

FH KÖLN ABT. GUMMERSBACH, FB MASCHINENTECHNIK

MITARBEITERSCHULUNG

DOZENT: DIPL. ING. LUTZ MÜLLER

STAND: 9. JULI 2001

Praktischer Einsatz von PGP als Datenverschlüsselungssystem auf MS-Windows

Vorwort

Liebe Kolleginnen und Kollegen,

dieses Skript soll Ihnen als Hilfe zur Mitarbeiterschulung dienen. Es erhebt keinen Anspruch auf eine vollständige Erklärung von PGP, insbesondere werde ich die mathematischen Hintergründe dieses Verfahren nicht ausführlich erklären.

Eine der Stärken von PGP ist die Verfügbarkeit auf fast allen Rechner und Betriebssystemen, wobei aber MS Windows an unserer FH am häufigsten eingesetzt wird. Deshalb steht die Erklärung von PGP als praktische Anwendung unter MS Windows in diesem Skript im Vordergrund. Ich denke aber, dass sich ein interessierter Anwender durch autodidaktisches Lernen (z.B. mit Hilfe des WWW) durchaus in der Lage ist sein Wissen im Themenkreis PGP relativ leicht zu erweitern.

Natürlich - eiderweil Morphy's Law auch bei der Erstellung von Skripten zur Anwendung kommt - habe ich mich auf die Erklärung von PGP im Zusammenhang mit DH/DSS Schlüsselpaaren beschränkt. Zur Anwendung an der FH Köln kommen aber wahrscheinlich RSA Schlüsselpaare. Dumm gelaufen, aber für Sie als Anwender nicht weiter tragisch weil Sie als Benutzer von PGP diese Änderung nur einmal, d.h. bei der Erzeugung „Ihres Schlüsselpaares" berücksichtigen müssen.

Mein besonderer Dank gilt meiner Frau, sowie Herrn Dipl.-Ing. Sacha Müller (ZAM) und Herrn Dipl.-Inf. Michael Willecke (FB INF) die dieses Skript korekturgelesen haben, und mir so eine Verbesserung des Inhalts ermöglichten.

Sparen Sie bitte nicht mit Anregungen und Kritik !

Gummersbach, März 2001

Lutz Müller

Anmerkung: Der hexadezimal Fingerabdruck meines öffentlichen DH/DSS Schlüssel lautet:

```
3824 B26D C0ED 8270 823D  7EF9 C034 1048 7489 7A67
```

Inhalt

VORWORT **1**

INHALT **2**

1. EINLEITUNG **4**

1.1 WARUM MAN DATEN VERSCHLÜSSELN BZW. ELEKTRONISCH UNTERSCHREIBEN SOLLTE 4
1.2 WAS IST ZU BEACHTEN ? 5

2. VERSCHLÜSSELUNGSVERFAHREN **6**

2.1 GRUNDSÄTZLICHES 6
2.2 SYMMETRISCHES VERSCHLÜSSELN/ ENTSCHLÜSSELN 6
2.2.1 Eine unvollständige Aufzählung moderner symmetrischer Verschlüsselungsverfahren *8*
2.3 UNSYMMETRISCHES VERSCHLÜSSELN/ ENTSCHLÜSSELN SOWIE ELEKTRONISCH ES UNTERSCHREIBEN 8
2.3.1 Unsymmetrische Verschlüsselung/ Entschlüsselung *9*
2.3.2 Elektronisch Unterschreiben *10*
2.3.3 Prinzip des unsymmetrischen Verschlüsselns und der elektronische Unterschrift *12*
2.3.4 Eine unvollständige Aufzählung moderner unsymmetrischer Verschlüsselungsverfahren *15*
2.4 HYBRIDES VERSCHLÜSSELN/ ENTSCHLÜSSELN 15
2.5 KRITERIEN SICHERER VERSCHLÜSSELUNGSVERFAHREN 18

3. PGP – EINFÜHRUNG **19**

3.1 WAS IST EIGENTLICH PGP GENAU ? 20
3.2 WELCHE SCHWACHSTELLEN HAT PGP 21
3.2.1 Angriff auf PGP durch „Mann in der Mitte“ *21*
3.2.2 Entwenden des privaten Schlüssels und der Passphrase *22*
3.2.3 Gefälschte Zeitangaben bei elektronisch unterschriebenen Nachrichten *22*
3.2.4 Indirekte Angriffe *23*
3.3 DIE VERTEILUNG ÖFFENTLICHER SCHLÜSSEL SOWIE MÖGLICHKEITEN DEREN AUTHENTIZITÄT SICHERZUSTELLEN 24
3.3.1 Möglichkeiten zum Austausch öffentlicher Schlüssel *24*
3.3.2 Zertifizierungsstellen *25*
3.3.3 Schlüsselpartys *26*
3.3.4 Das Netz des Vertauens (The web of trust) *28*
3.4 WAS PGP GUT KANN 29
3.5 WAS PGP NICHT SO GUT KANN 29
3.6 ALLGEMEINE HINWEISE ZUR NUTZUNG PGP 30
3.7 WAS IST BEI DER NUTZUNG VON PGP FÜR WINDOWS ZU BEACHTEN ? 30

4. PGP - INSTALLATION AUF MS WINDOWS RECHNERN **31**

4.1 DOWNLOAD DER „RICHTIGEN“ INSTALLATIONSDATEI 31
4.2 INSTALLATION STARTEN UND PGP GRUNDEINSTELLUNGEN VORNEHMEN 31
4.3 PGP KOHNFIGURYEN 37
4.4 PGP ERWEITERUNG FÜR VERSCHIEDENE EMAIL PROGRAMME 47

5. PGP - ANWENDUNG AUF MS WINDOWS RECHNERN **48**

5.1 SCHLÜSSELVERWALTUNG 48
5.1.1 In Datei exportieren *48*
5.1.2 In Email einfügen *49*
5.1.3 Export per Drag & Drop *49*
5.1.4 Auf Keyservern veröffentlichen *50*
5.1.5 Überprüfung des öffentlichen Schlüssels mittels Fingerabdruck *51*
5.2 PGPTRAY 52
5.3 PGPNET 53
5.4 PGPKEYS 53
5.4.1 Menübar-Icons *54*
5.4.2 Schlüsselfenster-Icons *55*
5.5 PGPTOOLS 56
5.5.1 PGPTools aufrufen *56*
5.5.2 PGPTools - Verschlüsseln aufrufen *56*
5.5.3 PGPTools - Unterschreiben aufrufen *58*
5.5.4 PGPTools - Verschlüsseln+Unterschreiben aufrufen *59*
5.5.5 PGPTools - Entschlüsseln/Verifizieren aufrufen *61*
5.5.6 PGPTools - Unwiederherstallbar löschen aufrufen *63*
5.5.7 PGPTools - Freien Speicherplatz löschen aufrufen *64*
5.6 AKTUELLES FENSTER 65
5.7 ZWISCHENABLAGE 69
5.8 PGP UND STANDARDANWENDUNGEN 73

6. PGP KURZEINFÜHRUNG FÜR UNGEDULDIGE 75

7. GLOSSAR 76

3DES 76
ADK 76
CA 76
CAST 76
DES 76
DH 76
DSA 76
DSS 76
EINWEG-HASHFUNKTIONEN 76
ELGAMAL 76
FINGERABDRUCK (FINGERPRINT) 77
GNUPG 77
HASH-KOMPRIMAT 77
HYBRIDE VERSCHLÜSSELUNG 77
IDEA 77
KRYPTANALYSE 77
KRYPTOGRAPHIE 77
KRYPTOLOGIE 77
MANTRA 77
MD5 78
NSA 78
PGP 78
PGP - ÖFFENTLICHER SCHLÜSSEL (PUBLIC KEY) 78
PGP - PASSPHRASE 78
PGP - SCHLÜSSELKENNUNGEN 78
PGP - SCHLÜSSELZERTIFIKATE 78
PGP NETZ DES VERTAUENS (WEB AUF TRUST) 78
PRIMZAHL 78
PRIVATER SCHLÜSSEL (PRIVAT KEY) 79
RIPEMD-160 79
RSA 79
SCHLÜSSEL 79
SCHLÜSSELMANAGEMENT 79
SHA-1 79
SIGNATURE 79
STEGANOGRAFIE 80
SYMMETRISCHE VERSCHLÜSSELUNG 80
UNSYMMETRISCHE VERSCHLÜSSELUNG 80
ZUFALLSZAHL 80

8. QUELLENANGABEN 81

8.1 KONVENTIONELLE QUELLEN 81
8.2 INTERNET QUELLEN 81

1.Einleitung

1.1 Warum man Daten verschlüsseln bzw. elektronisch Unterschreiben sollte

Bitte Beantworten Sie sich selber nachfolgende Fragen:

- Warum versenden Sie wichtige Nachrichten an den Freundeskreis, den Mediziner oder an Ihren Rechtsbeistand nicht mit einer Ansichtskarte oder in einem unverschlossenen Brief ?
  Vielleicht weil dann zahlreiche Leute diese Nachricht lesen könnten ?

- Können Sie heute schon via Email verbindliche Bestellungen aufgeben oder rechtswirksame Angebote erhalten ?

- Sind Sie ganz sicher das niemand Ihre Emails im Inhalt oder im Absendervermerk fälschen kann ?

Viele Email Benutzer vergessen scheinbar, dass die Email viele Mailserver passiert, und dass die Daten in der Regel im Klartext versendet werden. Personen, die Zugang zu diesen Mail-Servern haben, könnten diese Nachricht lesen und manipulieren. Hacker könnten mit Netzwerkanalyseprogrammen (z.B. mit den sogenannten „snifern") die Daten während des Versendens mitlesen.

Es ist auch recht einfach Emails unter falschen Namen zu verfassen und zu versenden. Auch Geheimdienste interessieren sich für die Email, Telefaxe und Telefonate der Bundesbürger. Der Bundesbeauftragte für den Datenschutz geht davon aus, dass auf diese Weise täglich Ferngespräche und Telefaxkorrespondenzen in sechsstelliger Größenordnung überwacht und etwa 4.000 Gespräche einschließlich der Verbindungsdaten aufgezeichnet werden, z.B. die NSA - ein US Amerikanischer Geheimdienst - betreibt mit dem Projekt ECHELON eine gigantische weltweite Abhöraktion.

Ein mögliches Risiko an einer Hochschule wäre z.B. dass der Herr Prof. Dr. Unbedarft den Mitarbeitern der Druckerei die neuen Klausuraufgaben unverschlüsselt „zumailt". Wenn diese mitgelesen würden, könnte es zu rechtlichen Problemen kommen; ich gehe davon aus dass es auch im Verwaltungsbereich der Fachhochschule eine große Menge schützenwerter Emails gibt.

Sie sehen dass es sehr gute Gründe gibt private und dienstliche Email und andere relevante Daten zu verschlüsseln. Darüber hinaus besteht oft noch dienstlicher und privater Klärungsbedarf was die Authentizität von Email und Daten angeht. Ohne die Möglichkeit einer elektronischen Unterschrift besteht immer die Gefahr das „Böse Buben" Ihre Email teilweise oder komplett verändern bzw. dass Ihnen Emails zugesandt werden deren Absendernamen und Adressen gefälscht worden sind.

In meinen Augen besteht erhöhter Handlungsbedarf gerade weil wir im Zeitalter der vernetzten Computer leben. Zum Glück stellen die Computer mit ihren vernetzten Anwendungen nicht nur eine Gefahr für die Datensicherheit dar, sondern bieten auch wirksame Schutzprogramme, wie z.B. das hier vorgestellte PGP, die richtig angewendet dafür sorgen, dass wir relativ sorgenfrei mit diesem Medium umgehen können.

Abschließend sei bemerkt, dass der Wunsch „sicher" zu kommunizieren uralt ist. Wer mehr über die gesamte Geschichte und die mathematischen Grundlagen der Kryptologie wissen möchte, den empfehle ich das Springer Lehrbuch, „Kryptologie" von Bauer.

1.2 Was ist zu beachten ?

Email Verschlüsselung und die Einführung einer elektronischen Unterschrift kann nur ein kleiner Teil eines gesamten Sicherheitskonzeptes sein kann. Daten verschlüsseln bzw. signieren alleine reicht oft nicht aus um Datensicherheit zu gewährleisten. Sehen Sie bitte darum in dieser Mitarbeiterschulung nur einen ersten Schritt in einem noch zu erstellenden Gesamtkonzept für Datensicherheit an unserer Hochschule.

Es sollte auch nicht verschwiegen werden dass die bei modernen Verschlüsselungsverfahren notwendige „Public-Key-Infrastruktur" nicht immer auf die Akzeptanz der Anwender trifft. Die anfängliche Euphorie der Fachleute ist heute einer nüchternen Betrachtungsweise gewichen (Siehe dazu Artikel c't 2/2001 S.60, „Wer braucht digitale Signaturen ?" von Stefan Krempl).

Darüber hinaus sollten Sie sich nicht scheuen im Zweifelsfall, wenn Sie irgendwelche Bendenken um die Sicherheit Ihrer dienstlichen Daten haben, die Fachleute der ZI anzusprechen.

2.Verschlüsselungsverfahren

2.1 Grundsätzliches

> „Was ein Mensch sich ausdenken kann, kann ein anderer Mensch auch herausbekommen.“ Sherlock Holmes in die „Das Abenteuer der tanzenden Männer“ von Sir Arthur Conan Doyle
>
> „Was von einer Maschine chiffriert worden ist, läßt sich um so einfacher auf einer Maschine wieder dechiffrieren.“ Andrew Hodges „Alan Turing: The Enigma"

Ein wenig Theorie muss, obwohl es sich ja eigentlich um eine praktische Mitarbeiterschulung handelt, dennoch sein. Nachfolgend werden zwei grundsätzliche Arten der Verschlüsselung sowie die „Mischform“ beider Verschlüsselungsverfahren vorgestellt. Für den Anwender wäre es gut zu wissen wann er welches Verschlüsselungsprinzip einsetzen sollte.

2.2 Symmetrisches Verschlüsseln/ Entschlüsseln

Die ältesten Codes verwandeln eine in Umgangssprache formulierte Nachricht in eine chiffrierte Botschaft, indem jeder Buchstabe des Alphabets, durch einen anderen ersetzt wird. Beim sogenannten Caesar-Code geschieht das **Verschlüsseln** gemäß folgender Methode:

1. Man ersetzt die Buchstaben der Nachricht (**A**, **B**, **C**, usw..) durch Zahlen von **0** bis **25**.
   Es wird also aus **A**=>**0**, **B**=>**1**, **C**=>**2**, usw.

2. Zu den einzelnen Zahlen wird ein bestimmter Schlüsselwert hinzu addiert. Wenn der Schlüssel z.B. **N** ist hat er einen Wert von **13**.
   Daraus folgt das aus **A**=>**0**=>0+13=**13**, **B**=>**1**=>1+13=**14**, **C**=>**2**=>2+13=**15**, usw. wird

3. Wenn eine Zahl größer gleich 26 sein sollte wird 26 subtrahiert.
   So wird aus **X**=>**23**=>23+13=**36**=>36-26=**10**

4. Die Zahlen aus Schritt 3 (**0**, **1**, **2**, usw.) werden wieder in Buchstaben von **A** bis **Z** umgewandelt.
   Man erhält dadurch die verschlüsselte Nachricht

Wenn obiges Verfahren auf die unverschlüsselte Nachricht,

SCHICKE EILENDS VERSTAERKUNG

mit dem Schlüssel **N** (Wert = **13**) angewendet wird, ergibt sich:

FPUVPXR RVYRAQF IREFGNREXHAT

Nach dem verschlüsseln sollte die Nachricht und der Schlüssel auf **getrennten** Wegen den vorgesehenen Empfänger erreichen. Dieser kann dann mit nachfolgenden Schritte das **Entschlüsseln** vornehmen:

1. Man ersetzt die Buchstaben der verschlüsselten Nachricht (**A**, **B**, **C**, usw..) durch Zahlen von **0** bis **25**.
   Es wird also aus **A**=>**0**, **B**=>**1**, **C**=>**2**, usw.

