zusammengefasst, die als Ablaufplan zum Aufbau einer Infrastruktur dienen können, bestehend aus einem unternehmensweiten Web of Trust, einem einheitlichen Schlüsselbestand und Grundsätzen zur Verbreitung der Schlüssel.

1. **Zertifizierung des CSK durch eine Zertifizierungsstelle, z.B. TC Trustcenter.[93]**

   Die Zertifizierung eines PGP-Schlüssels durch eine Zertifizierungsstelle ist mit Kosten verbunden. Dieser Punkt ist somit als Tipp für diejenigen Unternehmen zu sehen, die zwar generell von einer Zertifizierung Gebrauch machen, jedoch eine Zertifizierung aller Mitarbeiterschlüssel aus Kostengründen umgehen möchten.

   Bei der angegebenen Zertifizierungsstelle kostet die Zertifikatsverwaltung zwischen DM 96,00 und DM 120,00 jährlich, dies ist abhängig von der Anzahl der beantragten Zertifikate. Zusätzlich fallen pro Zertifikat einmalige Registrierungskosten von DM 5,00 bis DM 20,00 an.[94] Unternehmen, die diese Kosten scheuen oder PGP zunächst erproben wollen, sollten zumindest den Corporate Signing Key zertifizieren lassen. Wenn die öffentlichen Schlüssel der Mitarbeiter mit einer **exportierbaren** Signatur durch den CSK versehen werden, entsteht eine „Zertifizierungshierarchie“, anhand derer ein Dritter die Echtheit eines Mitarbeiterschlüssels kontrollieren kann: Anhand der Zertifizierung kann der CSK geprüft und seine Echtheit bestätigt werden. Die Signatur eines Mitarbeiterschlüssel durch den „echten“ CSK garantiert für die Echtheit des Mitarbeiterschlüssels.

   Voraussetzung ist, dass der Dritte neben dem öffentlichen Mitarbeiterschlüssel auch den öffentlichen CSK besitzt, damit er die Zertifizierung des CSK auch überprüfen kann. Der CSK ist daher, wie in Punkt 3 und 4 beschrieben, zu veröffentlichen.

---

93 Http://www.trustcenter.de

94 Stand 31.12.1998. Die Preise gelten zusätzlich der gesetzlich gültigen Mehrwertsteuer.

2. Aufbau eines unternehmensweiten Web of Trust

Unter der Voraussetzung, dass bei der Konfigurierung des Client-Setup (Kapitel 4.1.3) eine automatische Signierung des CSK durch die Client Keys festgelegt wurde, kann nun ein unternehmensweites Web of Trust aufgebaut werden, indem die öffentlichen Schlüssel aller Mitarbeiter mit einer exportierbaren Signatur des CSK versehen und im gegebenen Fall mit Vertrauen ausgezeichnet werden. Dasselbe gilt auch für externe Schlüssel. Nachdem sie auf ihre Echtheit hin geprüft wurden, können auch sie durch eine exportierbare Signatur mit dem CSK in das unternehmensweite Web of Trust mit einbezogen werden.

3. Die Schlüssel der Mitarbeiter sowie ADK, CSK und alle Schlüssel der externen Kommunikationspartner werden an einen Key Server des „pgp.net" geschickt.

Dadurch umgeht man folgendes Problem: In einem Netzwerk verwaltet jeder Benutzer PGPs einen eigenen Schlüsselbund mit den öffentlichen Schlüsseln seiner Kommunikationspartner. Dies erschwert den Aufbau einer unternehmenseinheitlichen Public Key Infrastruktur, da nicht jeder Benutzer auf den gleichen Bestand an öffentlichen Schlüsseln zurückgreift.

Durch das Versenden aller öffentlichen Schlüssel an einen Key Server des „pgp.net"[95] kann nun dieser Key Server als zentrale Schlüsselverwaltung dienen, auf dem somit u.a. sämtliche Schlüssel aller öffentlichen Schlüsselbunde des Unternehmens zu finden sind. Ebenso sind Aktualisierungen der Schlüssel, insbesondere die Signatur eines Schlüssels durch den CSK, zum Key Server zu schicken. Somit wird ein unternehmensweit einheitlicher, jederzeit aktueller Schlüsselbestand erzielt, der für jeden Anwender bequem über die im Modul PGPkeys enthaltene Schnittstelle zum Key Server abgerufen und aktualisiert werden kann.

4. Verbreiten der öffentlichen Schlüssel der Mitarbeiter und des CSK.

Mit Punkt 3 wurde bereits der erste Schritt getan, um die eigenen Schlüssel zu verbreiten. Die zweite Möglichkeit der Verbreitung besteht darin, dass jeder Anwender die Datei mit dem eigenen Schlüssel

[95] Es braucht nicht darauf geachtet werden, dass immer ein bestimmter Key Server des „pgp.net" benutzt wird. Der Schlüsselaustausch der Key Server untereinander geschieht in Sekundenbruchteilen, so dass problemlos von jedem Mitarbeiter ein anderer Key Server genutzt werden kann.

als Attachment an E-Mails anhängt. Insofern der CSK, wie in Punkt 1 beschrieben, zur Bestätigung der Echtheit des Mitarbeiterschlüssels dient, ist es sinnvoll, auch ihn den E-Mails hinzuzufügen. Für den Fall, dass das E-Mail-System des Senders oder des Empfängers keine Attachments verarbeiten kann, können die Schlüssel auch als ASCII-Zeichen verschickt werden. Die Schlüsseldatei liegt im ASCII-Format vor und braucht lediglich mit einem Texteditor ausgelesen und in den E-Mail-Editor kopiert zu werden.

Doch sicherlich ist es nicht praktikabel, jeder E-Mail diese zwei PGP-Schlüssel hinzuzufügen. Zum einen ist das Hinzufügen von Attachments für den Sender umständlich, zum anderen werden sich voraussichtlich viele Empfänger durch dieses Anhängsel belästigt fühlen, z.B. weil sie den Schlüssel schon haben oder aber mit dem Schlüssel gar nichts anfangen können, weil sie nicht im Besitz von PGP sind. In der Praxis findet man daher folgende Vorgehensweise, die hier als Empfehlung gelten soll:

Unter jeder E-Mail werden neben Grußformel und den Absenderangaben auch die Key ID des eigenen Schlüssels und gegebenenfalls des CSK geschrieben. (Bei den meisten E-Mail-Programmen kann dies automatisiert mit den vom Anwender gewünschten Daten erfolgen.) Diese Vorgehensweise wirkt nicht so störend wie das Versenden der Schlüssel, bietet aber die Möglichkeit, dass der interessierte Empfänger auf den Schlüssel aufmerksam wird und ihn entweder direkt vom Absender anfordern oder aber anhand der Key ID auf einem Key Server suchen kann.

Begleitend dazu sollte der Anwender auch dafür sorgen, den Fingerprint des eigenen Schlüssel und des CSKs auf geeignetem Wege zu verteilen, damit Kommunikationspartner sich von der Echtheit der Schlüssel überzeugen können. Die Veröffentlichung des Fingerprints kann z.B. auf der Homepage der Firma, auf Visitenkarten oder vergleichbare Weise erfolgen.

5.2 Auswahl des Mantras

Für den Fall, dass der geheime Schlüssel des Anwenders in die Hände eines Unbefugten gelangen sollte, ist er durch das Mantra geschützt. Dieser Schutz besteht selbstredend nur unter der Voraussetzung, dass der Dieb die Passphrase nicht kennt und nicht erraten kann. Die Problemstellung ähnelt der aus Kapitel 2.2.1.2, in der beschrieben wurde, dass der Zugang

zum Mail-Server zwar über Benutzerkennung und Passwort geschützt wird, das Passwort aber oftmals von einem Dritten mit vertretbarem Aufwand ermittelt werden kann.

Das Mantra muss, wie auch ein Kennwort, zwei Kriterien erfüllen:

1. Es darf für einen Unbefugten nicht zu ermitteln sein.
2. Es muss für den Anwender leicht zu merken sein.

Geht man davon aus, dass für eine Passphrase Groß- und Kleinbuchstaben sowie die Ziffern von 0-9 benutzt werden, ergibt dies bereits bei einer Passphrasenlänge von 8 Zeichen eine Anzahl von $8^{62} = 9{,}8 * 10^{55}$ möglichen Passphrasen. Eine Berechnung von Weikert[96] zeigt, dass selbst ein moderner Parallelrechner mit der Fähigkeit, 800.000 Passphrasen dieser Länge pro Sekunde zu berechnen, $3{,}88 * 10^{42}$ Jahre brauchen würde, um alle möglichen Kombinationen zu testen. D.h. im Durchschnitt würde in der Hälfte dieser Zeit, also nach $1{,}94 * 10^{42}$ Jahren eine Passphrase gefunden werden. Somit ist festzustellen, dass bereits 8 Zeichen für ein sicheres Mantra ausreichen.

Ein zufälliges Mantra, wie z.B. „kdN5li3Q“, ist allerdings prinzipiell schwer zu merken, so dass sich viele Anwender, wenn ihnen die Auswahl der Passphrase selbst überlassen bleibt, oftmals ein einfaches und leicht zu ermittelndes Passwort wählen, z.B. das eigene Sternzeichen oder den Namen der Freundin. Eine Studie von D. Klein[97] anhand von 14.000 benutzten Unix-Passwörtern hat gezeigt, dass knapp 25% dieser Passwörter mit der oben angesprochen Computertechnik innerhalb von nur einer Sekunde ermittelt werden konnten. Möglich wurde dies, indem in erster Linie Wörterlisten und deren Variationen (z.B. Umkehrungen der Wörter, Änderung der Groß- und Kleinschreibung usw.) durchprobiert wurden.