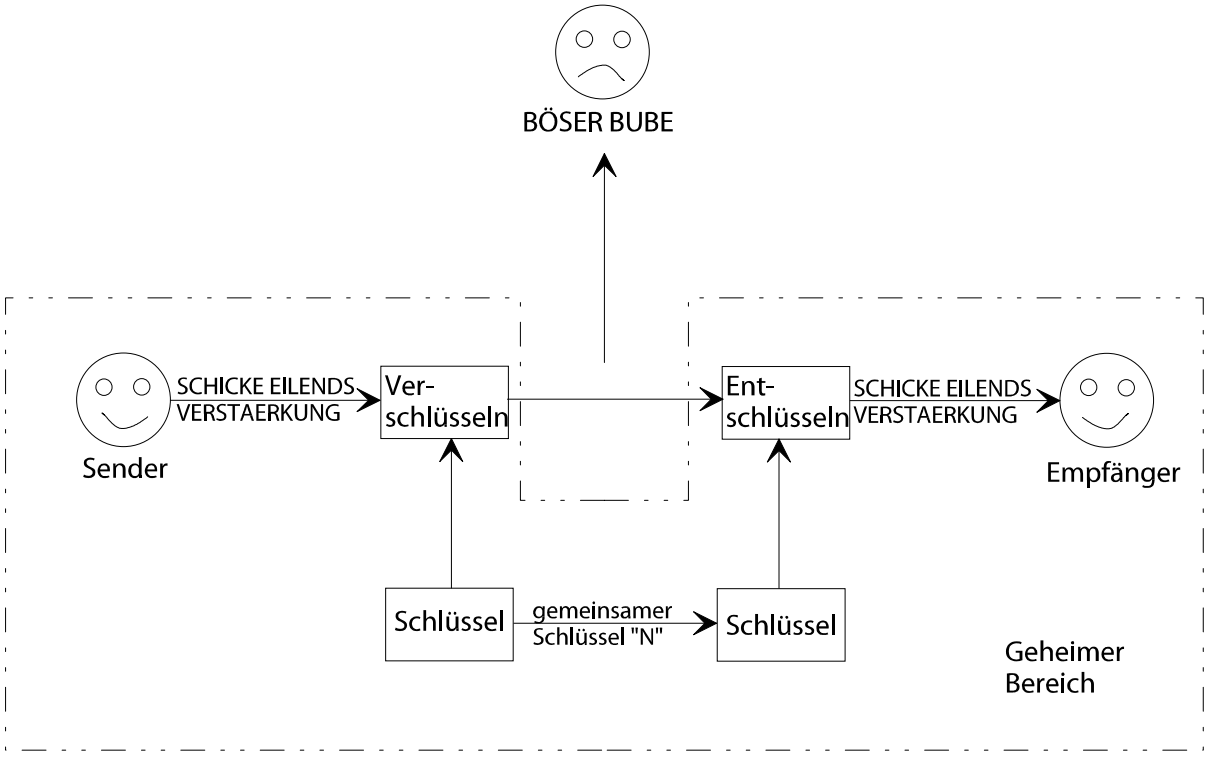
2. Der Schlüsselwert des Schlüssels (in unserem Fall ist der Schlüssel **N** mit dem Wert die **13**) wird von den in 1. ermittelten Zahlen subtrahiert.
   Daraus folgt das aus **13**=>13-13=**0**, **14**=>14-13=**1**, **15**=>15-3=**2** wird

3. Wenn eine Zahl negativ, d.h. kleiner **0** sei sollte muss man den Wert **26** addieren.
   So wird aus **10**=>10-13=-3=>-3+26=**23**

4. Die Zahlen aus Schritt 3 (**0**, **1**, **2**, usw.) werden wieder in Buchstaben von **A** bis **Z** umgewandelt. Der Empfänger hat damit aus der verschlüsselten Nachricht den Klartext wiederhergestellt

Der Caesar-Code ist heutzutage sehr leicht zu „knacken", aber im Prinzip arbeiten alle symmetrische Verfahren ähnlich. Siehe dazu auch nachfolgender Abbildung.

Prinzip der symmetrischen Verschlüsselung/ Entschlüsselung



Der „Böse Bube" hat kaum Chancen die Nachricht aus dem verschlüsselten Text zu rekonstruieren wenn:

- Sender und Empfänger ein modernes Verfahren (z.B. 3DES) einsetzen
- Die Schlüssellange des geheimen gemeinsamen Schlüssels hinreichend lang ist. Z.B. heute gilt bei dem DES Verfahren eine Schlüssellänge von 168 Bit (3 Fache der Standardlänge von 56 Bit) als sicher
- Der gemeinsame geheime Schlüssel auf einem **sicheren** Weg zwischen Sender und Empfänger ausgetauscht wird

Gerade der letzte Punkt ist der Grund dafür das Diffie und Hellmann ein anderes Verfahren für den Austausch von Daten vorgeschlagen haben. Die Verfahren der symmetrischen Verschlüsselung sind jedoch immer noch aktuell wenn es z.B. darum geht die eigenen Daten auf der Festplatte zu verschlüsseln.

2.2.1 Eine unvollständige Aufzählung moderner symmetrischer Verschlüsselungsverfahren

- 3DES Data Encryption Standard, mit 3facher Schlüssellänge
- Blowfish Dieser Algorithmus wurde von Bruce Schneier entwickelt
- CAST Vermutlich nach seinen Autoren Carlisle Adams und Stafford Tavares benannt
- DES Data Encryption Standard
- FEAL Fast Data Encipherment Algorithm
- IDEA International Data Encryption Algorithm
- SAFER Secure And Fast Encryption Routine

Bemerkung: Die PGP Anwendungen der Version 6.X.X unterstützen 3DES , CAST und IDEA

2.3 Unsymmetrisches Verschlüsseln/ Entschlüsseln sowie elektronisch es Unterschreiben

Wenn sich Sender und Empfänger einer verschlüsselten Nachricht an verschiedenen Orten befinden, müssen sie einem Kurier, einer Telefonverbindung oder einem anderen Kommunikationsmedium trauen, um die Offenlegung des geheimen Schlüssels zu verhindern. Jeder, der den Schlüssel während der Übertragung abfangen oder mithören kann, kann danach alle verschlüsselten Nachrichten lesen, ändern, fälschen oder unterschreiben, indem er diesen Schlüssel verwendet. Die Schlüsselerzeugung, -übertragung und -speicherung wird Schlüsselmanagement genannt. Alle Verschlüsselungssysteme müssen sich damit befassen. Da alle Schlüssel eines symmetrischen Verfahrens geheim bleiben müssen, haben diese Systeme oft Schwierigkeiten mit einem sicheren Schlüsselmanagement, speziell in offenen Umgebungen mit vielen Nutzern.

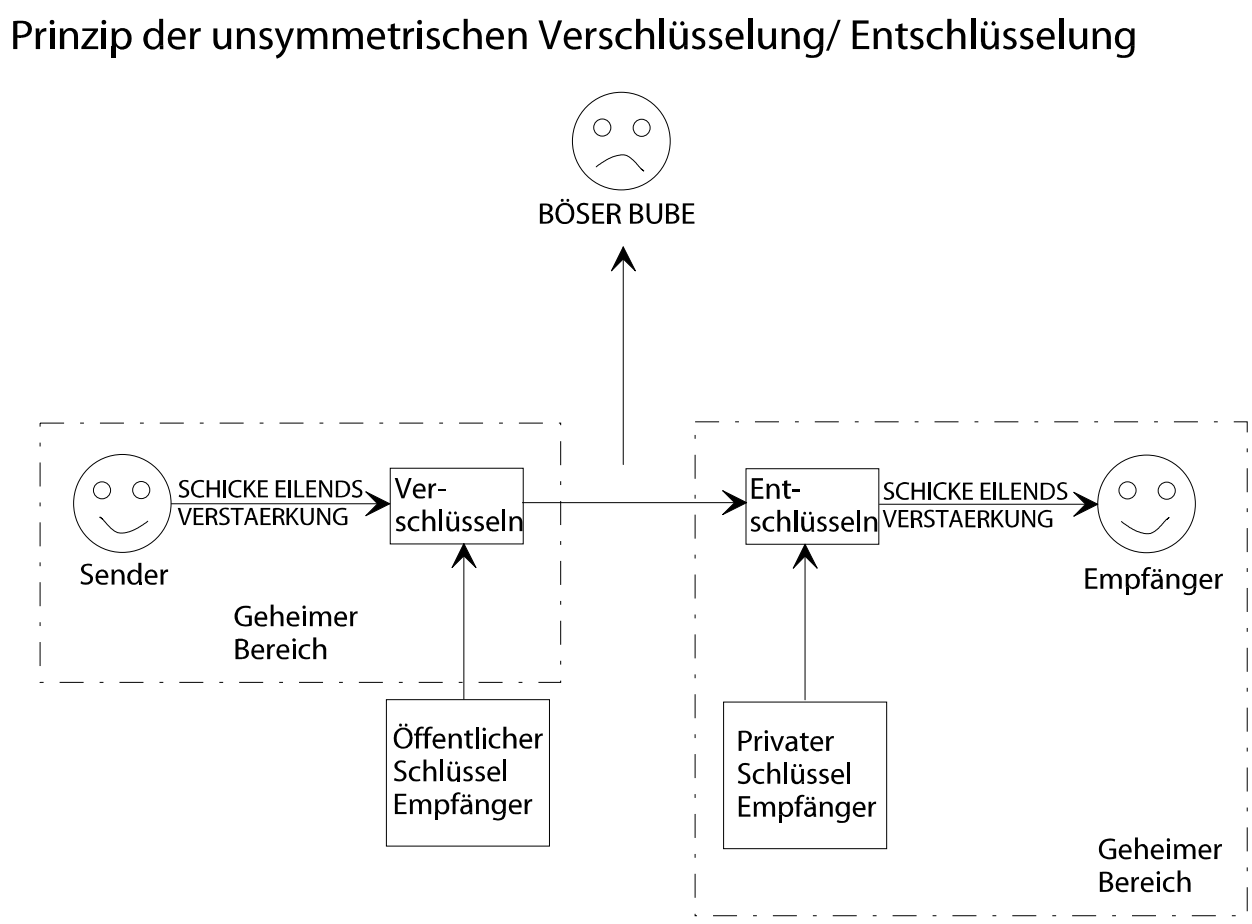
Das Konzept der asymmetrischen Kryptographie wurde 1976 von Whitfield Diffie und Martin Hellman vorgeschlagen, um das Schlüsselmanagementproblem zu lösen. In ihrem Konzept hat jeder Beteiligte zwei Schlüssel, einen Öffentlichen und einen Privaten. Jeder öffentliche Schlüssel wird veröffentlicht und der private Schlüssel beliebt geheim. Die Notwendigkeit eines gemeinsamen Geheimnisses zwischen Sender und Empfänger ist damit verschwunden: Jede Kommunikation umfasst nur öffentliche Schlüssel, private Schlüssel werden nie übertragen oder geteilt. Es ist nicht länger notwendig, einem Kommunikationskanal hinsichtlich Abhörsicherheit zu trauen. Die einzige Anforderung ist, dass der Zuordnung zwischen öffentlichem Schlüssel und Nutzer getraut werden kann. Jeder, der eine wichtige Information versenden will, verschlüsselt mit dem öffentlichen Schlüssel des Empfängers, die verschlüsselte Nachricht kann jedoch nur mit dem privaten Schlüssel des Empfängers entschlüsselt werden, der sich ausschließlich in der Hand des Empfänger befindet.

Im Prinzip arbeiten alle unsymmetrische Verschlüsselungsverfahren mit „öffentlichen Verschlüsselungsfunktionen“ und „privaten Entschlüsselungsfunktionen“. Der wunderbare Trick dieses Verfahrens beruht darauf, dass man trotz Kenntnis der „öffentlichen Verschlüsselungsfunktion“ praktisch nicht die Umkehrfunktion, d.h. die „private Entschlüsselungsfunktion“, ableiten kann. In diesem Zusammenhang spricht man auch von sog. „Falltürfunktionen“ die genau wie eine „richtige“ Falltür nur in einer Richtung begehbar sind.

2.3.1 Unsymmetrische Verschlüsselung/ Entschlüsselung

Wenn der Sender eine geheime Nachricht an den Empfänger senden will, so holt der Sender den öffentlichen Schlüssel des Empfängers von einem Schlüsselserver (bzw. via persönlichem Diskettenaustausch, Email Übertragung usw.) und benutzt diesen Schlüssel, nach Überprüfung der Authentizität (!), um die Nachricht zu verschlüsseln. Danach versendet er die verschlüsselte Nachricht. Der Empfänger benutzt seinen privaten Schlüssel, um die Nachricht zu entschlüsseln und zu lesen. Praktisch kann kein „Böser Bube" die Nachricht entschlüsseln. Jeder kann eine verschlüsselte Nachricht dem Empfänger senden, aber nur der Empfänger kann sie lesen. Es ist jedoch klar, dass niemand den privaten Schlüssel des Empfängers aus dem zugehörigen öffentlichen Schlüssel gewinnen können darf.

Nach folgende Abbildung stellt diesen Vorgang dar:



Der „Böse Bube" hat kaum Chancen die Nachricht aus dem verschlüsselten Text zu rekonstruieren wenn:

- Sender und Empfänger ein modernes Verfahren (z.B. RSA) einsetzen
- Der öffentliche Schlüssel des Empfängers nicht vom „Bösen Buben" gefälscht wurde
- Der private Schlüssel des Empfängers nicht vom „Bösen Buben" verwendet werden kann
- Die Schlüssellänge der verwendeten Schlüssel hinreichend lang ist. Z.B. gilt heute bei dem RSA Verfahren eine Schlüssellänge von 1024 Bit als (noch) sicher
- Es auch in Zukunft nicht gelingt aus dem öffentlichen Schlüssel des Empfängers den privaten Schlüssel „herauszurechnen"

2.3.2 Elektronisch Unterschreiben

Die unsymmetrische Verschlüsselungstechnik kann nicht nur zur Geheimhaltung sondern auch zur Authentifikation verwendet werden. Um eine Nachricht zu unterschreiben, berechnet der Sender mittels einer Hash-Funktion aus einer Nachricht ein sog. Hash-Komprimat. Vereinfacht kann man sich das Ergebnis als „digitalen Fingerabdruck" der Nachricht vorstellen. Es hat nachfolgende Eigenschaften:

- Mann kann praktisch aus dem Hash-Komprimat die eigentliche Nachricht nicht rekonstruieren
- Gleiche Nachrichten haben gleiche Hash-Komprimate
- Verschiedene Nachrichten haben verschiedene Hash-Komprimate

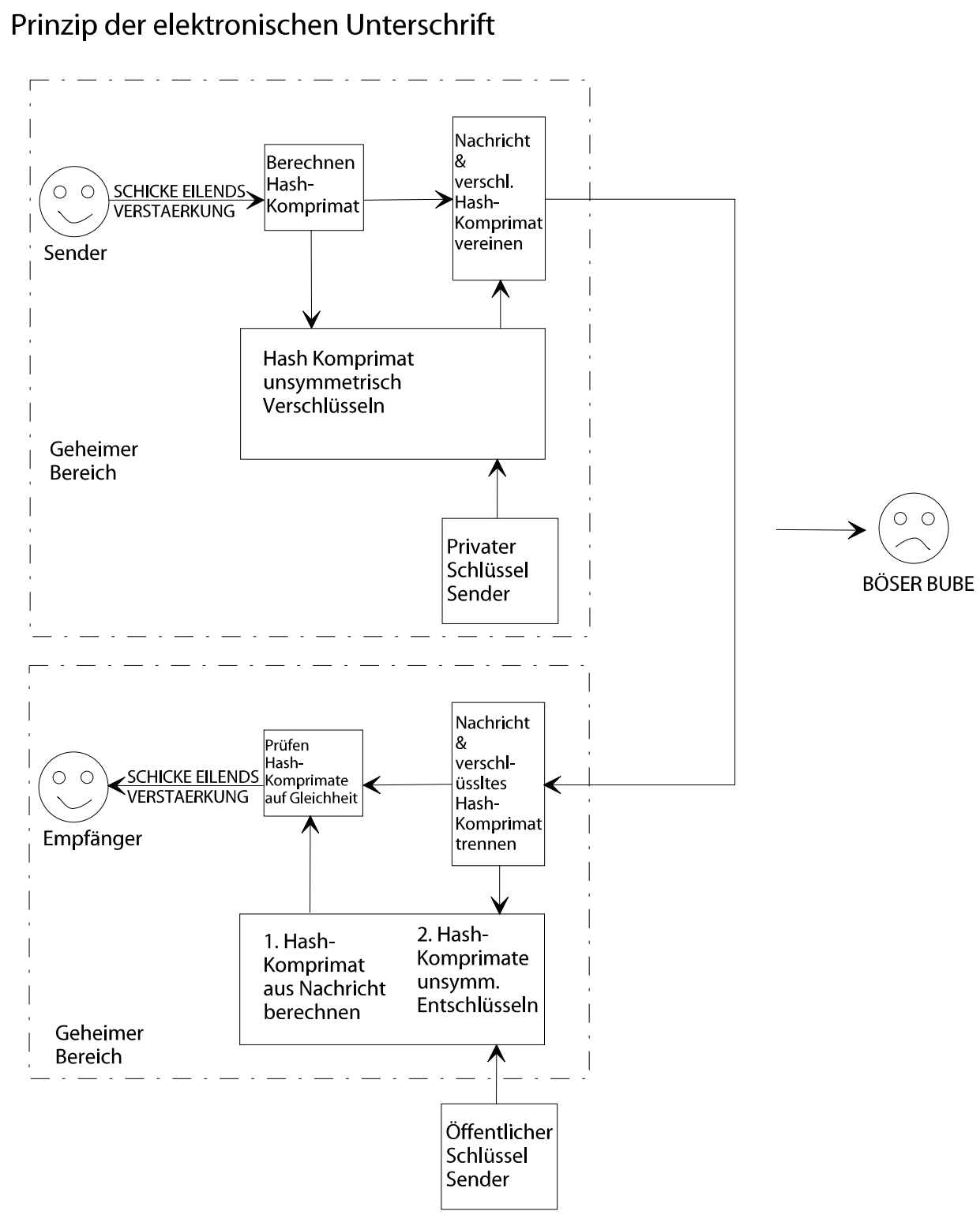
Dieses Hash-Komprimat wird dann mit dem privaten Schlüssel des Senders verschlüsselt. Das Ergebnis wird elektronische Unterschrift genannt und an die Nachricht angehängt. Der Empfänger kann die Unterschrift prüfen in dem er selber aus der Nachricht sein „1. Hash-Komprimat" berechnet und dann das „2. Hash-Komprimat", welches er erhält in dem er mit dem öffentlichen Schlüssel des Senders das der Nachricht angehängte „Hash-Komprimat" entschlüsselt, vergleicht. Nur wenn beide Hash-Komprimate gleich sind ist die Unterschrift gültig, anderenfalls ist die Unterschrift gefälscht oder die Nachricht wurde verändert.