PGP erlaubt es, eine beliebig lange Passphrase zu wählen, die z.B. aus einem ganzen Satz bestehen kann. Aber auch eine solch lange Passphrase ist nicht zu empfehlen, da die langwierige Eingabe umständlich ist und sich hier schnell ein Tippfehler einschleicht. Folgende Empfehlungen für die Gestaltung des Mantras sind daher hilfreich:

Eine einfache, aber effektive Strategie verfolgt z.B. der Internet-Provider AOL bei der Vergabe des Registrierungspasswortes. Dieses besteht aus zwei voneinander unabhängigen Wörtern, die durch einen Bindestrich

---

[96] Vgl. Alexandra und Hubert Weikert, Kryptographie mit dem Computer, 1997, S. 25.

[97] beschrieben in William Stallings, Datensicherheit mit PGP, 1995, S. 247.

voneinander getrennt sind. Diese Methode kann auch auf ein Mantra angewendet werden, Beispiel: **Wort-Becher**

A. und H. Weikert[98] empfehlen folgende Vorgehensweise:

„Nehmen Sie z.B. von Ihrem Lieblingsschlager jeweils den ersten Buchstaben eines jeden Wortes:
»**Am Sonntag will mein Süßer mit mir segeln gehen**« ergibt: »**ASwmSmmSg**«.
Ist der Titel nicht so lang, daß die Anfangsbuchstaben ein entsprechend langes Mantra ergeben, kann man auch die ersten zwei Buchstaben verwenden:
»**Veronika der Lenz ist da**« ergibt: »**VedeLeisda**«.
Natürlich kann auch aus dem Lieblingsfilm
»**2001 Odysee im Weltraum**« das Mantra »**2001OdimWr**« werden,
oder eine Vorliebe »**Erdbeereis mit Sahne und Schokosoße**« wird zu »**ErdSahSchok**«."

Andere Angaben zur Gestaltung eines Passwortes, wie z.B. das von Stallings[99] beschriebene Ergebnis einer Untersuchung von A. Alvare, geben über die beschriebenen Strategien hinaus bestimmte Umwandlungstechniken als Empfehlung zur Gestaltung des Mantras, die in der folgenden Tabelle zusammengefasst wurden:

---

98 Alexandra und Hubert Weikert, Kryptographie mit dem Computer, 1997, S. 25.

99 Vgl. William Stallings, Datensicherheit mit PGP, 1995, S. 250.

Transformation	**Beispielausdruck**	**Mantra**
Transliteration	Kryptographie	crübdografi
Verflechtung von Zeichen in aufeinanderfolgenden Worten	Blei Mine	BMlienie
Ersetzen des Anfangsbuchstabens	Ausländer	Busländer
Ersetzung der Buchstaben durch Dezimalziffern	Abakus	121112119
Verschiebung von der Normalposition der Tastatur	Computer	Xinozrwe
Ersetzung durch Synonyme	Butterkuchen	Margarinetorte
Ersetzung durch Antonyme	Weihnachtsmann	Osterfrau
Direkte Übersetzung	Floppy disk	Weichscheibe
Wiederholung	Bein	BeinBein
Bildliche Manipulation (Drehung der Buchstaben)	Rucksack	Suckrack
Betätigung der Umschalttaste	10.12.1492	!=:!“:!$)“
Ersetzung der Dezimalzahl durch ihren Anfangsbuchstaben (z.B. 1 = **e**ins, 2 = ***z***)	10.12.1492	enezevnz

Tabelle 1: Strategien zur Auswahl des Mantras

Darüber hinaus empfiehlt es sich, das Mantra regelmäßig zu ändern, z.B. monatlich. Grundsätzlich gilt: Das Mantra darf grundsätzlich niemals aufgeschrieben werden. Als Vorsorge für den Fall, das Mantra vergessen zu haben, empfehlen A. und H. Weikert folgende Maßnahmen:[100]

Der Anwender kopiert den geheimen Schlüssel auf eine Diskette und schützt ihn mit einem **anderen** Mantra. Das **neue** Mantra wird auf einem Zettel notiert und in einem Umschlag verschlossen. Die Diskette verschließt man in einem zweiten Umschlag und steckt beide Umschläge in einen weiteren Umschlag. Dieser Umschlag wird versiegelt und sollte an einem sicheren Ort, wie z.B. in einem Bankschließfach deponiert werden, aber keinesfalls zu Hause oder am Arbeitsplatz. Wenn der Anwender nun sein Mantra vergessen sollte, so kann er den geheimen Schlüssel wieder von der Diskette auf den Rechner spielen und das Mantra aus dem Umschlag verwenden. Er spart sich somit eine Neugenerierung und den Widerruf seines Schlüsselpaares.

[100] Vgl. Alexandra und Hubert Weikert, Kryptographie mit dem Computer, 1997, S. 36.

Die einzelnen unversehrten Umschläge geben ihm die Gewähr, dass weder das Mantra noch die Diskette von einem Zweiten eingesehen wurden.

5.3 Virenschutz

Aufgrund der Möglichkeit, mit PGP ganze Dateien zu verschlüsseln, kommt dem Virenschutz ein besonderer Aspekt zu. Wie auch in einer normalen Datei, kann ein Virus in einer verschlüsselten Datei versteckt sein und als Attachment einer E-Mail in das Netzwerk der Organisation eingeschleust werden. Gegenüber dem Virenbefall einer unverschlüsselten Datei ist dies im Falle einer verschlüsselten Datei insofern problematischer, als dass Antivirus-Software in verschlüsselten Dateien keine Viren aufspüren kann.[101] Jede empfangene verschlüsselte Datei ist daher vor der Prüfung auf Virenbefall zunächst zu entschlüsseln.

In Netzwerken reicht es somit nicht mehr aus, Antivirus-Software nur an zentraler Stelle, z.B. auf dem Mail-Server arbeiten zu lassen, weil verschlüsselte Dateien dort nicht mit dem Schlüssel des Empfängers dechiffriert und deshalb nicht geprüft werden können. Die Konsequenz aus diesem fiktiven Fall ist, auf jedem Client, auf dem PGP eingerichtet wurde, ebenfalls eine Antivirus-Software zu installieren.

Ein weiterer, denkbarer Fall wäre ein Virus, das den auf der Festplatte gespeicherten privaten Schlüssel des Anwenders kopiert und an einen Angreifer schickt, der somit die für den Anwender chiffrierte Mail lesen könnte.[102] Da der private Schlüssel jedoch in chiffrierter Form, durch das Mantra geschützt, gespeichert wird, ist auch in diesem Fall ein starkes Mantra der beste Schutz gegen ein solches Virus.

5.4 Rechtskraft der digitalen Signatur

Es stellt sich nun die Frage, inwieweit die digitale Signatur PGPs die gewöhnliche, papiergebundene Unterschrift in der Praxis ersetzen kann. Ihre gesetzliche Regelung erhielt die digitale Signatur mit dem Gesetz zur digitalen Signatur (Signaturgesetz, SigG), das als Artikel 3 des Informations- und Kommunikationsdienste-Gesetzes (IuKDG) am 1. August 1997 in Kraft getreten ist und die Rahmenbedingungen für rechtskräftige digitale Signaturen beinhaltet. Das Gesetz versteht unter einer digitalen Signatur

---

[101] Schriftliche Auskunft von Lorenzo Zarranz, Ansprechpartner der Firma Network Associates für PGP, vom 04.12.1998.

[102] Die Existenz eines solchen Virus wurde beschrieben in: PC-Welt-News vom 09.02.1999.

jene Form der Unterschrift, wie sie auch von PGP her bekannt ist: Eine Signatur, die auf asymmetrische Verschlüsselungsverfahren beruht und deren Aufgabe die Authentifikation des Verfassers sowie die Gewährleistung der Integrität des Dokumentes ist.[103]

Mit dem SigG wurde ein Rahmen geschaffen, mit dem digital signierte Dokumente Beweiskraft vor Gericht erlangen. Allerdings wurde die digitale Signatur nicht der gesetzlichen Schriftform nach § 126 BGB gleichgestellt.[104] Dies bedeutet, dass digital signierte Dokumente nur dort gleichwertig zu manuell unterschriebenen Papierdokumenten sind, wo die gewillkürte Schriftform erlaubt ist, wie z.B. bei den üblichen Handelsdokumenten. Wo ein Gesetz jedoch ausdrücklich die Schriftform vorschreibt, sind elektronische Dokumente bis auf einige, im jeweiligen Gesetz genannte Ausnahmen noch nicht als Urkunde anerkannt.[105]

Zum aktuellen Zeitpunkt ist es aber in erster Linie aus zwei Gründen noch gar nicht möglich, eine gemäß Signaturgesetz rechtskräftige Signatur mit PGP zu erzeugen:

1. Das Signaturgesetz geht von einer Infrastruktur (Public Key Infrastruktur) zur Zertifizierung öffentlicher Schlüssel aus. **Diese Infrastruktur befindet sich momentan im Aufbau und besteht deshalb faktisch noch gar nicht.**

   Als wesentliches Element dieser Infrastruktur sind im SigG Zertifizierungsstellen vorgesehen, die zur Ausgabe von **signaturgesetzkonformen** *Zertifikaten* eine Genehmigung von der Regulierungsbehörde Telekommunikation und Post (RegTP) benötigen (§4 SigG).

   Die Regulierungsbehörde selbst hat erst im November 1998 ihre Arbeit aufgenommen[106] und eine Genehmigung wurde bislang erst einmal, an die Fachgruppe „Telesec“ der Telekom, erteilt.[107] Die Telesec bietet allerdings keine Zertifizierungen für PGP-Schlüssel, sondern lediglich für Signaturschlüssel i.V.m. einer Software der Deutschen Telekom AG an.

---

[103] Vgl. Wolf-Christian Hingst in Internet Professional 10/97, URL: http://zdnet.de/internet/artikel/tech/9710-/disig.wc.htm.

[104] Vgl. Wolfgang Kopp, Rechtsfragen der Kryptographie und der digitalen Signatur, 1998, Kapitel C, Nr. I.1.b

[105] Vgl. Jürgen Gulbins in einem Aufsatz zum SigG in: Richard E. Smith, Internet-Kryptographie, 1998, S. 332

[106] Lt. einer schriftlichen Auskunft von Stephanie Willemsen vom 18.12.1998.

[107] Vgl. Focus Nachrichtenmagazin, Ausgabe 1 v. 04. 01.1999, S. 109.

Das Problem der fehlenden Infrastruktur betrifft selbstverständlich nicht nur PGP, sondern auch andere Verschlüsselungssoftware für E-Mail. Folglich wird es noch einige Zeit dauern, bis gemäß Signaturgesetz zertifizierte Schlüssel ihre Verbreitung finden.

2. PGP unterstützt nicht die Speicherung privater Schlüssel auf Chipkarten.

   §17 Abs. 1 der Signaturverordnung (SigV) verlangt i.V.m § 14 Abs. 4 SigG eine technische Komponente zur Speicherung des privaten Schlüssels des Anwenders mit einem Sicherheitsstandard, der momentan nur durch eine Hardwarekomponente, wie z.B. einer PIN-gesicherten Chipkarte, erfüllt wird.[108] D.h. selbst wenn eine Zertifizierungsstelle PGP-Schlüssel gemäß Signaturgesetz zertifizieren möchte, so ist dies technisch noch gar nicht möglich.[109]

Bevor mit PGP signaturgesetzkonforme Signaturen geleistet werden können, muss die Software hinsichtlich dieses Gesetzes umgeschrieben werden – und es ist fraglich, ob dies in naher Zukunft geschieht. Schließlich ist PGP kein deutsches Produkt, sondern ein für den internationalen Markt geschriebenes Programm. Dabei wären die angesprochenen Änderungen der Software überschaubar, denn in Bezug auf die Mindestanforderungen an die kryptographischen Algorithmen erfüllt PGP die Anforderungen des Signaturgesetzes bereits.[110]

Es ist allerdings festzustellen, dass das Signaturgesetz noch experimentellen Charakter besitzt. Insbesondere aufgrund der hohen technischen Anforderungen bleibt abzuwarten, inwieweit die Möglichkeiten der signaturgesetzkonformen Unterschrift überhaupt angenommen werden.[111] Bereits jetzt zeichnet sich ab, dass nicht alle Anwender Wert auf ein signaturgesetzkonformes Zertifikat legen – ein Umstand, der dadurch belegt wird, dass Zertifizierungsstellen wie z.B. TC Trustcenter[112] Zertifizierungen verschiedener Sicherheitsstufen anbieten, u.a. auch für PGP-Schlüssel. Es ist gut möglich, dass Gerichte bereits diese nicht signaturgesetzkonformen Zertifizierungen im Rahmen der freien Beweiswürdigung als Beweismittel

---

[108] Vgl. Jürgen Gulbins in einem Aufsatz zum SigG in: Richard E. Smith, Internet-Kryptographie, 1998, S. 338

[109] Lt. einer schriftlichen Auskunft von Melanie Nuesse vom 16.12.1998.

[110] Vgl. Bekanntmachung zur digitalen Signatur nach Signaturgesetz und Signaturverordnung vom 09.02.98 im Bundesanzeiger Nr. 31 v. 14.02.98.

[111] Lt. einer schriftlichen Auskunft von Stephanie Willemsen vom 21.12.1998.

[112] Http://www.trustcenter.de

für eine rechtskräftige Unterschrift anerkennen[113] – sicher ist dies jedoch nicht.

Aufgrund der beschriebenen Rechtsunsicherheit bleibt daher momentan festzuhalten, **dass sich eine digitale Signatur mit PGP vorerst nicht dazu eignet, um rechtssichere Verträge über E-Mail abzuschließen.** Hier ist neben Gesetzgebung und Rechtsprechung insbesondere die weitere Entwicklung der Software abzuwarten.

In allen anderen Fällen, in denen der Absender authentifiziert und die Integrität der Nachricht kontrolliert werden soll, auf die Rechtskraft der Signatur aber verzichtet werden kann, ist die Signatur ein sehr sinnvolles Instrument. Abgesehen von einem beabsichtigten Vertragsabschluss gilt dieser Fall letztendlich für jede Nachricht. Daher spricht nichts dagegen, die digitale Signatur auf jede E-Mail anzuwenden.

Abschließend ist an dieser Stelle noch in kurzer Form anzumerken, dass die Uhrzeit der PGP-Signatur nur eingeschränkte Verlässlichkeit bietet, denn sie richtig sich nach der Systemzeit des Rechners und diese ist z.B. bei Windows sehr einfach zu manipulieren. §9 SigG sieht daher einen manipulationssicheren Zeitstempeldienst als eine Dienstleistung der Zertifizierungsstellen vor. Für PGP ist allerdings noch kein signaturgesetzkonformer Dienst verfügbar. Anwender, die ihre Nachrichten trotzdem mit einem (nicht signaturgesetzkonformen) *Zeitstempel* versehen möchten, finden eine Adresse im Anhang auf Seite 109.

5.5 Anwendung der Verschlüsselung

Wie auch beim Einsatz der Signatur, so wird sich der Anwender bei der Verschlüsselung fragen, auf welche Nachrichten sie angewendet werden soll und wo auf eine Verschlüsselung verzichtet werden kann. Schröder zeigt in einem Diskussionspapier der Universität Münster[114], dass es nur für einen Bruchteil der jeden Tag übermittelten Nachrichten sinnvoll ist, sie zu verschlüsseln. Insbesondere ist eine Verschlüsselung nur selten bei Nachrichten notwendig, die

- sehr personenspezifisch sind, also lediglich für Sender und Empfänger, aber nicht für Außenstehende einen Wert besitzen, oder

---

[113] Vgl. c't, Heft 8, 1998, S. 113

[114] Vgl. Guido Schröder, Kryptographie – Schlüssel zur Informationsgesellschaft, 1997, S. 12f.

- an eine bestimmte Situation gebunden sind und ein zeitliches „Verfallsdatum“ haben.

Andererseits gibt er zu bedenken, dass nicht allein schon der Akt der Verschlüsselung einen Rückschluss auf die Wichtigkeit des Nachrichteninhaltes zulassen darf, indem unwichtige Nachrichten nie verschlüsselt, wichtige Nachrichten jedoch immer verschlüsselt werden. Folglich müsste nun doch jede Nachricht verschlüsselt werden.

Im betrieblichen Alltag wird sich jedoch die Forderung nach Verschlüsselung jeder E-Mail kaum durchsetzen lassen. Zum einen stellt sich die Frage der Kontrolle einer solchen Sicherheitsrichtlinie,[115] zum anderen ist PGP noch nicht flächendeckend verbreitet, so dass eine verschlüsselte Kommunikation mit externen Kommunikationspartnern oftmals gar nicht möglich ist.

Letztendlich kann eine Empfehlung nur lauten, die Mitarbeiter eines Unternehmens eindringlich über die Sicherheitsrisiken aufzuklären, die beim Versenden von E-Mail laut Kapitel 2.2 bestehen. Als Folge sollte die Verschlüsselung nach der Einführung PGPs zur betrieblichen Praxis gehören, also zum Regelfall und nicht zur Ausnahme der Kommunikation per E-Mail werden. **In den Fällen, in denen eine verschlüsselte Kommunikation per E-Mail nicht möglich ist, sollten vertrauliche Daten keinesfalls per E-Mail, sondern weiterhin mit der konventionellen Post verschickt werden.**

In diesem Zusammenhang sollten auch Kunden des Unternehmens für die Sicherheitsrisiken der E-Mail-Kommunikation sensibilisiert werden. Dabei kann darauf hingewiesen werden, dass aus diesem Grunde für die geschäftliche Kommunikation per E-Mail zur Verschlüsselung mit PGP geraten wird. Dies hätte eine weitere Verbreitung des Programms zur Folge und könnte auf lange Sicht die Verschlüsselung von E-Mails für eine breite Anwenderschicht selbstverständlich machen.

---

[115] Network Associates bietet als Erweiterung des PGP Softwarepaketes den „PGP Policy Management Agent“ an, mit dem eine frei bestimmbare unternehmensinterne Sicherheitsrichtlinie, wie z.B. die oben beschriebene, kontrolliert werden kann.

6 Zusammenfassung und Schlussbetrachtung

Eine E-Mail ist im Internet den drei Angriffsformen Datenspionage, Datenmanipulation und Datenfälschung ausgesetzt, wodurch sich unverschlüsselte E-Mails für eine geschäftliche Kommunikation disqualifizieren.