Verfahren zur Erzeugung von Hash-Komprimaten sind z.B.:

- MD5 steht für Message Digest
- RIPEMD-160
- SHA-1 steht für Secure Hash Algorithm

Bemerkung: Die PGP Anwendungen der Version 6.X.X unterstützen MD5 , SHA-1 und RIPEMD-160

Nach folgende Abbildung stellt den Vorgang der elektronischen Unterschrift im Prinzip dar:



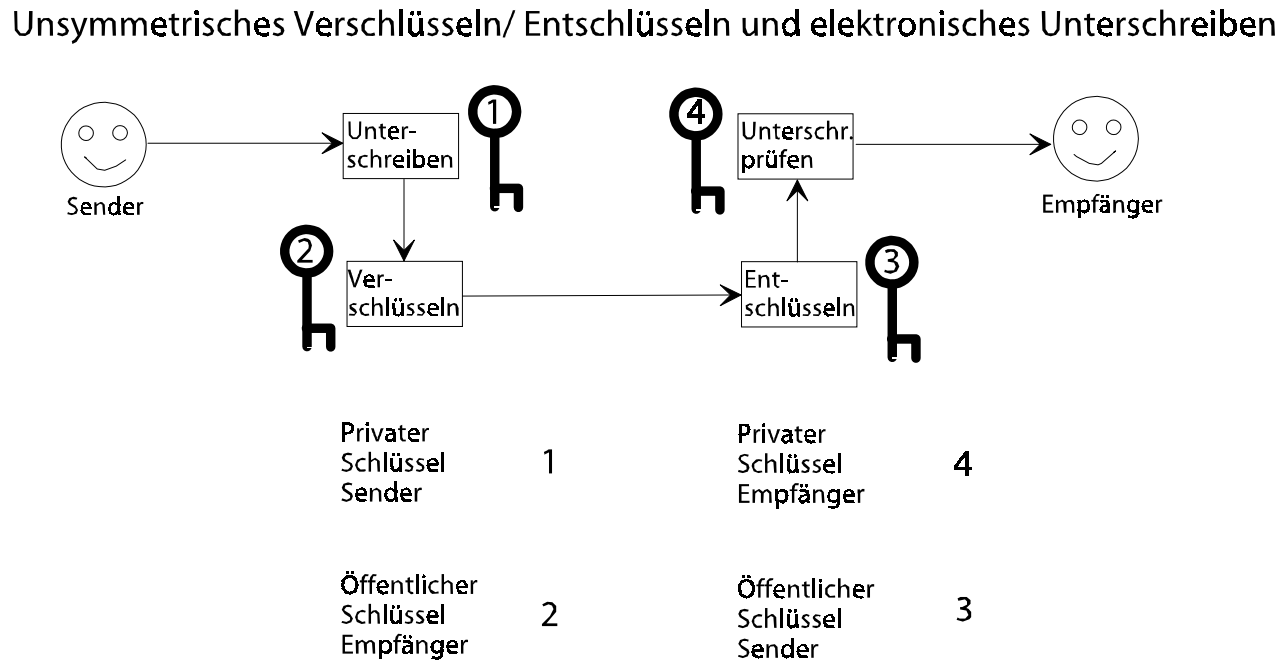
Es können je nach Bedarf verschlüsselte oder unverschlüsselte Daten elektronisch unterschreiben werden. Die Sicherheitsanforderungen sind die Gleichen wie bei der unsymmetrischen Verschlüsselung.

2.3.3 Prinzip des unsymmetrischen Verschlüsselns und der elektronische Unterschrift

Nun ja, wie in der Einleitung beschrieben möchte (und kann) ich keinen mathematischen Exkurs mit Ihnen durchführen. Ein wenig „empirische" Mathematik kann ich mir jedoch nicht verkneifen, vielleicht experimentieren Sie in einer stillen Stunde mit Ihrem PC und nachfolgend dargestellten Formeln. Für alle die dieses nicht vorhaben die Kernaussagen vorweg:

- Das vorgestellte Verfahren funktioniert nur, weil es bisher noch nicht gelungen ist ein Produkt aus zwei großen Primzahlen in vertretbarer Zeit wieder in seine Faktoren zu zerlegen
- Zum Verschlüsseln der Nachricht benötigt der Sender den öffentlichen Schlüssel des Empfängers
- Zum Entschlüsseln benötigt der Empfänger seinen privaten Schlüssel
- Zum unterschreiben der Nachricht benötigt der Sender seinen privaten Schlüssel
- Zum überprüfen der Unterschrift des Senders benötigt der Empfänger den öffentlichen Schlüssel des Senders

Nachfolgende Abbildung beschreibt den Vorgang im Prinzip:



Anmerkung zum Rechenbeispiel:

Die **mod** Funktion ist nichts weiter als der Divisionsrest aus zwei Zahlen. Z.B. ist **mod(12, 7) = 5**. eiderweil die 7 nur einmal in die 12 „reingeht" und 5 = 12 - 1x7 ist.

Die im Beispiel ausgewählten Primzahlen sind sehr klein, und damit für eine „richtige Verschlüsselung" nicht brauchbar.

Die Regeln sind für die RSA Verschlüsselung:
- Man nehme Primzahlen p und q
- Bilde deren Produkt n=p*q, welches Modul genannt wird
- Man wähle eine Zahl e die kleiner als n und teilerfremd zu p-1 und q-1 ist
- Finde eine Zahl d, so daß (e*d)-1 durch (p-1)*(q-1) teilbar ist

Erzeugen Schlüssel des Senders

$i := 1$ $e_i := 11$

$p_i := 13$ $q_i := 17$

$n_i := p_i \cdot q_i$ $n_i = 221$

Test ob gewählte Zahlen den Regeln entsprechen

$epTest_i := \frac{p_i - 1}{e_i}$ $epTest_i = 1.091$ $eqTest_i := \frac{q_i - 1}{e_i}$ $eqTest_i = 1.455$

$d_i := 35$ $dTest_i := \frac{e_i \cdot d_i - 1}{(p_i - 1) \cdot (q_i - 1)}$ $dTest_i = 2$

Ergebnis

$(n_1 \ e_1) = (221 \ 11)$ Öffentlicher Schlüssel des Senders

$(n_1 \ d_i) = (221 \ 35)$ Privater Schlüssel des Senders

Erzeugen Schlüssel des Empfängers

$i := 2$

$p_i := 11$ $q_i := 13$ $e_i := 7$

$n_i := p_i \cdot q_i$ $n_i = 143$

Test ob gewählte Zahlen den Regeln entsprechen

$epTest_i := \frac{p_i - 1}{e_i}$ $epTest_i = 1.429$ $eqTest_i := \frac{q_i - 1}{e_i}$ $eqTest_i = 1.714$

$d_i := 103$ $dTest_i := \frac{e_i \cdot d_i - 1}{(p_i - 1) \cdot (q_i - 1)}$ $dTest_i = 6$

Ergebnis

$(n_2 \ e_2) = (143 \ 7)$ Öffentlicher Schlüssel des Empfängers

$(n_2 \ d_2) = (143 \ 103)$ Privater Schlüssel des Empfängers

Nachfolgend wird die Zahl 42 mit obigen Schlüsselpaaren
verschlüsselt und unterschrieben. Benötigt wird:
- Zum verschlüsseln das öffentliche Schlüsselpaar des Empfängers
- Zum entschlüsseln das private Schlüsselpaar des Empfängers
- Zum unterschreiben das private Schlüsselpaar des Senders
- Zum prüfen der Unterschrift das öffentliche Schlüsselpaar des Senders

Übertragen vom Sender zum Empfänger werden:
- C = 81, dass ist die verschlüsselte Nachricht
- S = 190, dass ist die gültige Unterschrift für C=81

Sender verschlüsselt Nachricht durch Sender für Empfänger

$m_1 := 42$ Nachricht im Klartext

$c := \mathrm{mod}\left[\left(m_1\right)^{e_2}, n_2 \right]$ Verschlüsselungsfunktion des Empfängers

$c = 81$ Verschlüsselte Nachricht

Entschlüsseln der Nachricht durch Empfänger

$m_2 := \mathrm{mod}\left(c^{d_2}, n_2\right)$

$m_2 := 42$

$m_1 = m_2$ Damit hat der Empfänger die wichtige Zahl 42 "richtig" erhalten !

Unterschreiben der verschlüsselten Nachricht durch Sender

$c_1 := c \qquad c_1 = 81$

$s := \mathrm{mod}\left[\left(c_1\right)^{d_1}, n_1 \right]$

$s := 190$

Überprüfen der Unterschrift durch Empfänger

$c_2 := \mathrm{mod}\left(s^{e_1}, n_1\right)$

$c_2 := 81$

$c_1 = c_2$ Damit ist die Authentifizung des Senders ok !

2.3.4 Eine unvollständige Aufzählung moderner unsymmetrischer Verschlüsselungsverfahren

· DH/DSS — verschlüsseln nach Diffie Hellman, unterschreiben nach Digital Signature Standard

· ElGamal System

· Knapsack Kryptosystem

· Kryptosystem auf elliptischen Kurven

· RSA — nach Ron Rivest, Adi Shamir und Leonard Adleman

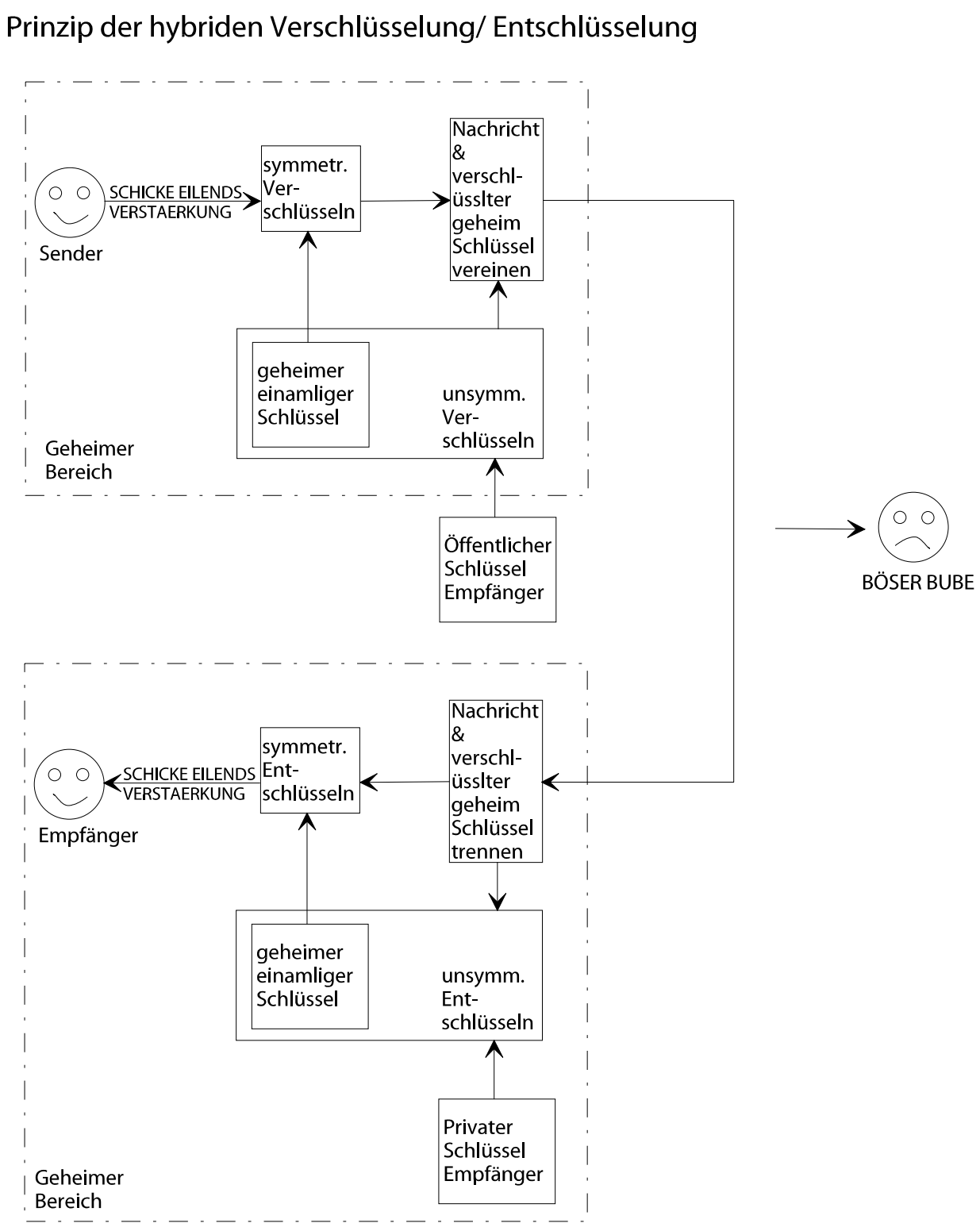
Bemerkung: Die PGP Anwendungen der Version 6.X.X unterstützen DH/DSS sowie RSA

2.4 Hybrides Verschlüsseln/ Entschlüsseln

Symmetrische Verfahren haben den Vorteil dass sie schon ab relativ kurzen Schlüssellängen (z.B. 168bit bei 3DES) praktisch nicht zu „knacken" sind. Dies bedeutet gegenüber unsymmetrischen Verfahren, die arbeiten „sicher" erst mit Schlüssellängen die ca. 10x länger sind, einen deutlichen Geschwindigkeitsvorteil beim Ver- bzw. Entschlüsseln von Daten. Dem Gegenüber bieten allerdings die unsymmetrischen Verfahren in der Praxis eine deutliche Erleichterung für den Anwender, eiderweil das verwalten und transportieren von Schlüsseln deutlich einfacher ist. Es müssen ja bei unsymmetrischen Verfahren „nur" die öffentlichen Schlüssel „sicher" verteilt werden. Die „Sicherheit des Verfahrens" besteht nicht in der Geheimhaltung der öffentlichen Schlüssel sondern in der Gewährleistung ihrer Authentizität.

Man möchte deshalb durch den Einsatz von hybriden Verschlüsselungsverfahren den Geschwindigkeitsvorteil der symmetrischen Verfahren und die Anwenderfreundlichkeit der unsymmetrischen Verfahren kombinieren.