Vor dem Hintergrund dieser Angriffsformen wurden drei Punkte als Sicherheitsziele genannt. Durch den Einsatz eines Public-Key-Verschlüsselungsverfahrens soll

1. die Vertraulichkeit der Nachrichten gewährleistet,
2. die Integrität der Nachrichten überprüft und
3. die Authentifikation des Absenders ermöglicht

werden. Die letzten beiden Punkte entsprechen der Forderung nach einer digitalen Signatur und dies kann die Anwendungsmöglichkeit der E-Mail in erheblichem Maße ausdehnen. So sind z.B. Vertragsabschlüsse per E-Mail denkbar.

Grundsätzlich lassen sich mit PGP alle drei Ziele erreichen. Die verwendeten kryptographischen Algorithmen bieten eine zur Zeit mehr als ausreichende Sicherheit vor kryptoanalytischen Attacken. Die Verschlüsselungsfunktion ermöglicht ein höchstes Maß an Vertraulichkeit in der Kommunikation per E-Mail, so dass sich PGP geradezu für die kommerzielle Nutzung empfiehlt. Auch die Signaturfunktion des Programms profitiert von den starken kryptographischen Algorithmen, wodurch sich die Absenderangaben und die Datenintegrität einer E-Mail zweifelsfrei überprüfen lassen.

Doch das Erreichen der drei genannten Sicherheitsziele hängt weniger von dem Verschlüsselungsprogramm PGP als von der korrekten Handhabung des Programmes ab. Besonders kritisch würde sich z.B. die Kompromittierung des geheimen privaten Schlüssel auswirken, denn der private Schlüssel dient sowohl zur Entschlüsselung als auch zur Signatur. Die Vorkehrungen zum Schutz des privaten Schlüssels sind daher äußerst genau einzuhalten.

Dieser Umstand drückt sich auch in dem Signaturgesetz aus, das die Rahmenbedingungen für rechtskräftige digitale Signaturen regelt. Das Gesetz verlangt die Speicherung des privaten Schlüssels auf einer Chipkarte, doch dies ist bei PGP noch nicht möglich. Dies hat zur Folge, dass eine PGP-Signatur keine Rechtskraft gemäß Signaturgesetz besitzt. Die Idee des

rechtssicheren Vertragsabschlusses per E-Mail hat sich damit vorerst erübrigt.

Doch es bleibt abzuwarten, inwieweit sich das Signaturgesetz und mit ihm die strengen Vorschriften der digitalen Signatur durchsetzen werden. Ebenso ist die Entwicklung PGPs im Hinblick auf die Anforderungen des Signaturgesetzes abzuwarten.

Ohnehin befinden sich Unternehmen, die PGP in ihre Kommunikationsstruktur einbinden, in einer Vorreiterrolle. Eine allgemeine Sensibilisierung für die Sicherheitsrisiken einer Kommunikation per E-Mail findet gerade erst statt, und so befindet sich auch die Nutzung von Verschlüsselungssoftware erst am Anfang. Es wird sicherlich noch einige Zeit dauern, bis eine breite Anwenderschicht Verschlüsselungssoftware benutzen wird, doch die Wahrscheinlichkeit ist groß, dass dies bei E-Mails mit PGP geschehen wird. PGP ist der De-facto-Standard bei der Verschlüsselung – ein Argument, dass bei der Frage, in welches Verschlüsselungssystem ein Unternehmen investieren soll, auch in Zukunft der ausschlaggebende Punkt sein wird.

7 Anhang

A Anlagen

A.1 Beschreibung eines symmetrischen Verschlüsselungsalgorithmus am Beispiel IDEA

IDEA ist ein blockorientierter, symmetrischer Verschlüsselungsalgorithmus, der von Xuejia Lai und James Massey im Jahre 1990 entwickelt wurde. Mit einem 128 Bit langen Schlüssel werden Daten in Blöcken von je 64 Bit verschlüsselt. Jeder Datenblock wird in 8 Durchläufen (Iterationen), gefolgt von einer abschließenden Transformationsfunktion, verändert.

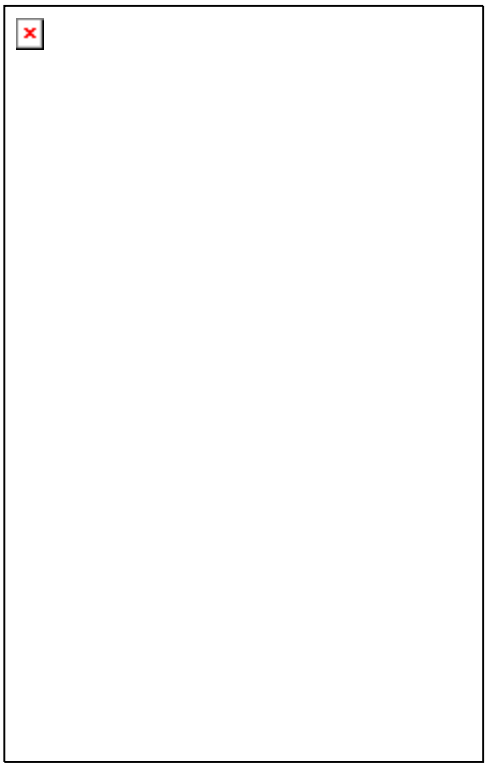


Abbildung 70: Funktionsweise des IDEA-Algorithmus[116]

Die 64 Eingabebits werden durch den Algorithmus zunächst in vier 16 Bit lange Teilblöcke (K_i) aufgeteilt. In jedem folgenden Iterationsdurchlauf werden die vier 16 Bit Blöcke bearbeitet und vier neue 16 Bit Ausgabeblöcke (T_i) erzeugt. Die letzten vier 16 Bit Datenblöcke werden abschließend transformiert und zum 64 Bit langen Chiffreblock (VT_i) zusammengefügt. In jeder Iteration werde sechs der 16 Bit langen Teilschlüssel gebraucht, die abschließende Transformation benutzt vier 16 Bit Teilschlüssel. Insgesamt werden somit 52 Teilschlüssel verwendet, die alle aus dem 128 Bit langen ursprünglichen Schlüssel erzeugt werden.

Der IDEA-Algorithmus verwendet in jeder Iteration drei verschiedene mathematische Operationen, durch die aus jeweils zwei 16 Bit langen Eingabeblöcken ein 16 Bit Ausgabeblock gebildet wird. Die Operationen sind laut Weikert:[117]

---

[116] Abb. aus: Alexandra und Hubert Weikert, Kryptographie mit dem Computer, 1997, S. 17.

[117] Alexandra und Hubert Weikert, Kryptographie mit dem Computer, 1997, S. 17.

- Bitweise exklusives ODER
- Addition zweier ganzer Zahlen modulo 2^{16} (=65536), die man als vorzeichenlose ganze Zahl behandelt, ebenso wie das Ergebnis. D.h. die Funkton addiert zwei 16 Bit-Zahlen und gibt eine 16 Bit-Zahl aus. Der Überlauf im 17. Bit bleibt unbeachtet.
- Multiplikation zweier Zahlen modulo $2^{16} + 1$ (=65537), wobei die Multiplikation als vorzeichenlose 16 Bit-Zahlen behandelt werden. Die einzige Ausnahme ist die Folge von 16 Nullen, die 2^{16} repräsentiert.

A.2 Erzeugung eines Schlüsselpaares am Beispiel des RSA-Algorithmus

Die Schlüssel des Beispiels zur RSA-Verschlüsselung auf Seite 36 wurden wie folgt erzeugt:[118]

1. Wähle zufällig zwei Primzahlen, hier **p** = 7 und **q** = 17
2. Berechne **n** = **p** * **q** = 7 * 17 = 119
3. Berechne ⇔**(n)** = **(p - 1)*(q - 1**) = 96
4. Wähle **e** so, dass **e** und ⇔**(n)** keinen gemeinsamen Teiler außer 1 besitzen: **e** = 5 τ ggT(96,5) = 1
5. Bestimme **d** derart, dass **d** * **e** = 1 mod ⇔**(n)** und **d** < ⇔**(n)**.
   τ **d** * 5 = 1 mod 96 und **d** < 96
   τ **d** = 77, da 77 * 5 = 385 = 4 * 96 + 1

Der öffentliche Schlüssel ist (**e,n**) = (5,119), der geheime Schlüssel (**d,n**) = (77,119).

Die Verschlüsselungsfunktion lautet: $C = M^{\mathbf{e}} \pmod{\mathbf{n}}$

Die Entschlüsselungsfunktion lautet: $M = C^{\mathbf{d}} \pmod{\mathbf{n}}$,

wobei M = Ausgangstext[119] < **n** , C = chiffrierter Text

A.3 Beschreibung einer Hashfunktion am Beispiel des MD5-Algorithmus

Der MD5-Algorithmus erzeugt aus einem beliebig langen Eingabetext einen 128 Bit Ausgabeblock, den Message Digest. Die Berechnungen können in fünf Schritten dargestellt werden:[120]

---

[118] William Stallings, Sicherheit im Datennetz, 1995, S. 163.

[119] Ist M > n so wird M in Blöcke von Länge log2(n) Bit aufgeteilt.

[120] Vgl. William Stallings, Sicherheit im Datennetz, 1995, S. 335ff und William Stallings, Datensicherheit mit PGP, 1995, S. 242f.

- **Schritt 1: Zufügen von Füllbits**
  Zunächst wird der Eingabetext mit entsprechend vielen Bits aufgefüllt,[121] so dass die Länge der aufgefüllten Nachricht genau um 64 Bit kürzer ist als ein Vielfaches von 512. Das erste Füllbit ist eine 1, gefolgt von der entsprechenden Anzahl 0-Bits.