Nach folgende Abbildung stellt diesen Vorgang im Prinzip dar:



Die notwendigen Arbeitsschritte dieses hybriden Verfahrens sind wie folgt:

- Der Sender erzeugt einen geheimen und einmaligen Schlüssel, den sog. Sitzungsschlüssel (session key)
- Mit diesem Sitzungsschlüssel wird die Nachricht symmetrisch verschlüsselt
- Der Sitzungsschlüssel wird mit dem öffentlichen Schlüssel des Empfängers unsymmetrisch verschlüsselt
- Die symmetrisch verschlüsselte Nachricht und der unsymmetrisch verschlüsselte Sitzungsschlüssel werden zusammengepackt und danach versendet
- Der Empfänger entschlüsselt mit seinen privaten Schlüssel den Sitzungsschlüssel
- Mit dem entschlüsselten Sitzungsschlüssel wird die Nachricht entschlüsselt

Der „Böse Bube" hat kaum Chancen die Nachricht aus dem verschlüsselten Text zu rekonstruieren wenn:

- Sender und Empfänger moderne Verfahren z.B. RSA und CAST einsetzen
- Sichergestellt ist das der Sitzungsschlüssel wirklich geheim und einmalig ist
- Der öffentliche Schlüssel des Empfängers nicht vom „Bösen Buben" gefälscht wurde
- Der private Schlüssel des Empfängers nicht vom „Bösen Buben" verwendet werden kann
- Die Schlüssellange der verwendeten Schlüssel hinreichend lang ist
- Es auch in Zukunft nicht gelingt aus dem öffentlichen Schlüssel des Empfängers den privaten Schlüssel „herauszurechnen"

2.5 Kriterien sicherer Verschlüsselungsverfahren

Nachfolgend einige qualitative Kriterien an denen Sie abschätzen können ob ein Verfahren als „sicher" gilt:

1. Eine Geheimhaltung der verfahrensinternen Rechenvorschriften ist nicht notwendig. Auch wenn der Angreifer das Verfahren bis in alle Einzelheiten kennt, sollte er daraus keine Möglichkeit erhalten irgendwelche Nachrichten zu entschlüsseln

2. Die verfahrensinternen Rechenvorschriften und der Programmiercode der Anwendung werden veröffentlich. Das schließt zum einen (fast) aus das Ihnen ein gewiefter Programmierer irgendwelche „offenen Hintertüren" eingebaut hat und zum anderen können (sehr qualifizierte) Kryptologen und Programmierer das Verfahren leicht auf Schwachstellen testen und es evtl. weiterentwickeln

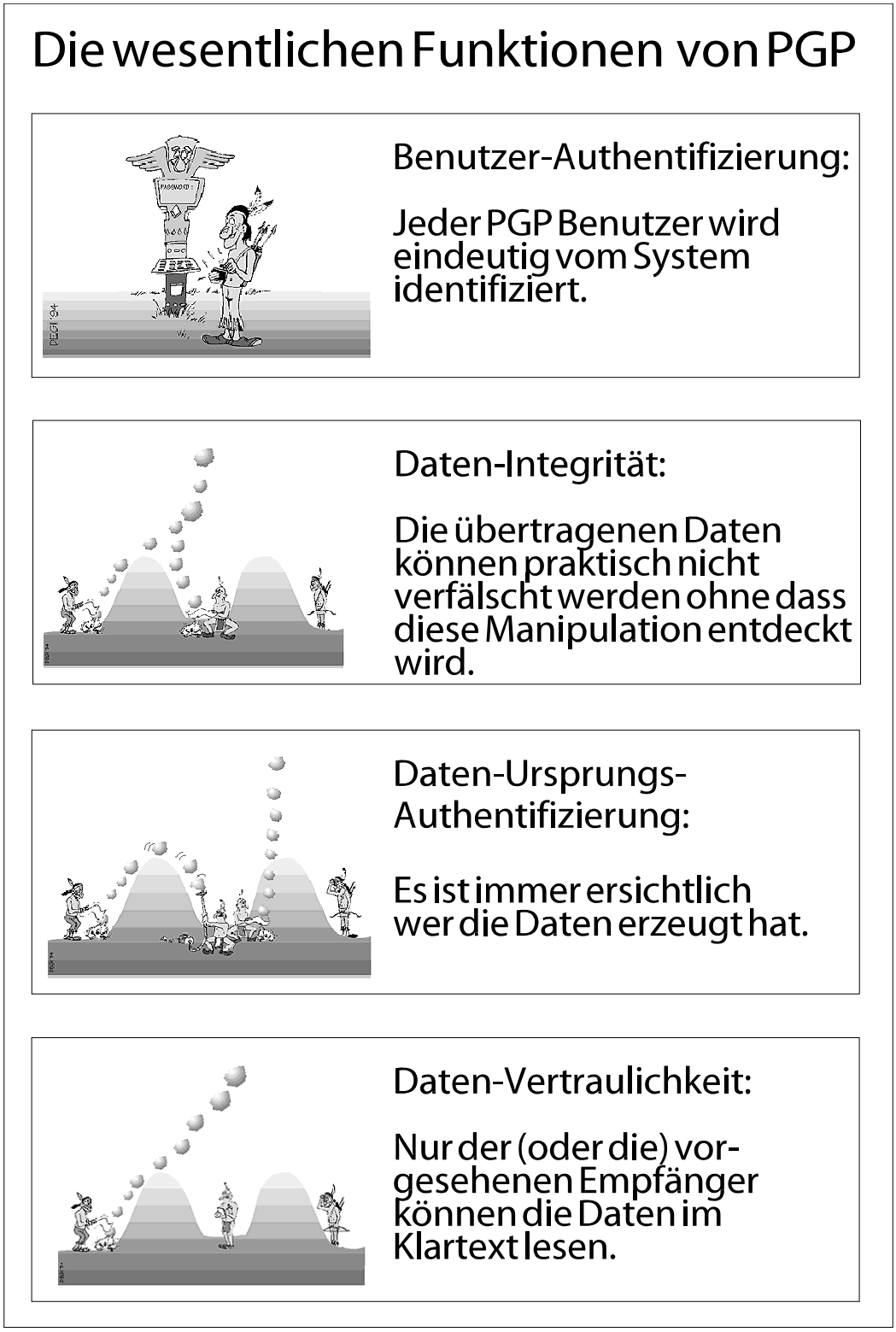
3. Das Verfahren und die Programme sollten gezielt zur Verschlüsselung von Daten entwickelt worden sein. Verfahren und Programme deren „Nebentätigkeit" das Verschlüsseln darstellt sind nicht sicher. Bestes Beispiel dafür ist die Verschlüsselungsfunktion in vielen Datenkomprimierungswerkzeugen (z.B. ZIP) die von Experten als eher unsicher angesehen wird

Wenn obige Punkte erfüllte werden, gehen die Experten davon aus das einzig und alleine eine „Brute-Force-Attacke", also ein Durchrechnen aller möglichen Schlüssel, zu einem erfolgreichen Angriff führen. Dem kann man leicht begegnen indem man eine hinreichende Schlüssellänge vorsieht, z.B. gilt DES mit 56 Bit Schlüssellänge als nicht mehr sicher, 3DES mit 168 Bit Schlüssel widersteht zur Zeit (und wohl auch noch die nächsten Jahre) jedem dieser Angriffe.

Bemerkung: Die PGP Anwendung erfüllt sicher 1. und 3. Der Quellcode von PGP liegt zwar auch vor, zumindest aber bei der in dieser Schulung verwendeten PGP Anwendung wird, dieser jedoch oft als „schlecht Lesbar" bezeichnet.

3.PGP – Einführung

Die Möglichkeiten der PGP Nutzung gehen aus nachfolgender Abbildung hervor:



Diese Funktionen kann PGP nur dann leisten wenn es hinreichend „gut“ angewendet wird und durch flankierende Maßnahmen gestützt wird (wie z.B. die Nutzung von zertifizierten Schlüsseln).

3.1 Was ist eigentlich PGP genau ?

PGP steht für **P**retty **G**ood **P**rivacy (d.h. übersetzt "recht gute Privatsphäre") und ist eine Computeranwendung, die Ihrer elektronischen Post sowie anderen Daten eine Eigenschaft verleiht, die sie sonst nicht hätten: Vertraulichkeit.

Dies wird durch Verschlüsselung erreicht, so dass sie von keiner anderen als der berechtigten Person gelesen werden kann. Im verschlüsselten Zustand sieht die Nachricht aus wie ein bedeutungsloses Durcheinander zufälliger Buchstaben. PGP hat seine Fähigkeit bewiesen, sogar den ausgeklügeltesten Analyseversuchen zu widerstehen. PGP kann auch verwendet werden, um eine digitale Signatur anzubringen, ohne die Nachricht zu verschlüsseln. Diese Funktion wird z.B. in öffentlichen Newsbeiträgen verwendet, wo Sie nichts verstecken, was Sie zu sagen haben, sondern vielmehr Anderen erlauben wollen, Ihre Urheberschaft zu überprüfen. Wenn die digitale Signatur erst einmal erzeugt ist, kann praktisch niemand mehr die Nachricht oder die Signatur verändern, ohne dass PGP die Manipulation entdeckt. Während PGP leicht zu benutzen ist, hat es auch seine Tücken, Sie sollten sich mit den verschiedenen Optionen in PGP gründlich vertraut machen, bevor Sie es für den Versand wirklich ernster Nachrichten verwendest.

Nachfolgende Tabelle fast die Zusammenhänge zusammen.

Risiko	***Schutzmöglichkeit***
Emails, mitlesen durch Unbefugte	Verschlüsseln mit PGP
Das komplette Fälschen bzw. verfälschen von Emails oder anderen Daten, verfälschen des Urhebrechtes von Emails oder anderen Daten	Elektronisch unterschreiben mit PGP (signieren)

Wichtig zu erwähnen ist noch, das PGP intern unsymmetrisch und symmetrisch verschlüsselt. Wie das im Prinzip funktioniert wird unter 2.4 erläutert. Die gerade aktuellen PGP Verschlüsselungsstandardeinstellungen sind CAST mit 128 Bit Schlüssellänge (auch als CAST5 bekannt) für das symmetrische Verschlüsseln/ Entschlüsseln, sowie DH/DSS mit 2048/1024 Bit für das unsymmetrische Verschlüsseln/ Entschlüsseln.

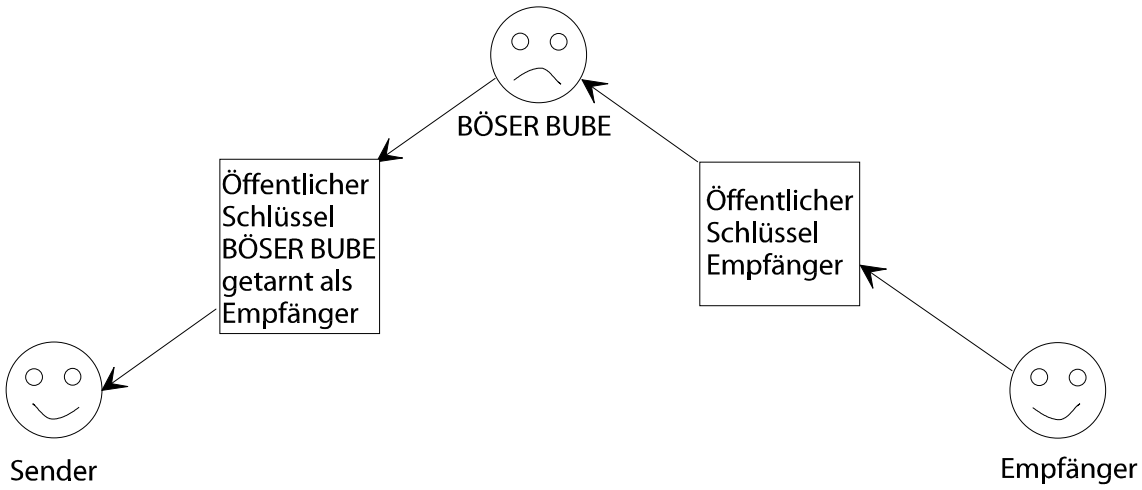
3.2 Welche Schwachstellen hat PGP

Wenn man davon ausgeht das die von PGP intern angewendeten Verschlüsselungsverfahren als „praktisch sicher“ zu betrachten sind, ist die Achillesferse von PGP die Schlüsselproblematik sowie die Anfälligkeit von MS Windows für Trojanerprogramme und Viren. Nachfolgend sind einige Angriffsmethoden beschrieben.

3.2.1 Angriff auf PGP durch „Mann in der Mitte“

PGP Angriff "Mann in der Mitte"

1. Sender möchte Empfänger eine geheime Nachricht senden
2. Der Empfänger versendet seinen öffentlichen Schlüssel zum Sender
3. Der "Böse Bube" fängt den öffentlichen Schlüssel des Empfängers ab
4. Der "Böse Bube" versendet seinen öffentlichen Schlüssel, getarnt als öffentlicher Schlüssel des Empfängers, zum Sender
5. Alle Nachrichten die der Sendern mit diesem Schlüssel verschlüsselt kann praktisch nur der "Böse Bube" lesen



Abwehr dieses Angriffs durch folgende Maßnahmen:

- Verwenden Sie öffentliche Schlüssel die zertifiziert sind. Prüfen Sie die elektronische Unterschrift der Zertifizierungsstelle. Man spricht in diesem Zusammenhang auch von einem „Trustcenter“

- Verwenden Sie öffentliche Schlüssel die vertrauensvolle Bekannte unterschrieben haben. Prüfen Sie die elektronischen Unterschriften Ihrer Bekannten. Man spricht in diesem Zusammenhang auch von einem „Web of Trust“

- Verwenden Sie öffentliche Schlüssel die Sie mit Bekannten auf Disketten austauschen. Fingerabdruck des Schlüssels prüfen ist notwendig. Man spricht in diesem Zusammenhang auch von einer „Schlüsselparty“

- Verwenden Sie öffentliche Schlüssel die Sie mit Bekannten via Schlüsselserver oder Email austauschen. Fingerabdruck des Schlüssels prüfen ist zwingend notwendig. Notfalls könnte man die Richtigkeit des Fingerabdrucks via Telefon oder FAX, aber auf keinen Fall via Email nachprüfen

- Damit Sie nicht in den Verdacht geraten mit dem „Bösen Buben“ gemeinsame Sache zu machen :

  UNTERSCHREIBEN SIE NICHT OHNE PRÜFUNG DIE ÖFFENTLICHEN SCHLÜSSEL ANDERER LEUTE !

3.2.2 Entwenden des privaten Schlüssels und der Passphrase

Stellen Sie sich vor aus Ihrem Büro wird Ihr PC mit einigen Unterlagen gestohlen. Da Sie, PGP verwenden ist Ihr Schlüsselpaar auf der Festplatte und (so wie ich) vergesslich sind steht die Passphrase (mit der Ihr privater Schlüssel geschützt ist) auf einem Zettel der am PC Bildschirm klebt. Der GAU ist damit in meinen Augen eingetreten. Der „Böse Bruder“ (Einbrecher seines Zeichens) kann dem „Bösen Buben“ Ihr Schlüsselpaar und die Passphrase aushändigen und dieser könnte Sie dann in Ihrem Namen im Internet so richtig auf die „Pauke hauen“. Die Folgen für Sie sind evtl. übelst z.B. Konto leer, Ruf geschädigt, sind durchaus möglich.

Die Abwehr dieses Angriffs ist durch folgende Maßnahmen zu erreichen:

- Wählen Sie die Passphrase so das diese erstens nicht zu erraten ist, und zweitens Sie diese gut im Kopf behalten können. Eine Methode dazu ist das man sich gut merkbare zusammengesetzte Wörter ausdenkt die aber eigentlich keinen Sinn ergeben zusammen mit mind. Zwei Sonderzeichen , wie z.B. „&Wurstbier/\“. Eine andere Methode wäre sich z.B. ein KFZ Kennzeichen zu merken was es bestimmt nicht real gibt, wie z.B. „XYA-FGK-4711“

- Wählen Sie Passphrasen die mind. 12 Zeichen lang sind (Wenn Sie kompatibel bleiben möchten mit „nicht deutschen“ PGP Versionen vermeiden Sie bitte deutsche Umlaute)

- NOTIEREN SIE SICH DIE PASSPHRASE AUF GAR KEINEN FALL !

- Im Falle eines Falles stellen Sie umgehend mit PGP eine Schlüssel-Rückrufurkunde aus. Leiten Sie diese Urkunde schnellstens an Ihre Zertifizierungsstelle, Schlüsselserver und an Bekannte die auch PGP nutzen

- Bei dienstlichem Gebrauch von PGP informieren Sie bitte umgehend unsere (zukünftige) Zertifizierungsstelle der ZI. Diese wird dann schnell geeignete Maßnahmen ergreifen

3.2.3 Gefälschte Zeitangaben bei elektronisch unterschriebenen Nachrichten

Ich denke zur Zeit ist PGP in Deutschland noch nicht reif um damit Vorgänge zu bearbeiten die zeitkritisch sind wie z.B. Verträge bei denen es u.a. auf das Datum der Unterschrift ankommt. In meinen Augen ist man da bei einem Notar momentan noch am besten aufgehoben, bzw. dieser sollte mindestens mit seiner elektronischen Unterschrift die aktuelle Zeitangabe bestätigen. In Zukunft wird es aber sicherlich auch in Deutschland Zeitstempeldienste wie z.B. http://www.itconsult.co.uk/stamper.htm für PGP geben.

3.2.4 Indirekte Angriffe

Nachfolgend sind einige Angriffsarten aufgeführt die PGP zwar nicht direkt verhindern kann, aber bei „richtiger“ Anwendung von PGP werden evtl. die Schäden vermindert.

- Trojaner Programme
- Mitlesen der Eingaben durch HF-Empfänger
- Ungenügend gelöschte Daten auf Datenträger

3.3 Die Verteilung öffentlicher Schlüssel sowie Möglichkeiten deren Authentizität sicherzustellen

Damit Sie mit PGP zum elektronischen Unterschreiben und Verschlüsseln anwenden können, müssen Sie und der Empfänger Ihrer Nachricht die jeweils Öffentlichen Schlüssel der „Gegenseite" besitzen.

Der Dreh- und Angelpunkt einer „sicheren" elektronischen Unterschrift und Verschlüsselung ist dabei die Eindeutigkeit und Authentizität der verwendeten öffentlichen Schlüssel. Die Schlüsselverwaltung von PGP ist dezentral ausgerichtet, es bedarf im Prinzip keiner Einrichtung, die die Gültigkeit der Schlüssel bestätigt. Der PGP Anwender sollte deshalb selber für die Richtigkeit „seiner Sammlung" öffentlicher Schlüssel sorgen. Nachfolgend sind einige Möglichkeiten aufgeführt dieses zu bewerkstelligen.

3.3.1 Möglichkeiten zum Austausch öffentlicher Schlüssel

Medium	***„Gute Sicherheit" durch***	***„Weniger gute Sicherheit" durch***
Öffentlicher Schlüsselserver Email Homepage im WWW FTP Datenträger (z.B. Diskette) übergeben durch dritte Person	Schlüssel sind zertifiziert und vor dem Gebrauch wird das Zertifikat überprüft	Schlüssel sind durch vertrauensvolle Bekannte signiert und deren elektronische Unterschrift wird vor dem Gebrauch überprüft Schlüsseleigenschaften (Benutzer ID, Fingerabdruck, Verfahren usw.) werden vor dem Gebrauch überprüft. Die Vergleichsdaten zur Überprüfung sollten nicht über das gleiche Medium erhalten werden, z.B. ein Schlüssel und der zugehörige Fingerabdruck via Email sind nicht sicher !
Datenträger (z.B. Diskette) persönlich übergeben	Schlüsseleigenschaften (Benutzer ID, Fingerabdruck, Verfahren usw.) werden vor dem Gebrauch überprüft. Die Vergleichsdaten sollten sich die Partner auf Papier notieren	

Sie sehen das es viele Möglichkeiten gibt öffentliche Schlüssel auszutauschen. Wichtig dabei ist nur das Sie die Richtigkeit der erhaltenen Schlüssel vor dem Gebrauch überprüfen. Eine Überprüfung mittels Zertifikate oder elektronische Unterschriften von Bekannten bedingt die Verfügbarkeit der öffentlichen Schlüssel der Unterzeichner. Wenn eine Überprüfung via Schlüsseleigenschaften stattfinden soll, empfiehlt es sich über einen „nicht digitalen Kommunikationskanal" (Telefon, FAX, SMail usw.) die Vergleichdaten einzuholen.

Beispiel: Sie erhalten den öffentlichen Schlüssel von Lieschen Meier via Email. Elektronisch Unterschrieben ist dieser Schlüssel von Ihrem guten Freund Hänschen Klein. Sie benötigen den öffentlichen Schlüssel von Hänschen Klein um dessen Signatur des Schlüssels von Lieschen zu prüfen. Als (nicht so gute) Alternative könnten Sie persönlich Lieschen Meier anrufen und fernmündlich die via Email erhaltenen Schlüsseleigenschaften verlesen, Lieschen Meier kann dann mündlich Kundtun ob die Schlüsseleigenschaften im allgemeinen und im besonderen der Fingerabdruck „richtig" sind.

3.3.2 Zertifizierungsstellen

Für die kommerzielle bzw. dienstliche Anwendung muss es eine oder mehrere zentrale Einrichtungen geben, die zweifelsfrei bestätigen können, dass ein Schlüssel echt ist. Genauso stellt sich das Problem für den Privatanwender, wenn er mit jemand sicher kommunizieren will, den er nie zuvor gesehen hat, wenn er niemand kennt, der vertrauenswürdig den Schlüssel des Unbekannten beglaubigt hätte.

Deswegen gibt es zentrale Zertifizierungsstellen, sogenannte TrustCenter oder Certificate Authorities (CA). Das sind manchmal Firmen, oft aber auch gemeinnützige Einrichtungen wie Universitäten und sogar einige Bürgernetze. Damit diese Stellen überhaupt arbeiten können bietet PGP die Möglichkeit auch öffentliche Schlüssel digital zu Unterschreiben (signieren).

Um seinen öffentlichen Schlüssel zertifizieren zu lassen muss man bei einer Zertifizierungsstelle persönlich vorstellig werden und mit Personalausweis oder Reisepass seine Identität belegen. Man bringt dabei seinen PGP-Schlüssel auf Diskette mit. Die Zertifizierungsstelle signiert daraufhin den PGP-Schlüssel mit ihrem öffentlichen Schlüssel und bestätigt so dessen Echtheit. Eine andere Möglichkeit, speziell für unsere FH (eine sozusagen „Rundum glücklich Benutzerbetreuung“) wäre, dass ein Mitarbeiter der Zertifizierungsstelle Ihnen „Ihr Schlüsselpaar“ auf einem Laptop PC generiert und auf Ihren PC aufspielt.

Die öffentlichen Schlüssel der Zertifizierungsstellen sind allgemein verfügbar; wenn man einen signierten öffentlichen Schlüssel bekommt, weiß man sicher, dass der Schlüssel echt ist und es die betreffende Person wirklich gibt, sowie dass die angegebene Mailadresse wirklich der Person gehört.

Die öffentlichen Schlüssel der Zertifizierungsstellen kann man von deren Seiten im Internet herunterladen. Sie sollten das sofort tun nachdem Sie PGP installiert haben.

Liste einiger deutschen Zertifizierungsstellen:

- Certification Authority IuK NRW
  http://www.iuk-nrw.de/
- Die Zertifizierungsinstanz für das deutsche Forschungsnetz
  http://www.pca.dfn.de/dfnpca/
- Arbeitsgruppe Zertifikationsinfrastruktur
  http://www.in-ca.individual.net/
- Zertifizierungsstelle der DLRG
  http://www.dlrg.de/Service/CA/
- TC TrustCenter GmbH
  http://www.trustcenter.de/
- Zertifizierungsstelle der UNI Münster
  http://www.uni-muenster.de/ZIV/PGP

Die Verteilung zertifizierter öffentlicher Schlüssel gestaltet sich sehr einfach. Da ein Zertifikat (praktisch) nicht gefälscht werden kann, dürfen hier auch „unsichere Verteilungswege“ (z.B. unverschlüsselte Email) in betracht gezogen werden. Wichtig ist nur dass diese öffentlichen Schlüssel vor dem Gebrauch anhand Ihrer Signaturen überprüft werden.

Ich denke dass wir an unserer Fachhochschule in Zukunft eine eigene Zertifizierungsstelle mit zugehörigem Schlüsselserver haben werden. Das ist jedoch noch Zukunftsmusik, bis es diese Einrichtung gibt empfiehlt sich nachfolgende Methode.

3.3.3 Schlüsselpartys

Eine gute und Gelegenheit zum gegenseitigen Austausch der öffentlichen Schlüssel bieten dienstliche und private Treffen. Dazu notiert sich jeder Teilnehmer folgende Daten über seinen PGP-Schlüssel auf ein Blatt Papier, das er mitbringt:

- Name
- Vorname
- Email-Adresse
- Art des Schlüssels (RSA oder DH/DSS)
- Erstellungsdatum des Schlüssels
- Verfallsdatum des Schlüssels
- Fingerabdruck („fingerprint“) des Schlüssels am besten in hexadezimal Form

Außerdem benötigt jeder Teilnehmer seinen öffentlichen Schlüssel auf einer sonst leeren Diskette.

Auf dem Treffen liest jeder der Anwesenden diese Angaben zu seinem Schlüssel vor. Wenn sich nicht alle Anwesenden persönlich kennen, zeigt jeder außerdem seinen Personalausweis vor, so dass seine Identität eindeutig ist. Alle Teilnehmer notieren sich die vorgelesenen Angaben.

Danach werden die öffentlichen Schlüssel der Teilnehmer von Diskette in ein leeres PC Unterverzeichnis geschrieben. Sind alle Schlüssel in diesem Verzeichnis schreibt man dieses „gesammelten Werke“ zurück auf die einzelnen Disketten der Teilnehmer.

Nach dem Treffen, am eigenen PC werden die Schlüsseldaten von Diskette nach PGP importiert. Danach ist es zwingend erforderlich diese Schlüssel selber zu signieren und die digitalen Angaben (besonders die digitalen Fingerabdrücke der Schlüssel) mit den schriftlichen Angaben zu vergleichen.

Alternativ besteht noch die Möglichkeit den Kopiervorgang zu vereinfachen in dem man statt der Diskette öffentliche Schlüsselserver benutz. Hierbei muss man aber noch sorgfältiger die Papierform mit den digitalen Daten vergleichen.

Liste einiger öffentlicher Schlüsselserver:

- PGP-Public-Keyserver des MIT
  http://pgpkeys.mit.edu:11371/

- PGP-Public-Keyserver der UniGH Paderborn
  http://math-www.uni-paderborn.de/pgp/

- JoGuNET PGP Public Key Server
  http://pgp.zdv.Uni-Mainz.DE/keyserver/

3.3.4 Das Netz des Vertauens (The web of trust)

Eine sehr gute Möglichkeit zur Überprüfung von öffentlichen Schlüsseln ist das „Netz des Vertrauens". Man kann Sich dieses Netz durchaus als „dezentrale Zertifizierungstelle" vorstellen. Und das funktioniert wie folgt:

Für jeden selbst signierten öffentlichen Schlüssel eines Bekannten vergeben Sie eine Vertrauensstufe. Damit legen Sie fest in wieweit Sie dem Bekannten vertrauen was die Überprüfung der Echtheit der öffentlichen Schlüssel von dritten Personen angeht.

Es gibt drei Stufen des Vertauens:

- Volles Vertrauen
- Eingeschränktes Vertrauen
- Kein Vertrauen

Wenn Sie nun einen neuen öffentlichen Schlüssel von einer dritten Person erhalten der von Ihrem Bekannten elektronisch Unterschrieben (signiert) wurde prüft PGP die Brauchbarkeit dieses Schlüssels wie folgt:

Vertauensgrad	***Einfluss auf Gültigkeit des neuen öffentl. Schlüssel***
Volles Vertrauen zum Bekannten	Der neue öffentliche Schlüssel ist auch für Sie gültig
Eingeschränktes Vertrauen zum Bekannten	Der neue öffentliche Schlüssel ist erst dann gültig wenn noch mindestens ein weiterer Bekannter mit eingeschränkten Vertrauen diesen Schlüssel unterschrieben hat
Kein Vertrauen zum Bekannten	Der neue öffentliche Schlüssel ist erst dann gültig wenn noch mindestens zwei weiterer Bekannte mit eingeschränkten Vertrauen oder ein Bekannter mit vollem Vertrauen diesen Schlüssel unterschrieben haben

Zu Beachten ist das die Vertrauensstufen von jedem Nutzer selbst festgelegt werden. Das hat evtl. zur Folge dass der gleiche öffentliche Schlüssel für Nutzer „A" als brauchbar angesehen wird, von Nutzer „B" aber nicht mehr. Das liegt dann daran das Nutzer „B" ein anderes Vertrauensverhältnis zu den Unterzeichnern des Schlüssels hat. Nach meinem persönlichen Dafürhalten ist dies der Grund warum „Das Netz des Vertrauens" für die dienstliche Anwendung von PGP eher nicht so gut geeignet ist.

3.4 Was PGP gut kann

Es ist nun für Sie kein Geheimnis mehr, das PGP folgende Punkte „gut“ erfüllt:

- Verschlüsseln von Daten für andere Personen
- Entschlüsseln von Daten anderer Personen
- Unterzeichnen von Daten mit Ihrer elektronischen Unterschrift, damit andere Personen prüfen können dass Sie der Unterzeichner sind
- Überprüfen elektronischer Unterschriften anderer Personen
- Schlüsselpaare verwalten

3.5 Was PGP nicht so gut kann

Wenn man „nur“ für den „Eigengebrauch“ ganze Verzeichnisstrukturen mit vielen Dateien verschlüsseln will, ist es dieses mit den „neuen und freien PGP Varianten“ für Windows nur sehr unkomfortabel; d.h. nur manuell in dem man jede Datei einzeln verschlüsselt/entschlüsselt, möglich.
In diesem Fall wäre die besserer Lösung das für den privaten Gebrauch freie Produkt „Scramdisk“ welches ganze Festplatteninhalte auf einmal verschlüsselt, und nach einmaliger Eingabe eines Passwortes wieder freigibt. Das verschlüsseln bzw. entschlüsseln geschieht bei diesem Produkt im Hintergrund, ohne das der Anwender sein Passwort bei jeder „angepackten“ Datei erneut eingeben muss. Sramdisk ist erhältlich unter:

- http://www.scramdisk.clara.net/

3.6 Allgemeine Hinweise zur Nutzung PGP

- Verwenden Sie PGP richtig ! Den nichts ist schlechter für Ihre Datensicherheit als ein „gutes Programm" unbedarft und somit evtl. „schlecht" zu benutzen. Die Gefahr die daraus erwächst ist vergleichbar mit der eines Bergsteigers der nur denkt sein Sicherungshaken wäre „gut" angebracht. In diese Fällen wären Sie mit Ihrer Datensicherheit und der Bergsteiger mit seiner „Klettersicherheit" besser gestellt wenn keine „schlecht" angewendeten Sicherheitsmechanismen Sicherheit vorgaukeln würden

- Machen Sie sich mit dem PGP System spielerisch vertraut bevor Sie „wichtige" Daten verschlüsseln

- Kein Verschlüsselungssystem ist für alle Zeit als Sicher anzusehen. Der Schöpfer von PGP, Zimmermanns bemerkt in der Anleitung zu PGP 2.6.2 dazu: „*Ich bin von der Sicherheit von PGP nicht so überzeugt, wie während meines Studiums von der Sicherheit meines "genialen" Verschlüsselungsverfahrens. Wäre ich von PGP vollkommen überzeugt, wäre das ein schlechtes Zeichen. Aber ich bin ziemlich sicher, daß PGP keine ins Auge springenden Schwachstellen hat. Die Algorithmen, die in PGP verwendet werden, stammen von zivilen Kryptographen mit sehr gutem Ruf, und sie sind eingehend untersucht worden. Selbstverständlich ist der komplette Sourcecode erhältlich, so daß jeder, der programmieren kann (oder eine vertrauenswürdige Bekannte hat, die dazu in der Lage ist), das System durchleuchten kann. Der Quellcode ist über Jahre professionell entwickelt worden. Im übrigen arbeite ich nicht für die NSA. Ich hoffe, daß der Schritt, Vertrauen in PGP zu gewinnen, nicht zu viel Überwindung kostet.*"

- Falls Sie mal in die Gelegenheit kommen sollten PGP als rein symmetrisches Verfahren anwenden zu wollen, müssen Sie der Empfängerseite einen „geheimen Schlüssel" zusenden. Verwenden als „geheimen Schlüssel" **nie** Ihre PGP Pasphrase !

- Vergessen Sie ihre Pasphrase nicht

- Verlegen Sie ihren privaten Schlüsselbund nicht. D.h. dieser sollte nicht nur auf Ihrer PC Festplatte, sonder auch als Kopie auf einer sicher verschlossenen Diskette befinden

3.7 Was ist bei der Nutzung von PGP für Windows zu beachten ?

- PGP für Windows ist nur für private und gemeinnützige Anwendungen „Freeware". Die kostenlose Nutzung ist daher nur erlaubt für private und nicht kommerzielle Zwecke. Für alle anderen Verwendungszwecke muss PGP für Windows lizenziert werden, das gilt nach meinem Dafürhalten auch für eine dienstliche Nutzung an unserer Fachhochschule

- Benutzen Sie wenn möglich PGP Versionen die eine deutsche Benutzeroberfläche haben und „internationalen" Verschlüsselungsstandard bieten. Den „internationalen Standard" erkennt man am „i" im der Installationsdatei. (z.B. PGP6.5.1**i**.zip)

Bemerkung: In meinen Augen ist angebracht dass Sie die internationale Version von PGP verwenden. Diese unterliegt den US amerikanischen Exportbeschränkungen die vorschreiben das Verschlüsselungsprodukte entweder eine - für Profis leicht „knackbare" - Schlüssellängen besitzen oder es muss oder, falls „stärkere" Schlüssel eingesetzt werden, eine für US Regierungsstellen „offene Hintertüre" in die Produkte eingebaut werden. Aus diesem Grunde sollte man auch den eigenen Verschlüsselungsverfahren von Netscape bzw. Mircosoftprodukten (z.B. Comminicator, IE usw.) kritisch gegenüberstehen.