- **Schritt 2: Hinzufügen der Länge**
  Die fehlenden 64 Bit enthalten die Längeninformation der Originalnachricht. Dazu wird berechnet: Ursprungslänge mod 2^{64}. Das Ergebnis wird zu der Bitfolge aus Schritt 1 hinzugefügt.

  Nach den ersten beiden Schritten erhält man eine Bitfolge, deren Länge ein Vielfaches von 512 Bit ist.

- **Schritt 3: Initialisieren des MD-Speichers**
  Um Zwischen- und Endergebnis der Hashfunktion zwischenzuspeichern, wird ein 128 Bit großer Speicher verwendet, der aus vier 32-Bit-Registern besteht. Die Register werden folgendermaßen initialisiert:

  ```
  A = 01234567
  B = 89ABCDEF
  C = FEDCBA98
  D = 76543210
  ```

- **Schritt 4: Verarbeitung der Nachricht in 512-Bit-Blöcke**
  Dieser Schritt stellt die eigentliche Verarbeitung der Daten dar. Als Eingabe verwendet der Algorithmus den gerade zu berechnenden 512-Bit Block und den Wert des 128-Bit-Speichers ABCD. Diese Eingaben werden in vier Durchläufen AND-, OR-, XOR-Operationen und einer Addition modulo 2^{32} unterzogen, wobei in jedem Durchlauf der Inhalt des 128-Bit-Speichers erneuert wird. Der Inhalt des Speichers nach dem vierten Durchlauf wird wieder als Eingabe für den ersten Durchlauf mit dem folgenden 512-Bit-Block benutzt usw.

- **Schritt 5: Ausgabe**
  Nachdem der letzte 512-Bit-Block verarbeitet wurde bildet der letzte Inhalt des 128-Bit-Speichers den Message Digest der Nachricht.

[121] Es wird immer aufgefüllt, auch wenn die Nachricht schon die entsprechende Länge, z.B. 448 Bit hat. In diesem Fall werden 512 Bit aufgefüllt, so dass sie eine Länge von 960 Bit aufweist.

A.4 Verschlüsselung auf einen Blick

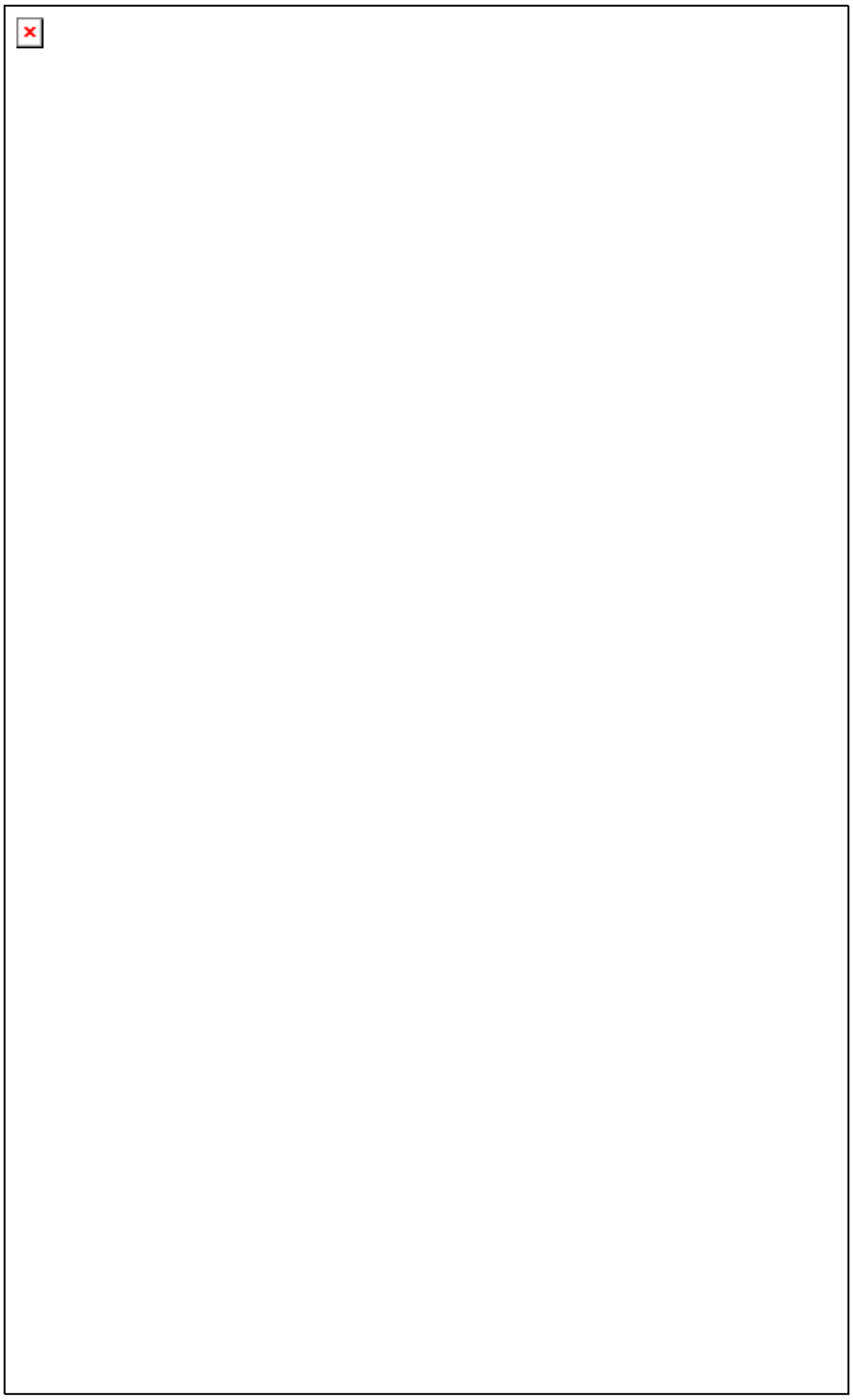


Abbildung 71: Verschlüsselung mit PGP auf einen Blick[122]

[122] Übersicht zusammengefügt aus Abbildungen aus: Network Associates, Dokumentation zu PGP 6.0 Freeware, Intro to Crypto, Oktober 1998, S. 16, 17, 20.

A.5 Verzeichnis von Key Servern

Hier sind Key Server aufgeführt, die über die Key-Server-Schnittstelle des Moduls PGPkeys erreicht werden können.[123] Die folgende Tabelle gibt die notwendigen Daten an, die zur Einrichtung eines neuen Key Servers erforderlich sind, vergleiche Abbildung 72.

Bis auf den Key Server des TC Trustcenter bilden die aufgeführten Key Server ein Netzwerk, in dem von den Servern die Schlüssel untereinander ausgetauscht und ständig aktualisiert werden. Diese Key Server eignen sich zum Aufbau einer internen Public Key Infrastruktur im Sinne von Kapitel 5.1.3. Der Key Server des Zertifizierungsstelle TC Trustcenter hingegen stellt nur Schlüssel zur Verfügung, die von der Zertifizierungsstelle zertifiziert wurden.

E-Mail Domain (oder Name)	**HTTP**	**LDAP**	**Adresse des Servers**
mit.edu	x		Http://pgpkeys.mit.edu:11371
pgp.com		x	Ldap://certserver.pgp.com
pgp.net	x		Http://wwwkeys.pgp.net:11371
pgp.net	x		Http://wwwkeys.ch.pgp.net:11371
pgp.net	x		Http://wwwkeys.cz.pgp.net:11371
pgp.net	x		Http://wwwkeys.dk.pgp.net:11371
pgp.net	x		Http://wwwkeys.de.pgp.net:11371
pgp.net	x		Http://wwwkeys.es.pgp.net:11371
pgp.net	x		Http://wwwkeys.nl.pgp.net:11371
pgp.net	x		Http://wwwkeys.uk.pgp.net:11371
TC Trustcenter	x		Http://www.trustcenter.de:11371

Tabelle 2: Übersicht verschiedener Key Server

In die unten abgebildete Maske zur Einrichtung eines neuen Key Servers gelangt der Anwender durch Klick auf das Icon des PGPtray in der Taskleiste...Auswahl des Punktes PGP PREFERENCES...Auswahl des Registers SERVERS...und Klick auf die Schaltfläche NEW.

[123] Auf eine Aufzählung von Key Servern, die per E-Mail, ftp oder WWW erreicht werden können, wurde verzichtet.

Abbildung 72: Hinzufügen eines neuen Key Servers

A.6 Verzeichnis von Trustcentern

Nachfolgend sind die WWW-Adressen einiger **Trustcenter** aufgeführt, die PGP-Schlüssel zertifizieren. Die Zertifizierung unterliegt je nach Trustcenter verschiedenen Richtlinien und Verfahrensweisen, die aber bei jedem Anbieter ausführlich und zu genüge erläutert werden, wodurch sich hier eine nähere Darstellung erübrigt.

- **http://www.trustcenter.de**

  Die Firma TC Trustcenter unterscheidet PGP-Zertifikate für private und geschäftliche Zwecke. Private Zertifizierungen sind in 3 Klassen erhältlich und kostenlos. Geschäftliche Zertifikate werden in 2 Klassen gegen eine Jahresgebühr sowie eine einmalige Bearbeitungsgebühr vergeben.

- **http://www.in-ca.individual.net**

  Unter dieser Adresse ist eine Vielzahl regionaler Zertifizierungsstellen zu finden, die sich unter dem Namen Individual Network e.V. zusammengeschlossen haben. Die Zertifizierung erfolgt kostenlos, es gibt keine gesonderten Zertifikate für geschäftliche Zwecke.