4.PGP - Installation auf MS Windows Rechnern

4.1 Download der „richtigen“ Installationsdatei

Unter http://www.pgpi.org finden Sie die relevanten Softwarepakete für Ihren PC um PGP sowie diverse PGP Werkzeuge installieren zu können. Wenn möglich „downloaden“ Sie sich die aktuellste deutsche PGPi – das „i“ steht für international – Version in das Verzeichnis Ihrer Wahl. Für Windows 95/98/NT heißt die aktuelle „i“ Version PGP 6.5.1i. (Stand 15.01.2001) Beachten Sie bitte das für Windows 2000 spezielle Versionen erforderlich sind die natürlich auch auf obigen Server, aber in einem anderen Verzeichnis, zu finden sind.

4.2 Installation starten und PGP Grundeinstellungen vornehmen

Klicken Sie am besten via Explorer die heruntergeladene *.EXE Datei. Bei Windows NT bzw. Windows 2000 ist es zwingend erforderlich das Sie für diesen Vorgang Administrator Rechte besitzen.

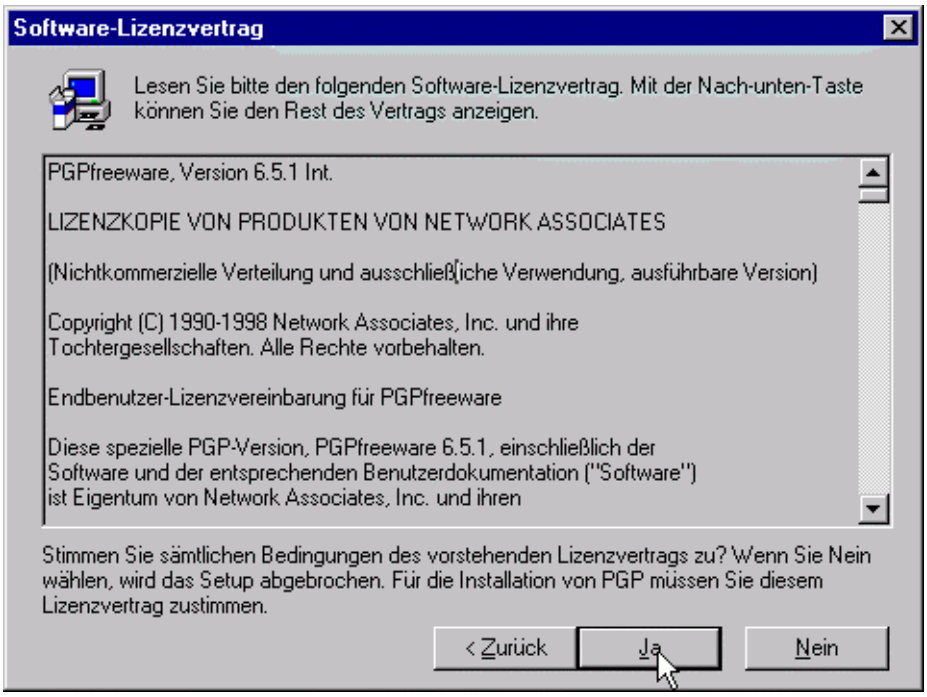
Wenn Sie sich für eine „deutsche Version“ von PGP entschieden haben erscheinen nacheinander, während des Installationsvorgangs nachfolgende folgende Bildschirmmasken.



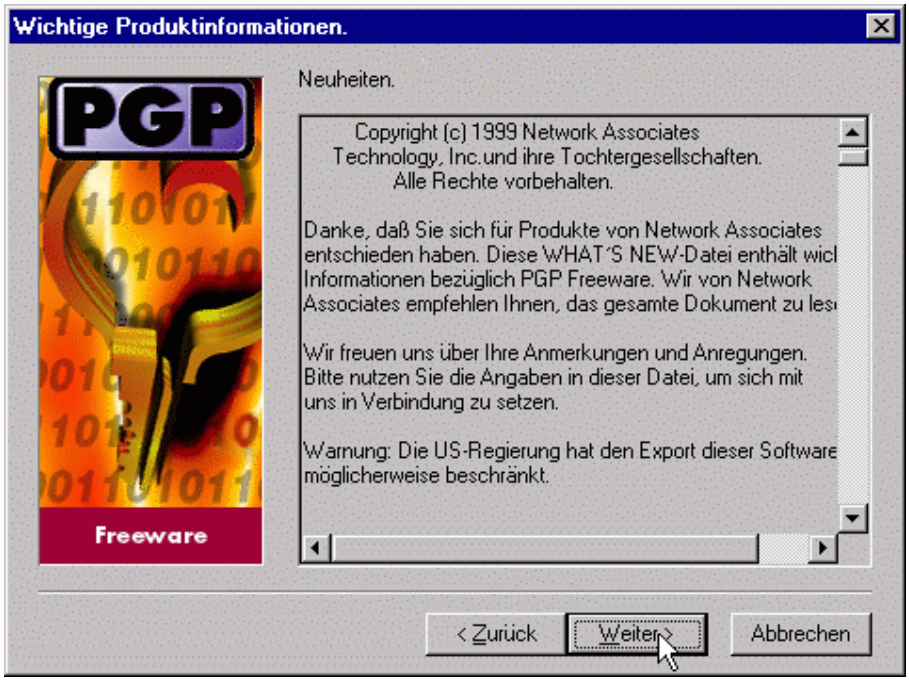
a) Diese Maske zeigt an dass die Programmdateien sich gerade selbst entpacken.



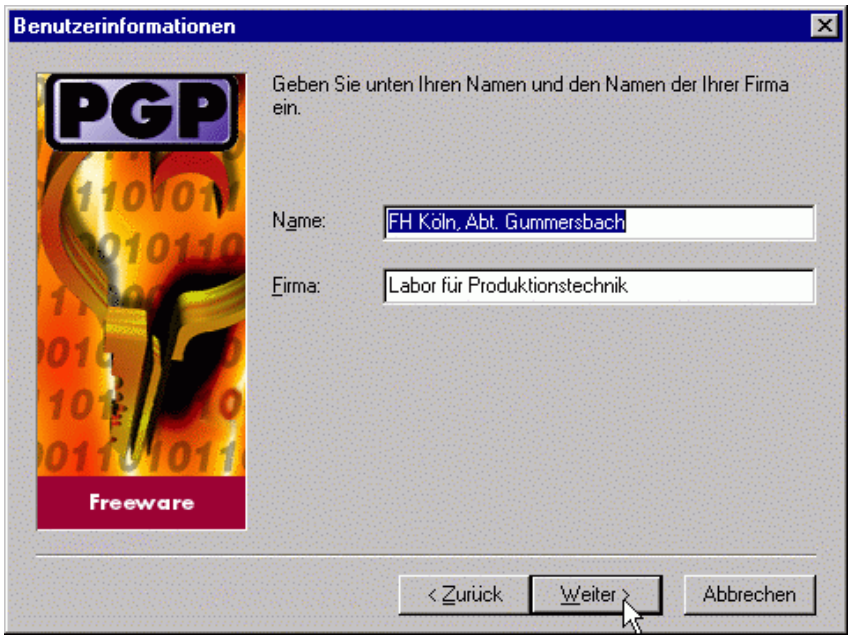
b) Hier werden Sie aufgefordert die eigentliche Installation von PGP auf Ihrem System zu starten.



c) Danach erfolgt die Darstellung des PGP Lizenzvertrages. Als Erstanwender sollten Sie sich Zeit nehmen um diesen Lizenzvertrag durchzulesen. Bei Unklarheiten scheuen Sie sich nicht die Fachleute der ZI um Rat zu fragen.



d) An dieser Stelle werden weitere PGP Produktinformationen vorgestellt. Die Warnung vor den Exportbeschränkungen dieses PGP Produktes durch die US-Regierung erfolgt, weil hier eine internationale PGP Version installiert wird.



e) Hier können Sie Ihre Dienststelle und das Labor eintragen.



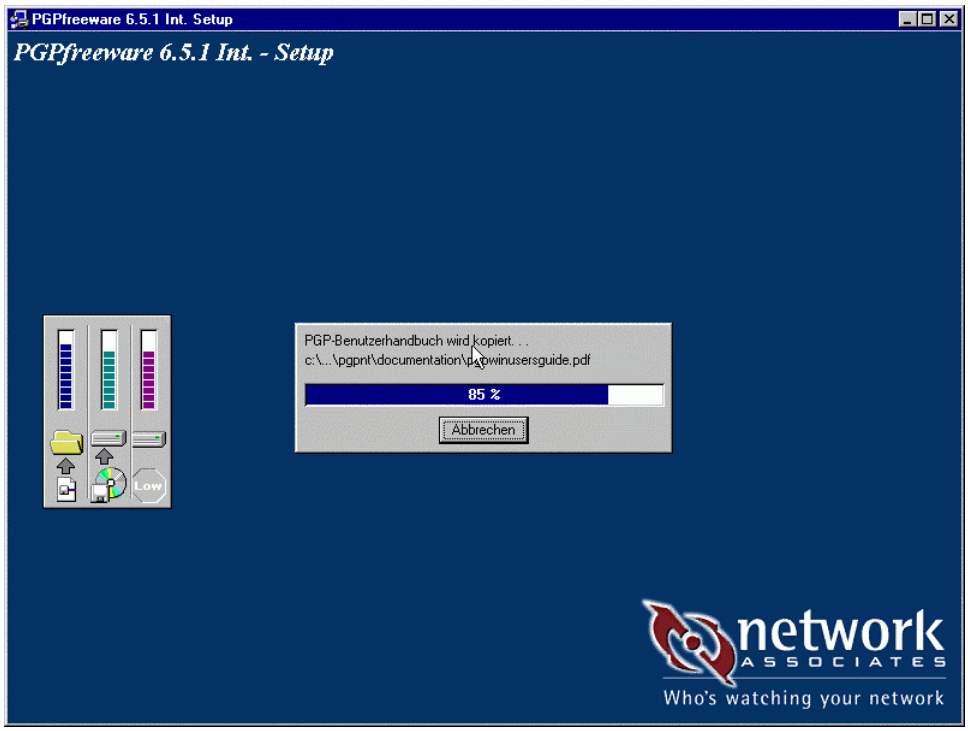
f) An dieser Stelle wird das Installationsverzeichnis von PGP aufgezeigt. „C:\...\Network Associates\PGPNT“ heist „richtig“ „C:\Programme\Network Associates\PGPNT“. Wenn Ihnen dieser Pfad nicht gefällt steht es Ihnen frei über [Durchsuchen] ein anderes Verzeichnis anzugeben. Ich persönlich habe mir angewöhnt diese Pfade nicht zu ändern um evtl. spätere „Updates“ eines Softwarepaketes zu erleichtern.



g) Eine der wichtigsten Stellen der Installation ist die Auswahl der PGP Komponenten. Suchen Sie hier besonders nach einem „PGP Plugin“ (d.h. PGP Erweiterung) für Ihr Emailprogramm. Die Auswahl der PGP Dokumentation erscheint mir auch sinnvoll. Wenn Ihr Email Programm hier nicht aufgeführt sein sollte erhalten Sie in Kap. 4.4 weitere Informationen.



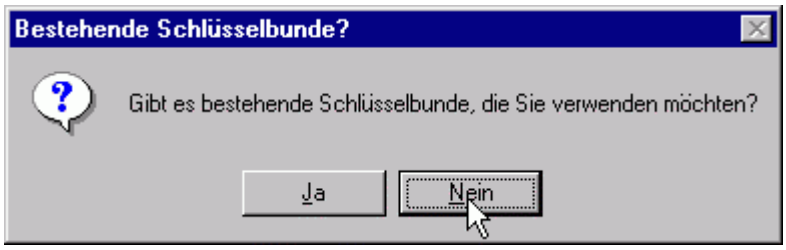
h) Vor dem eigentlichen kopieren der PGP Programmdateien erhalten Sie die Möglichkeit zu überprüfen ob das, was PGP an Komponenten installieren möchte mit Ihren Vorstellungen übereinstimmt. Wenn Komponenten fehlen sollten betätigen Sie bitte den **<Zurück** Knopf um das Fehlende nachzutragen.



i) Der eigentliche Installationsvorgang wird in diesem Fenster dargestellt.



j) Falls Sie sich in obiger Komponentenauswahl auch für PGPNet entschieden haben, möchte „PGP Install" nun von Ihnen wissen mit welchem Netzwerkadapter es zusammenarbeiten soll. Bemerkung: PGPNet hat nichts mit direkter Verschlüsselung von Dateien bzw. Email zu tun, sondern bietet die Möglichkeit auf Netzwerkprotokollebene den Datenaustausch zu einem anderen PC zu verschlüsselt. In meinen Augen eine gute Sache, ich möchte aber hier an dieser Stelle nicht weiter darauf eingehen.



k) Wenn dies nicht Ihre erste PGP Installation sein sollte, kann an dieser Stelle an Datenträger mit bestehenden Schlüsselbunden „eingespielt“ werden.

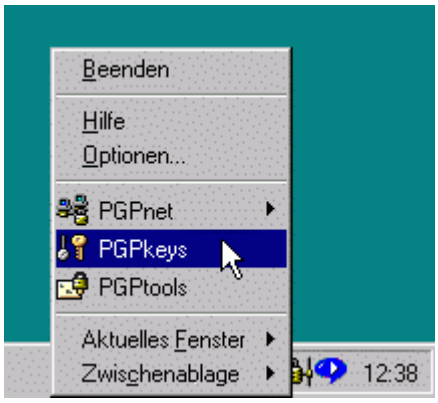


l) Die PGP Installation ist nun fast abgeschlossen, allerdings ist noch ein Neustart des PC von notwendig. Dieser Neustart kann von hier aus getätigt werden.

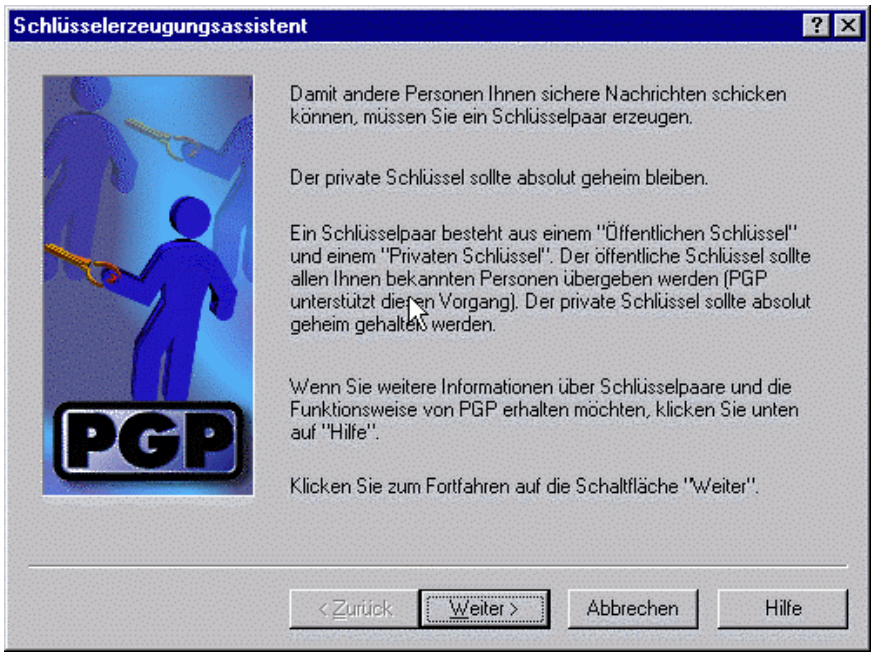
4.3 PGP Kohnfiguryen



a) Nach dem Neustart des PC - Windows NT/2000 Nutzer sollten dabei mit Ihrem „normalen“ Benutzernamen anmelden – erscheint nun im Tray (d.h. Tablett) zusätzlich zu den gewohnten Icons ein symbolisiertes Vorhängeschloss. Über Symbol sind alle wesentlichen PGP Funktionen ansprechbar.



b) Bewegen Sie bitte den Mauszeiger über das „Vorhängeschloss“ und betätigen Sie dann die linke Maustaste. Es sollte dann obiges Auswahlmenü öffnen. Da PGP in der praktischen Anwendung im wesentlichen auf vorhandenen Schlüsseln aufbaut, empfiehlt es sich als erste Funktion die PGP Schlüsselverwaltung (PGPKeys) auf zu rufen. Das Aufrufen der von PGPKeys geschieht in dem Sie den Mauszeiger über den Menüpunkt PGPKeys führen und die linke Maustaste erneut betätigen.



c) PGPKey bemerkt beim ersten Aufruf dass Sie noch kein Schlüsselpaar besitzen. Sie werden im folgenden aufgefordert PGP mitzuteilen welches Schlüsselpaar es für Sie anlegen soll. Betätigen Sie zunächst bitte den **Weiter>** Knopf.



d) Eine wesentliche Angabe für Ihr neues Schlüsselpaar ist Ihr Name und Ihre Email Adresse. PGP leitet daraus Ihre Benutzer ID ab, d.h. PGP ist dadurch in der Lage verschlüsselte Email bzw. andere Daten den „richtigen" Schlüsseln zuzuordnen.



e) An dieser Stelle entscheiden Sie, mit welchem Verfahren Sie arbeiten wollen. Standard bei der hier vorgestellten Version ist DH/DSS. In erster Näherung ist dieser Schlüsseltyp meiner Ansicht nach die richtige Wahl. Es ist aber nicht ausgeschlossen das in Zukunft an unserer Fachhochschule RSA eingesetzt wird.



f) Ein weiteres wichtiges Merkmal für Ihren Schlüsselbund sind die Schlüssellängen. Hier ist abzuwägen zwischen der angestrebten Sicherheit, der Bearbeitungsgeschwindigkeit und evtl. angestrebte Kompatibilität mit älteren PGP Versionen. Als Faustregel gilt, je länger die Schlüssellänge „desto besser" die Sicherheit aber auch „desto schlechter" die Arbeitsgeschwindigkeit von PGP. Darüber hinaus könnte es bei ganz großen Schlüssellängen (z.B. von 4096 Bit) Schwierigkeiten bei der Verwendung dieser Schlüssel im Zusammenhang mit älteren PGP Versionen geben. Deshalb ist in meinen Augen die Voreinstellung für DH/DSS - ein Schlüsselpaar von 2048/1024 Bit Länge – die beste Wahl.



g) Bei dieser Einstellung können Sie angeben bis zu welchem Datum Ihr Schlüsselpaar gültig sein soll. In erster Näherung ist es richtig die Gültigkeit nicht zu beschränken. Aber auch hier gilt dass in der Zukunft evtl. eine Gültigkeitsdauer für die dienstliche angewendeten Schlüsselpaare fest gelegt wird.



h) Bemerken Sie die von mir gemachten Fehler, die Sie bei der Eingabe Ihrer Passphrase (man sagt auch Mantra dazu) nicht wiederholen sollten ?

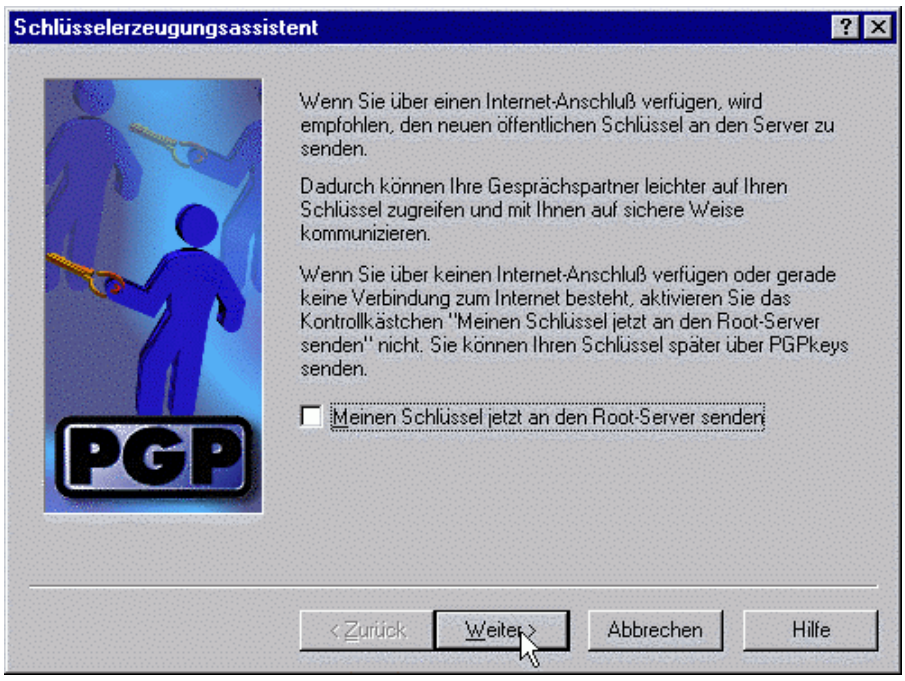
- Zum einen habe ich die Eingabe meines Mantras nicht verborgen, jeder der mir bei der Eingabe über die Schulter schaut kann es leicht mitlesen

- Zum anderen denke ich das die Passphrase „PGP Schulung“ zu simpel, und damit evtl. zu leicht zu erraten ist

- Bitte denken Sie eine weile über die Qualität Ihrer Passphrase nach. Sie sollte auf jeden Fall für Sie leicht zu merken sein, und dennoch für anderer Leute nicht erratbar sein. Wählen Sie die Passphrase so das diese erstens nicht zu erraten ist, und zweitens Sie diese gut im Kopf behalten können. Eine Methode dazu ist das man sich gut merkbare zusammengesetzte Wörter ausdenkt die aber eigentlich keinen Sinn ergeben zusammen mit mind. Zwei Sonderzeichen , wie z.B. „&Wurstbier/\“. Eine andere Methode wäre sich z.B. ein KFZ Kennzeichen zu merken was es bestimmt nicht real gibt, wie z.B. „XYA-FGK-4711“



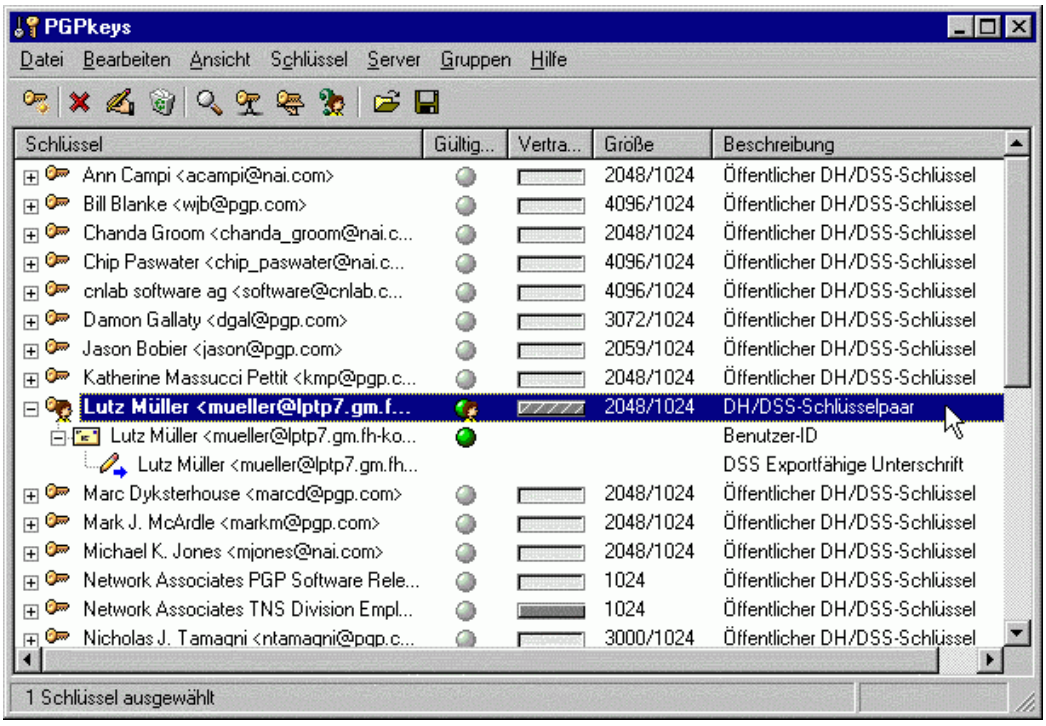
i) PGP benötigt nun, je nach Rechnerkonfiguration, einige Zeit zum Berechnen Ihres Schlüsselpaar. Es werden dabei intern sehr große Primzahlen „berechnet“, um als Grundlage dieses Schlüsselpaars zu dienen.



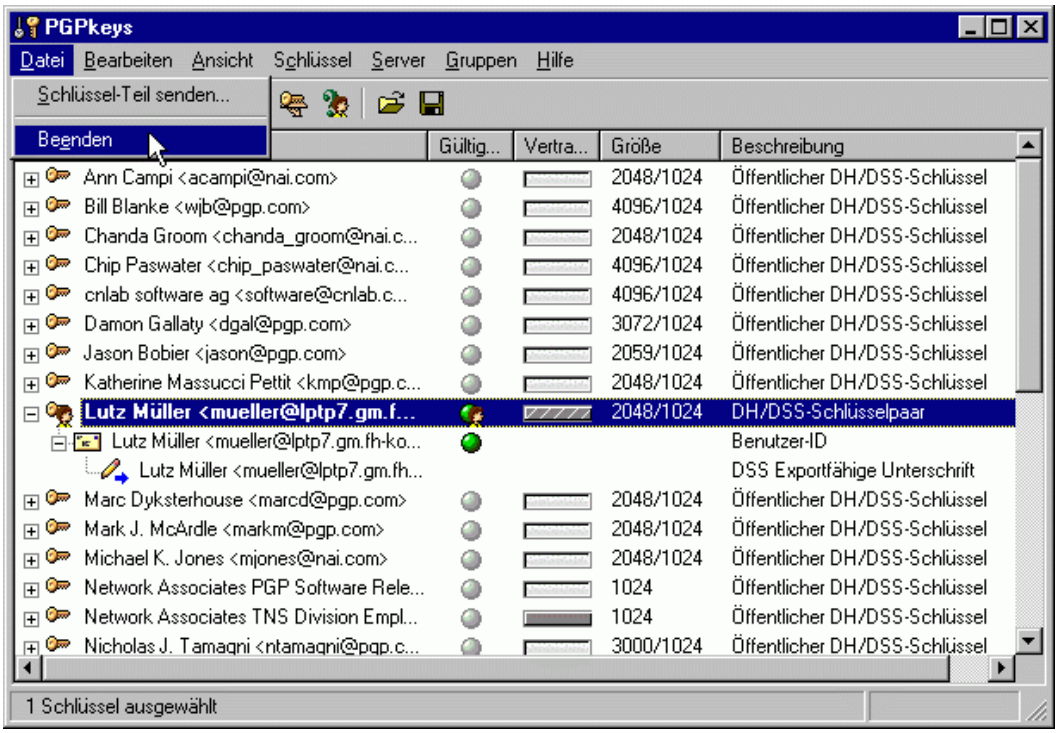
j) Nun gut !? Ich persönlich empfinde diese Möglichkeit, nämlich Ihren öffentlichen Schlüssel direkt nach der Generierung an einen öffentlichen Server zu senden, als verfrüht. Ihr Schlüssel ist bis jetzt weder von einer Zertifizierungsstelle noch von vertrauensvollen Bekannten elektronisch Unterschrieben worden. Daraus folgt dass der Nutzwert Ihres öffentlichen Schlüssel für andere PGP Nutzer eher gering sein wird.



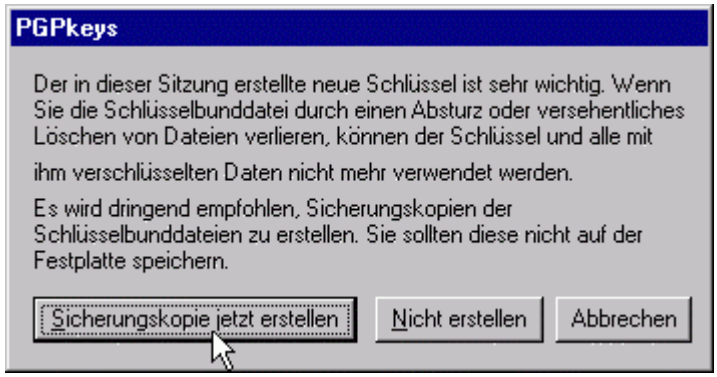
k) Dem kann ich mich nur anschließen. Eine weitere Hürde auf dem Weg zur Nutzung von PGP wurde von Ihnen überwunden.



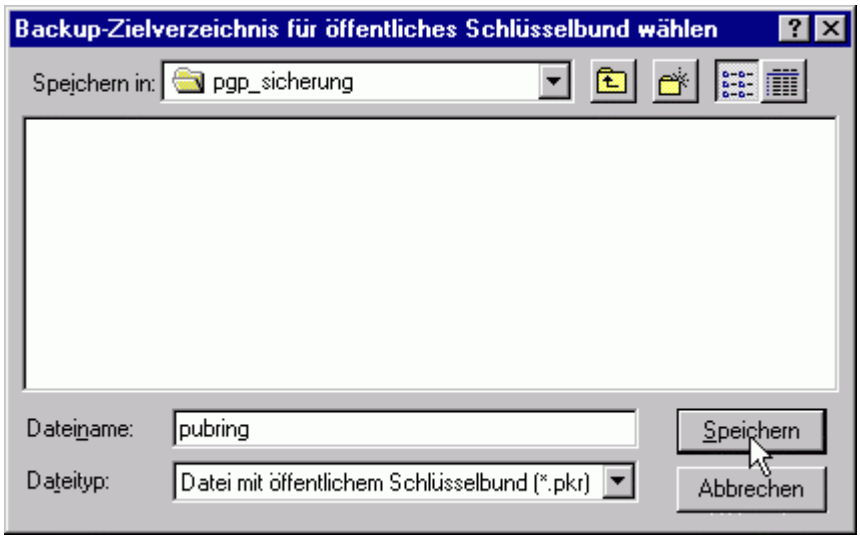
l) Ihr DH/DSS Schlüsselpaar, erkennbar an dem Symbol ist in eine Liste von öffentlichen Schlüsseln eingetragen worden. Ob Sie diese öffentlichen Schlüssel beibehalten, oder mit dem Symbol löschen ist eher eine Frage Ihres Geschmacks.



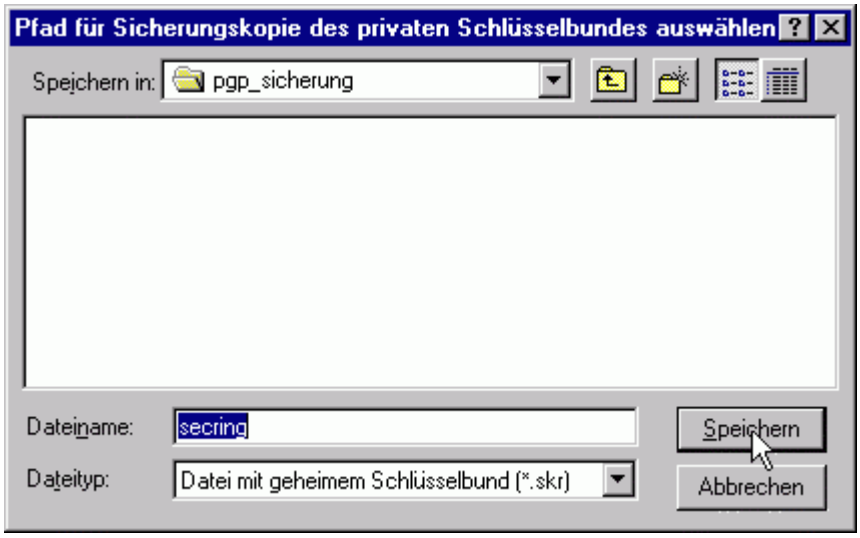
m) Nun da Sie Ihr Schlüsselpaar besitzen kann das Programm „PGPKeys“ zunächst einmal beendet werden.



n) „PGPKeys“ erkennt das noch keine Sicherungskopie Ihres Schlüsselpaars besteht, und fordert Sie mit diesem Fenster auf eine Sicherungskopie zu erstellen. Eine, nach meinem Empfinden, sehr vernünftige Maßnahme.



p) Die öffentlichen Schlüssel die das System kennt werden in das Verzeichnis „pgp_sicherung“ geschrieben. Eine Sicherung auf Diskette erscheint mir hier noch sinnvoller.



q) Die privaten (und geheimen) Schlüssel die das System kennt werden in das Verzeichnis „pgp_sicherung“ geschrieben. Eine Sicherung auf Diskette erscheint mir hier noch sinnvoller.