- **http://www.cert.dfn.de/dfnpca/certify/**

  Zertifizierungsstelle des deutsches Forschungsnetzes. Zertifizierungen sind für private Anwender kostenlos, für gewerblich genutzte Schlüssel kostenpflichtig.

- **http://www.heise.de/ct/pgpCA/**

  Der Heise-Verlag (Zeitschrift c't) zertifiziert kostenlos PGP-Schlüssel, zwischen gewerblich und privat genutzten Schlüsseln wird nicht unterschieden.

A.7 Zeitstempeldienste

- **http://www.itconsult.co.uk/stamper.htm**

  Hier findet sich eine Anleitung zu einem kostenlosen Zeitstempeldienst von Matthew Richardson.

  Das Prinzip: An seine E-Mail-Adresse eingehende Nachrichten werden mit einer gewöhnlichen PGP-Signatur versehen, die standardmäßig eine Zeitangabe enthält. Jeder Nachricht wird darüber hinaus durch einen Signaturzähler eine eindeutige Referenznummer zugewiesen. Anschließend wird die signierte Nachricht an den Absender zurückgeschickt.

  Durch tägliche öffentliche Protokollierung der Referenznummern und abgetrennten Signaturen wird die Echtheit der Zeitstempel bekundet, so dass sie kontrolliert werden können.[124]

- **http://www.timesafe.de**

  Informationen zu einem patentierten Zeitstempelverfahren[125] der Firma TimeSafe TrustCenter GmbH, Nürnberg, das den Anforderungen des Maßnahmenkataloges zum SigG entspricht und daher in Zukunft zum Einsatz kommen könnte.

---

[124] Vgl. c't, Heft 8, 1998, S. 116.

[125] Patentschrift DE 19532617

B Abkürzungsverzeichnis

ADK	Additional Decryption Key
AOL	American Online
ARPA	Advanced Research Projects Agency
bzgl.	bezüglich
CA	Certificate Authority
CAST	Algorithmus nach Carlisle Adams und Stafford Tavares
CFB	Cipher-Feedback-Modus
CSK	Corporate Signing Key
d.h.	das heißt
Def.	Definition
DES	Data Encryption Standard
DH	Algorithmus nach Diffie und Hellman
DSS	Digital Signature Standard
evtl.	eventuell
f	folgende [Seite]
ff	folgende [Seiten]
ftp	file transfer protocol
HR	Handelsregister
i.Allg.	im Allgemeinen
i.d.R.	in der Regel
i.V.m.	in Verbindung mit
IADK	Incoming Additional Decryption Key
IDEA	International Data Encryption Algorithm

IMP	Interface Message Processor
IP	Internet Protocol
IuKDG	Informations- und Kommunikationsdienste-Gesetz
LAN	Local Area Network
lt.	laut
MD5	Message Digest 5
MIME	Multipurpose Internet Mail Extensions
MRK	Message Recovery Key
NCP	Network Control Protocol
OADK	Outgoing Additional Decryption Key
PCA	Public Certification Authority
PGP	Pretty Good Privacy
PIN	Persönliche Identifikationsnummer
POP	Post Office Protocol
RegTP	Regulierungsbehörde Telekommunikation und Post
RSA	Algorithmus nach Rivest, Shamir und Adleman
S.	Seite
SHA-1	Secure Hash Algorithm 1
SigG	Signaturgesetz
SigV	Signaturverordnung
SMTP	Simple Mail Transfer Protocol
sog.	so genannt
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol

u.a.	unter anderem
u.U.	unter Umständen
usf.	und so fort
usw.	und so weiter
vgl.	vergleiche
WWW	World Wide Web
z.B.	zum Beispiel
z.Zt.	zur Zeit
Zw.sp.	Zwischenspeicher

C Abbildungsverzeichnis

D Tabellenverzeichnis

E Literaturverzeichnis

Bauer, Friedrich L.

Kryptologie: Methoden und Maximen – Berlin, Heidelberg: Springer-Verlag, 2. Auflage, 1994

Beutelspacher, Albrecht

Kryptologie: Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen – Braunschweig, Wiesbaden: Friedr. Vieweg & Sohn Verl.-Ges., 3. Auflage, 1993

Beutelspacher, Albrecht

Referat in: Hamm, Rainer; Möller, Klaus Peter (Hrsg.): Datenschutz durch Kryptographie: ein Sicherheitsrisiko? Forum Datenschutz; Bd. 6 – Baden-Baden: Nomos Verl.-Ges., 1. Auflage, 1998, Seite 16 ff

Christophers, Jens; Nonhoff, Jürgen (Hrsg.)

Going online = going public: Ein Leitfaden für das Internet als Medium der Geschäftspolitik – Münster: LIT, 1997

Diffie, Whitfield;. Hellman Martin E.

New Directions in Cryptography, in: IEEE Transactions on Information Theory 1976, Vol. IT-22, S. 644 - 654

Gabler Wirtschafts-Lexikon

Elektronische Ausgabe auf CD-ROM – Wiesbaden: Betriebswirtschaftler Verlag Dr. Th. Gabler GmbH, 1993

Garfinkel, Simson

PGP: Pretty Good Privacy: Verschlüsselung von E-Mail – Bonn: O'Reilly / International Thomson Verlag, 1. Auflage, 1996

Hagemann, Hagen u.a.

Kryptologie – Interaktives Training; Technischer Datenschutz in Kommunikationsnetzen, CD-ROM mit Handbuch – Bonn: Addison-Wesley-Longman, 1997

Lienemann, Gerhard

TCP/IP-Grundlagen; Protokolle und Routing – Hannover: Heise, 1996

Network Associates

PGP for Business Security, Windows User's Guide Version 5.5v, September 1997, (Online-Dokumentation)

Network Associates

PGP Security Officer's Guide Version 5.5, September 1997, (Online-Dokumentation)

Network Associates

Dokumentation zu PGP 6.0 Freeware, Intro to Crypto, Oktober 1998, (Online-Dokumentation)

Nusser, Stefan

Sicherheitskonzepte im WWW – Berlin, Heidelberg: Springer, 1998

Reiser, Christian

Internet – die Sicherheitsfragen: Antworten für Manager und Techniker – Wien: Ueberreuter, 1998

Scheller, Martin u.a.

Internet: Werkzeuge und Dienste; von „Archie“ bis „World Wide Web“ – Berlin, Heidelberg: Springer, 1994

Schneier, Bruce

Angewandte Kryptographie: Protokolle, Algorithmen und Sourcecode in C – Bonn u.a.: Addison-Wesley, 1. Auflage, 1996

Schröder, Guido

Kryptographie – Schlüssel zur Informationsgesellschaft? Verschlüsselungstechnik zwischen Wettbewerb und Marktversagen; Diskussionspapier Nr. 6 des Instituts für Verkehrswissenschaft an der Universität Münster, 1997

Smith, Richard E.

Internet-Kryptographie – Bonn u.a.: Addison-Wesley-Longman, 1998

Stallings, William

Datensicherheit mit PGP – München u.a.: Prentice-Hall-Verlag, 1995

Stallings, William

Sicherheit in Netzwerk und Internet – München u.a.: Prentice-Hall-Verlag, 1995

Weikert, Alexandra; Weikert, Hubert

Kryptographie mit dem Computer: Verschlüsselungspraxis mit dem PC – München: Pflaum 1997

Wobst, Reinhard

Abenteuer Kryptologie: Methoden, Risiken und Nutzen der Datenverschlüsselung – Bonn u.a.: Addison-Wesley-Longman, 1998

Sonstige Quellen

Network Associates, Infoblatt zu PGP for Business Security 5.5

Utech Verlag, Datenschutz CD „Hacker's Best Friend", Version IV, 1. Auflage, 1998

Zeitschriften

C't, Heft 8, 1998, Seite 112 – 116

DOS, Ausgabe April 04/1997, Seite 228 – 262

Focus Nachrichtenmagazin, Ausgabe 1/1999, Seite 108 – 110, Artikel von Jochen Wegner

Gateway, Ausgabe Mai 1998, Seite 34, Artikel von Achim Born

PC-Online, Ausgabe 10/98, Seite 52 – 55, Artikel von Michael Tischer

Internetquellen

Deutsches Forschungsnetz

Online im Internet [Stand: 04.01.1999]:
URL: http://www.cert.dfn.de/dfnpca/certify/

Deutsche Telekom AG – Telesec

Online im Internet [Stand: 04.01.1999]:
URL: http://www.telesec.de

Feisthammel, Patrick

Online im Internet[Stand: 14.12.1998]:
URL: http://www.rubin.ch/pgp/pgp.en.html

FoeBuD (Verein zur Förderung des bewegten und unbewegten Datenverkehrs) e.V. Bielefeld

PGP-Dokumentation
Online im Internet [Stand 03.11.1998]:
URL: http://www.fto.de/fthp/kirchner/pgp/buch.htm

Heise-Verlag

Online im Internet [Stand: 04.01.1999]:
URL: http://www.heise.de/ct/pgpCA/

Individual Network e.V.

Online im Internet [Stand: 04.01.1999]:
URL: http://www.in-ca.individual.net/

Internet Professional

Hingst, Wolf Christian
Abdruck des Artikels aus der Ausgabe 10/97, S. 87ff
Online im Internet [Stand: 20.12.1998]:
URL: //www.zdnet.de/internet/artikel/tech/9710/disig-wc.htm

Kirchner, Jens

Online im Internet [Stand: 12.11.1998]:
URL: http://www.fto.de/fthp/kirchner/d_index.htm

Kopp, Wolfgang

Rechtsfragen der Kryptographie und der digitalen Signatur, Seminararbeit, Ludwig-Maximilian-Universität München, Juristische Fakultät, 1998
Online im Internet [Stand 21.12.1998]
URL:http://www.stud.uni-muenchen.de/~wolfgang.kopp/krypto.html

Nuesse, Melanie

Assistentin im Bereich IT-Sicherheit der Firma Competence Center Informatik GmbH (CCI), Meppen.
Mailto: nuesse@cci.de

PC-Welt-News

Newsletter der PC-Welt.
Mailto: red-online@pcwelt.com

Raven, Kai

Deutsche Anleitung zu PGP 5.5.
Online im Internet [Stand: 29.10.1998]:
URL: http://home.kamp.net/home/kai.raven/index.html

Richardson, Matthew

Online im Internet [Stand: 14.12.1998]
URL: http://www.itconsult.co.uk/stamper.htm

Rudrich, Michael

Network Associates, München
Mailto: michael_rudrich@nai.com

Signaturgesetz

Mit Signaturverordnung, Maßnahmenkataloge zum SigG, Bekanntmachung zur digitalen Signatur nach SigG und SigV vom 09.02.1998 im Bundesanzeiger Nr. 31 vom 14.02.1998
Online im Internet [Stand: 20.12.1998]:
URL: http://www.regtp.de/fachinfo/digitale%20Signatur/start.htm

TC Tustcenter GmbH, Hamburg

Online im Internet [Stand: 21.12.1998]
URL: http://www.trustcenter.de

TimeSafe TrustCenter GmbH, Nürnberg

Online im Internet [Stand: 21.12.1998]
URL: http://www.timesafe.de

Uplawski, Michael

Deutsche Übersetzung der comp.security.pgp FAQ, Version 1.5.
Online im Internet [Stand: 14.12.1998]:
URL: http://www.iks-jena.de/mitarb/lutz/security/pgpfaq.html

Willemsen, Stephanie

Produktbeauftragte für PGP der Zertifizierungsstelle TC Trustcenter.
Mailto: willemsen@trustcenter.de

Zarranz, Lorenzo

Ansprechpartner der Firma Network Associates für PGP, „technical support Europe“.
Mailto: lorenzo_zarranz@nai.com

F Glossar

ADK

Additional Decryption Key oder auch Message Recovery Key (MRK). „Zusätzlicher Dechiffrierungsschlüssel“, mit dem (zusätzlich zum jeweiligen Empfängerschlüssel) sämtliche eingehende als auch ausgehende chiffrierte Nachrichten einer Organisation ver- und entschlüsselt werden können. Der ADK kann aufgeteilt werden in den Incoming Additional Decryption Key (IADK) für eingehende und den Outgoing Additional Decryption Key (OADK) für ausgehende E-Mails.

Analytische Attacke

Suche nach Schwachpunkten im verwendeten Algorithmus, indem z.B. der Chiffretext auf Gesetzmäßigkeiten hin untersucht wird, um schließlich den Schlüssel oder den Klartext zu ermitteln.

Angriff

In diesem Buch ist mit Angriff der Versuch gemeint, (unverschlüsselte) E-Mails zu kopieren, zu stehlen, zu verändern oder zu fälschen.

ARPA

Advanced Research Projects Agency. Eine dem amerikanischen Verteidigungsministerium unterstelle Behörde, die maßgeblich am Aufbau des Arpanets und späteren Internets beteiligt war.

Arpanet

Ein von der ARPA ins Leben gerufene Computernetz, aus dem sich schließlich das Internet entwickelte.

ASCII-Armor

In ASCII-Format umgewandelter Binärcode. Die von PGP verschlüsselten Daten liegen zunächst im Binärcode vor und werden anschließend in das ASCII-Format umgewandelt, damit sie als E-Mail versendet werden können.

Asymmetrische Verschlüsselung

Verschlüsselungsverfahren, bei dem zur Ver- und Entschlüsselung zwei unterschiedliche Schlüssel verwendet werden: Der öffentliche Schlüssel

(public key) des Empfängers dient dem Sender zur Verschlüsselung, der Empfänger kann die Nachricht nur mit seinem geheimen Schlüssel (secret key) wieder entschlüsseln.

Attacke

Versuch bzw. Durchführung einer Kryptoanalyse.

Benutzer-ID

Siehe User-ID.

Blockchiffren

Verschlüsselungsalgorithmen, die nicht einen kontinuierlichen Datenstrom, sondern Datenblöcke fester Länge verarbeiten. Beispiel hierfür sind die von PGP genutzten symmetrischen Verschlüsselungsalgorithmen Triple-DES, CAST und IDEA.

Brute-Force-Attacke

Versuch, einen Schlüssel durch Ausprobieren aller möglichen Schlüssel zu erhalten.

Chiffrieren

Daten von Klartext in Chiffretext umwandeln, verschlüsseln.

Certificate Authority

Siehe Trustcenter.

Cipher-Feedback-Modus (CFB)

Modus der Blockchiffrierung, bei dem der Chiffrieralgorithmus nicht direkt zur Verschlüsselung der Daten, sondern der Erzeugung eines temporären Schlüssels dient, mit dem der anstehende Datenblock verschlüsselt wird.

Corporate Signing Key (CSK)

Schlüsselpaar, dessen öffentlicher Schlüssel automatisch von allen Client-Schlüsseln als gültig und voll vertrauenswürdig anerkannt wird. Vorteil: Jeder Schlüssel, der später vom privaten Schlüssel des CSK signiert wird, erhält unternehmensweite Gültigkeit.

Dechiffrieren

Einen Chiffretext in Klartext umwandeln, entschlüsseln.

Digitale Signatur

Siehe Signatur.

Digitales Zertifikat

Siehe Zertifikat.

Einweg-Hashfunktion

Siehe Hashfunktion.

Elektronische Signatur

Siehe Signatur.

E-Mail

Internetdienst zur Übertragung von Nachrichten zwischen Netzbenutzern.

Fingerabdruck (Fingerprint)

Eindeutiges Identifizierungsmerkmal eines Schlüssels, eine Zahlenfolge aus 16 (RSA-Schlüssel) bzw. 32 (DH-Schlüssel) Hexadezimalzahlen, die mittels einer Hashfunktion aus dem Schlüssel errechnet wird.

Firewall

Rechner, der zwischen dem internen Netz (Intranet) und dem Internet geschaltet wird und nach bestimmten Regeln kontrolliert, welche Art des ein- und ausgehenden Netzverkehrs zulässig ist. Schirmt unberechtigte Angriffe vom Internet auf das Intranet ab.

FTP

File Transfer Protocol. Anwendungs- und Netzprotokoll im Internet zur Übertragung von Dateien zwischen zwei Rechnern.

Geheimer Schlüssel (privater Schlüssel, secret key, private key)

Der in einem (symmetrischen oder asymmetrischen) Verschlüsselungssystem benutzte Schlüssel, von dessen Geheimhaltung auch die Geheimhaltung der Daten abhängt.

Speziell: In einem asymmetrischen Verschlüsselungssystem dient der geheime Schlüssel a) zur Entschlüsselung von Nachrichten, die mit dem entsprechenden öffentlichen Schlüssel chiffriert wurden und b) zur Signierung von Nachrichten.

Gültigkeit (Validity)

Der öffentliche Schlüssel eines Kommunikationspartners erhält mit der Signatur Gültigkeit für den Signierenden. Mit der Signatur bekundet der Signierende, dass er sich von der Echtheit und Unverfälschtheit des öffentlichen Schlüssels überzeugt hat.

Hashfunktion

Algorithmus, der aus einem beliebig langen Klartext ein immer gleich langes Komprimat, den Message Digest, errechnet, wobei auch nur die kleinste Änderung des Klartextes zu einem anderen Ergebnis führen würde. Bei einer **Einweg-Hashfunktion** ist der Vorgang nicht umkehrbar, d.h. aus dem Komprimat kann nicht der Ursprungstext ermittelt werden.

Incoming Additional Decryption Key (IADK)

Siehe Additional Decryption Key.

Initialisierungsvektor

Eine zufällige Bitfolge, die als Ausgangswert für weitere Berechnungen in einem symmetrischer Verschlüsselungsalgorithmus im Cipher Feedback Modus benutzt wird.

Internet

Weltweites, durch das TCP/IP-Protokoll verbundenes Computernetzwerk.

Iteration

Die Verschlüsselung geschieht in den besprochenen symmetrischen Verschlüsselungsalgorithmen in mehreren Durchläufen, den Iterationen.

IP-Adresse

Rechneradresse im Internet, (in der gewöhnlichen Darstellungsform) bestehend aus vier durch Punkte getrennte Zahlen zwischen 1 und 256. Beispiel: 192.168.47.11

Key ID

Identifikationsnummer des Schlüssels, bestehend aus 8 hexadezimalen Zahlen und einem vorangestellten `0x`. Beispiel: `0xBD85B7C3`

Key Server

Datenbank, die öffentliche PGP-Schlüssel sammelt und auf Anfrage zur Verfügung stellt.

Konventionelle Verschlüsselung

Siehe symmetrische Verschlüsselung.

Kompromittierung

Die wörtliche Übersetzung von kompromittieren ist „bloßstellen“. Auf einen Schlüssel bezogen heißt dies, dass der Schlüssel einem Angreifer in die Hände fällt und ihm bekannt wird.

Kryptoanalyse

1. Lehre von der (unbefugten) Entschlüsselung von Geheimschriften.
2. Versuch, Chiffrierschlüssel oder Klartext in einem kryptographischen System zu ermitteln.

Kryptographie

Die wissenschaftliche Disziplin von der Verheimlichung der Information.

Kryptographisches System

Ein kryptographisches System umfasst mindestens einen kryptographischen Algorithmus und die Gesamtheit aller möglichen Schlüssel.

Kryptographischer Algorithmus

Mathematische Prozedur zur Ver- und Entschlüsselung von Daten.

Kryptologie

Der Oberbegriff für die wissenschaftlichen Disziplinen Kryptographie und Kryptoanalyse.

Kryptosystem

Siehe Kryptographisches System.

Mantra

Siehe Passphrase.

Message Digest

Das immer gleich lange Komprimat, das von einer Hashfunktion aus einem Klartext errechnet wird, wobei auch nur die kleinste Änderung des Klartextes zu einem anderen Message Digest führen würde. Der mit dem geheimen Schlüssel des Absenders chiffrierte Message Digest wird von PGP als Signatur einer Nachricht verwendet.

Message Recovery Key (MRK)

Siehe Additonal Decryption Key.

Meta-Introducer

Signiert der Anwender den Schlüssel eines Kommunikationspartners mit dem Zusatz Meta-Introducer, so werden alle vom Partner mit dem Zusatz Trusted Introducer signierten Schlüssel für den Anwender gültig und vertrauenswürdig. Diese wiederum besitzen nun auch für den Anwender die Eigenschaft des Trusted Introducer, was bedeutet, dass alle von Ihnen signierten Schlüssel nun auch für den Anwender gültig werden.

Öffentlicher Schlüssel (public key)

Schlüssel, der in einem asymmetrischen Verschlüsselungsverfahren zur Verschlüsselung von Daten und zum Verifizieren von Signaturen dient. Der öffentliche Schlüssel kann öffentlich verbreitet werden, ohne die Sicherheit der chiffrierten Daten zu gefährden.

Outgoing Additional Decryption Key (OADK)

Siehe Additional Decryption Key.

Passphrase (Mantra)

Eine von dem Anwender frei wählbare und beliebig lange Zeichen- oder Wortfolge, die den geheimen Schlüssel PGPs vor unbefugtem Zugriff schützt, vergleichbar mit einem langen Kennwort.

Post Office Protocol (POP)

Anwendungsprotokoll, das dem Mail-Client die Zugangsmöglichkeit zum Mail-Server verschafft, um E-Mails zu versenden oder abzuschicken.

Private key

Siehe geheimer Schüssel.

Privater Schlüssel

Siehe geheimer Schüssel.

Public Certification Authority (PCA)

Siehe Trustcenter.

Public key

Siehe öffentlicher Schlüssel.

Public-Key-Verschlüsselungsverfahren

Verschlüsselungsverfahren, das einen asymmetrischen Verschlüsselungsalgorithmus benutzt, d.h. mit öffentlichen Schlüsseln (public keys) verschlüsselt und mit privaten Schlüsseln (private keys) entschlüsselt.

Router

Grenzrechner an der Schnittstelle zweier Netze, der Datenpakete auf ihrem Weg vom Sender zum Empfänger im Internet weiterleitet.

Schlüssel

Ein Wort, eine Zahl oder andere Datenfolge, die zusammen mit einem Verschlüsselungsalgorithmus dazu benutzt wird, eine Nachricht zu (de)chiffrieren.

Schlüsselbund

PGP speichert öffentliche Schlüssel in Dateien mit der Endung „pkr“ und private Schlüssel mit „skr“, was soviel bedeutet wie „private keyring“ bzw. „secret keyring“, also privater oder geheimer Schlüsselbund.

Als Schlüsselbund kann man auch die Anzeige des Moduls PGPkeys bezeichnen, da hier die Schlüssel im Besitz des Anwenders angezeigt werden.

Schlüssel-ID

Siehe Key ID.

Schlüsselpaar

Der öffentliche und der dazugehörige private Schlüssel.

Secret key

Siehe geheimer Schüssel.

Session Key

Siehe Sitzungsschlüssel.

Signatur

Der mit dem privaten Schlüssel chiffrierte Message Digest einer Datei. Die Verifizierung der Signatur mit dem öffentlichen Schlüssel erfüllt zwei Aufgaben:

1. Die Authentifikation des Absenders.

2. Die Prüfung der Integrität der Nachricht.

Sitzungsschlüssel (Session Key)

Einmalig verwendeter Schlüssel in einem symmetrischen Verschlüsselungsalgorithmus. In PGP wird die Nachricht zunächst mit einem Sit-

zungsschlüssel verschlüsselt. Dieser wird anschließend mit dem öffentlichen Schüssel des Empfängers verschlüsselt und zusammen mit der Nachricht verschickt.

SMTP (Simple Mail Transfer Protocol)

Dieses Protokoll beinhaltet die nötigen Direktiven, um bei der Datenübertragung elektronischer Mail den Sender, den Empfänger sowie den Text einer Nachricht festzulegen.

Stromchiffrierung

Chiffrierung, die im Gegensatz zur Blockchiffrierung keine Datenblöcke, sondern einen kontinuierlichen Datenstrom verschlüsselt.

Substitution

Ersetzen eines Zeichens durch ein anderes.

Symmetrische Verschlüsselung

Verschlüsselungsverfahren, bei dem für die Ver- und Entschlüsselung derselbe Schlüssel verwendet wird.

TCP/IP (Transmission Control Protocol / Internet Protocol)

Protokollsatz, der im Internet die Datenübertragung steuert.

Telnet

Internet-Protokoll für fernen Terminalzugriff.

Transposition

Vertauschen der Reihenfolge der Zeichen in einer Zeichenfolge.

Trust

„Vertrauen“, Eigenschaft eines Schlüssels, womit der Schlüsselbesitzer eingeschätzt wird. Verleiht der Anwender dem Schlüssel seines Kommunikationspartners die Eigenschaft Trust, so werden alle vom Partner signierten Schlüssel auch für den Anwender gültig.

Trustcenter

Ein *Trustcenter*, zu deutsch „Zentrum des Vertrauens“, ist ein Key Server, der über die Funktion des Schlüsselverteilers hinaus als Zertifizierungsstelle dient: Das Trustcenter bestätigt mit seiner Signatur, dass der signierte öffentliche PGP-Schlüssel auch einer genau bestimmten Person gehört.

Trusted Introducer

Signiert der Anwender den Schlüssel eines Kommunikationspartners mit dem Zusatz Trusted Introducer, so werden alle vom Partner signierten Schlüssel auch für den Anwender gültig.

User-ID

Die persönlichen Angaben über den Benutzer des PGP-Schlüssels. I.d.R. der Name und E-Mail-Adresse.

Validity

Siehe Gültigkeit.

Verifizierung

Die Verifizierung der Signatur einer Nachricht hat zum Ziel:

1. Die Authentifikation des Absenders.

2. Die Prüfung der Integrität der Nachricht.

Vertrauen

Siehe Trust.

Web of Trust

„Netz des Vertrauens“, Vertrauensmodell von PGP: Öffentliche Schlüssel im Schlüsselbund des Anwenders werden vom Anwender mit der Eigenschaft Validity (Gültigkeit) ausgezeichnet, wenn die Echtheit des Schlüssels bestätigt wurde. Gültige Schlüssel können darüber hinaus die Eigenschaft Trust (Vertrauen) erhalten, womit die persönliche Eigenschaft des Schlüsselinhabers eingeschätzt wird.

Alle weiteren Schlüssel, die von einem mit Vertrauen ausgezeichneten Schlüssel signiert wurden, werden automatisch für den Anwender gültig. Folge: Der Anwender braucht nicht mehr die Echtheit dieser weiteren Schlüssel zu prüfen, die von einem vertrauensvoll eingestuften Schlüssel signiert wurden. Er verlässt den als vertrauensvoll eingestuften Schlüsselinhaber, der mit seiner Signatur bestätigt, die Echtheit des anderer Schlüssel bereits kontrolliert zu haben.

Ein Netz dieser Verflechtungen wird auch als das Web of Trust bezeichnet.

Siehe auch die Erläuterung zu Meta-Introducer und Trusted Introducer.

World Wide Web (WWW)

Internetdienst, dessen vielfach grafisch und multimedial gestaltete Informationen per Hypertext miteinander verbunden sind. Das WWW vereint mehrere Internet-Dienste unter einer Benutzeroberfläche.

Zeitstempel

§2 Abs. 4 SigG: „Ein Zeitstempel [...] ist eine mit einer digitalen Signatur versehene digitale Bescheinigung einer Zertifizierungsstelle, dass ihr bestimmte digitale Daten zu einem bestimmten Zeitpunkt vorgelegen haben."

Anmerkung: Für PGP ist es z.Zt. noch nicht möglich, einen signaturgesetzkonformen Zeitstempel zu erzeugen.

Zertifikat

Signatur einer Zertifizierungsstelle unter dem öffentlichen Schlüssel des Antragstellers, mit der die Zertifizierungsstelle bestätigt, dass zu dem signierten öffentlichen PGP-Schlüssel auch eine genau bestimmte Person gehört.

Zertifizierungsstelle

Siehe Trustcenter.

ZIP-Komprimierungsroutinen

In PGP benutzte und aus dem Programm PKZIP bekannte Algorithmen zur Komprimierung von Daten.

G Stichwortverzeichnis

A

B

C

D

E

F

G

H

I

K

S

T