4.4 PGP Erweiterung für verschiedene Email Programme

PGP arbeitet mit vielen Email Programmen via „Plugin“ sehr gut zusammen. Nachfolgend eine Liste von bekannten Email Programmen und die zur Verfügung stehen Erweiterungen. Beachten Sie bitte dass die Angaben für die PGP Version 6.5.1i unter Windows 9x/NT gelten.

Produkt	***Erweiterung***
AK Mail	Im Email Programm integriert
Clypso	http://www.mcsdallas.com/mcs/calypso/
Eudora	Bestandteil der PGP Installation
Lotos Notes	Bestandteil der PGP Installation
MS Exchange	Bestandteil der PGP Installation
MS Outlook 97/98/2000	Bestandteil der PGP Installation
MS Outlook Express	Bestandteil der PGP Installation
Netscape Messenger	Zur Zeit „offiziell“ nicht verfügbar weil Netscape einen anderen Verschlüsselungsstandard bevorzugt, bekannt als S/MIME, der nicht mit PGP kompatibel ist. Eine „beta – Version“ liegt unter http://bear-software.freeservers.com/downloads.html zum „download“ bereit. Beachten Sie bitte dass kein Quelltext zu dieser Anwendung veröffentlicht wird, die „sichere“ Nutzung dieses Produkts ist eine Frage des Vertrauens.
Pegasus Mail	http://community.wow.net/grt/qdpgp.html
The Bat	Im Email Programm integriert

Sie sehen das die meisten Email Programme PGP unterstützen. Die konkrete Anwendung dieser Erweiterungen kann allerdings nicht - aufgrund der Vielfalt der Produkte – Bestandteil dieser Mitarbeiterschulung sein.

5.PGP - Anwendung auf MS Windows Rechnern

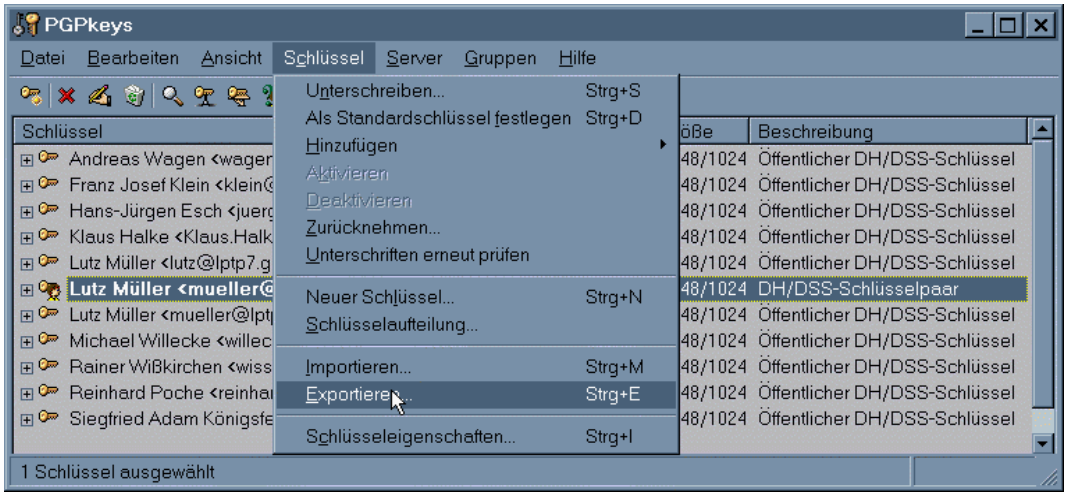
Nachdem nun die Installation der PGP Anwendung auf Ihrem PC unter MS Windows (hoffentlich) geklappt hat, sind Sie nun in der Lage Daten mit PGP zu bearbeiten. Was praktisch fehlt ist die Erklärung der Schlüsselverwaltung (5.1) sowie die Darstellung der verschiedenen Arten mit PGP zu arbeiten (ab 5.2). Es sei hier an dieser Stelle noch mal ausdrücklich darauf hingewiesen dass nachfolgend wertfrei die verschiedene Möglichkeiten mit PGP zu arbeiten vorgestellt werden. Ob eine Vorgehensweise - dass gilt besonders für die Schlüsselverwaltung - nun „sicher“ oder „unsicher“ ist geht aus Kapitel 3 hervor. Analog gilt dass das Aufrufen der verschiedenen PGP Funktionen auf verschiedenen Wegen möglich ist. Bitte entscheiden Sie sich für die Wege die Ihnen am meisten zusagen.

5.1 Schlüsselverwaltung

Um mit anderen Personen verschlüsselte Nachrichten auszutauschen, müssen Sie vorher Ihren Kommunikationspartnern Ihren öffentlichen Schlüssel (public key) geben. Das alle beteiligten Personen PGP Versionen installiert haben müssen die kompatibel sind, versteht sich von selbst. Es gibt mehrere Methoden, um den öffentlichen Schlüssel zu verteilen.

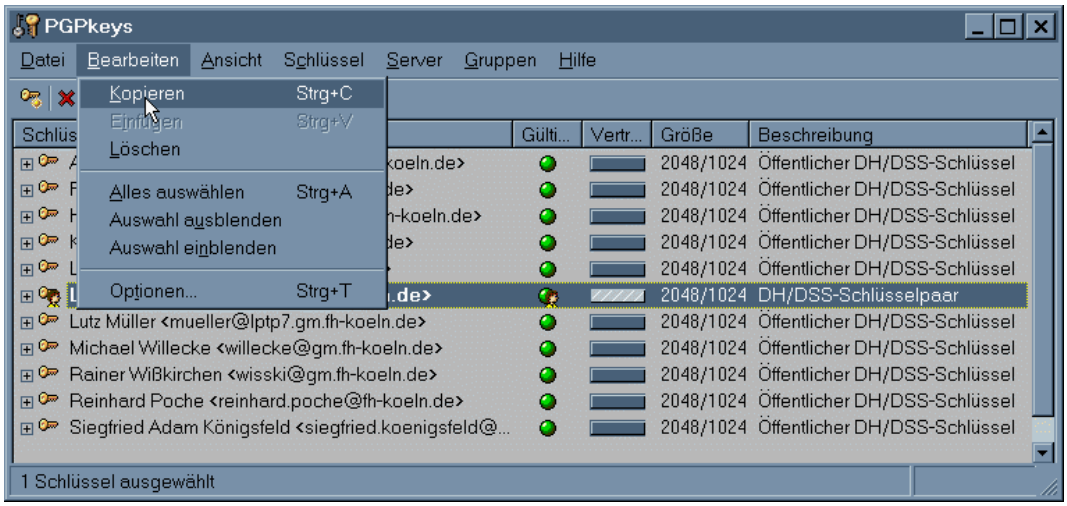
5.1.1 In Datei exportieren

In PGPkeys wählen Sie mit der Maus den Schlüssel mit Ihrem Namen aus. Gehen Sie anschließend auf **Schlüssel⇒Exportieren** und geben Sie den Namen der Datei an, in die der öffentliche Schlüssel exportiert werden soll. Sie können diese Datei künftig an Emails anhängen oder auf Diskette weitergeben. Der Empfänger kann diesen Schlüssel dann importieren.



5.1.2 In Email einfügen

Wenn Sie Emails verschicken wollen, geht es etwas einfacher, wenn Sie in PGPkeys den Schlüssel mit Ihrem Namen markieren und dann auf **Bearbeiten⇒Kopieren** gehen bzw. STRG+C drücken. Öffnen Sie nun das Email, das Sie verschicken möchten und fügen Sie den Schlüssel ein. Plazieren Sie dazu den Cursor im Textfeld und drücken STRG+V, benutzen Sie die rechte Maustaste oder gehen Sie über **Bearbeiten⇒Einfügen** des Email-Programms.

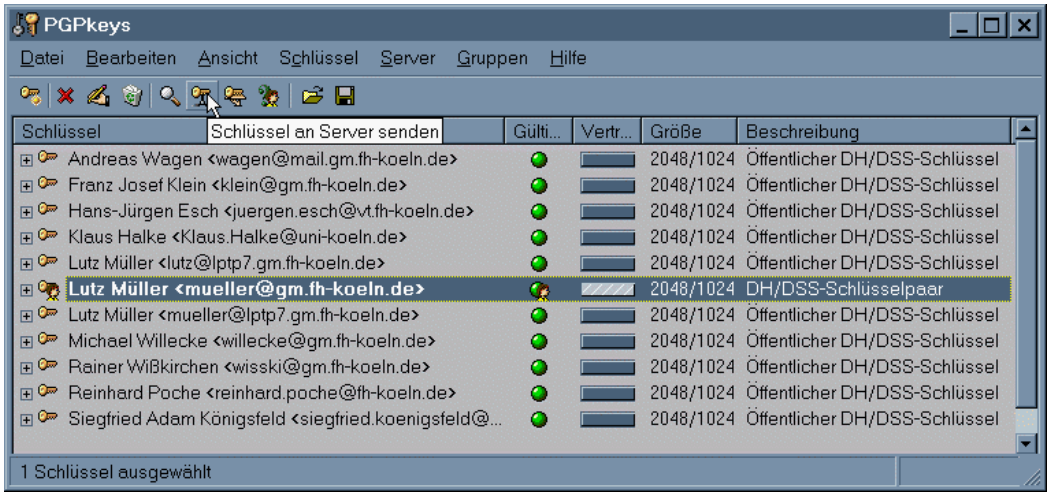


5.1.3 Export per Drag & Drop

Besonders einfach geht es per Drag and Drop, was allerdings nicht bei allen Anwendungen funktioniert. Klicken Sie auf Ihren Schlüssel und halten Sie die Maustaste gedrückt. Ziehen Sie den Schlüssel nun in eine geöffnete Datei (z.B. ein Email oder eine Textdatei) oder in einen Ordner im Windows Explorer. Wenn Sie den Schlüssel direkt in eine Datei ziehen, exportieren Sie den Schlüssel als Text (Sie sehen einen Buchstabensalat). Das Importieren kann dann für den Empfänger etwas schwieriger werden, als wenn der Schlüssel in Form einer Datei vorliegt.

5.1.4 Auf Keyservern veröffentlichen

Sie können (und sollten) Ihren öffentlichen Schlüssel auch auf einem Keyserver veröffentlichen. Denn dort kann jeder, der Ihnen eine Verschlüsselte Nachricht zukommen lassen will, aber nicht im Besitz Ihres öffentlichen Schlüssels ist, nach dem Schlüssel suchen. Öffnen Sie PGPkeys und klicken Sie mit der rechten Maustaste auf Ihren Schlüssel. Wählen Sie aus dem Kontextmenü  aus und wählen Sie danach einen Server aus.



Sie können Ihren Schlüssel auch mit der Maus markieren und dann **Server⇒Senden an⇒ein Server** Ihrer Wahl wählen.

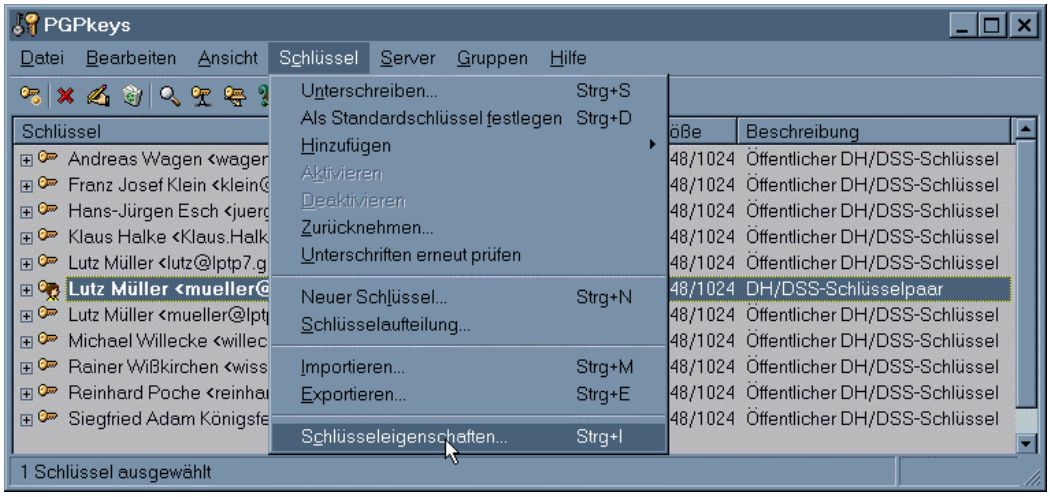


WARNUNG: Sobald ein Schlüssel auf einem Keyserver veröffentlich wurde kann er in der Regel nur dann wieder „gelöscht“ werden wenn Sie Ihre Passphrase zum Zeitpunkt des „Löschens“ parat haben.

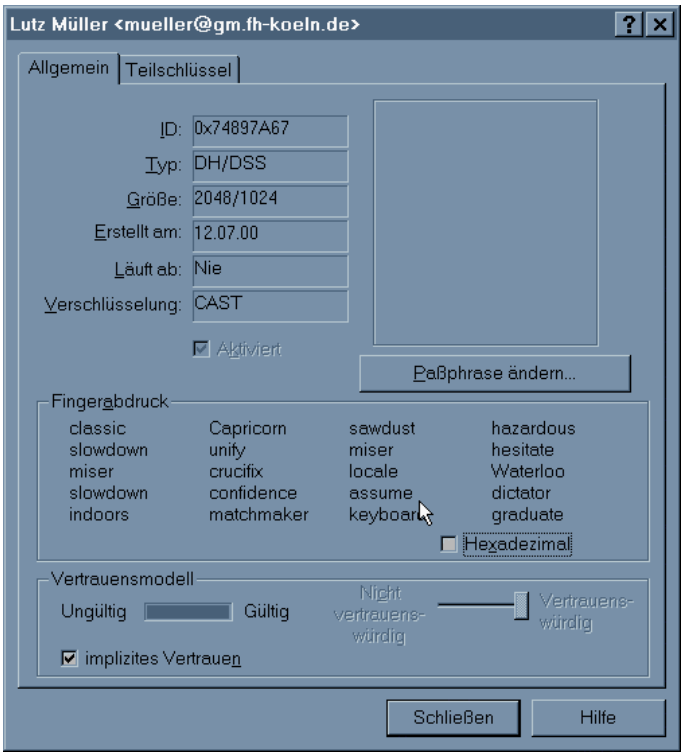
5.1.5 Überprüfung des öffentlichen Schlüssels mittels Fingerabdruck

Jeder Schlüssel trägt einen Fingerabdruck. Es ist eine zufällige Zeichenfolge, die es nur einmal gibt und einen Schlüssel eindeutig kennzeichnet. Um nun den Fingerabdruck überprüfen zu können geht man wie folgt vor.

Markieren Sie den zu überprüfenden Schlüssel mit der rechten Maustaste und wählen Sie aus dem Kontextmenü **Schlüssel⇒Schlüsseleigenschaften**. Es erscheint ein Dialog mit den Schlüsseleigenschaften.



Auf der Registerkarte „Allgemein“ sehen Sie den Fingerabdruck. Sie haben die Wahl zwischen zwei Darstellungen. Der Fingerabdruck wird standardmäßig als Liste von Wörtern dargestellt. Diese Wörter wurden so ausgewählt, dass es am Telefon möglichst wenig Missverständnisse geben kann. Durch markieren des Kontrollkästchens „Hexadezimal“ ändern Sie die Darstellung des Fingerabdruck in eine Hexadezimalzahl um.



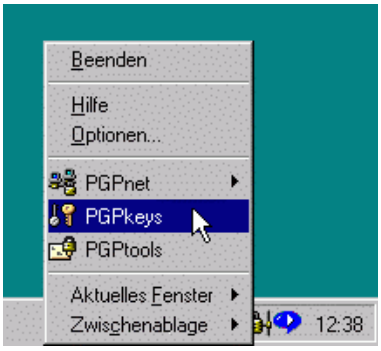
Fingerabdrücke kann man z.B. anwenden um öffentliche Schlüssel die man z.B. auf Schlüsselpartys erhalten hat auf ihre Echtheit zu überprüfen. Eine weitere Möglichkeit besteht darin, den Besitzer des Schlüssel

anzurufen und sich den Fingerabdruck vorlesen zu lassen. Es ist sehr unwahrscheinlich, dass jemand diesen zufälligen Anruf abfängt und dann auch noch in der Lage ist die Stimme des Gegenübers zu imitieren.

Überhaupt keinen Sinn macht die Verbreitung des Fingerabdrucks zusammen mit dem öffentlicher Schlüssel per Email, denn der Fingerabdruck und der öffentliche Schlüssel, kann ohne weiteres in der Email verändert werden.

5.2 PGPtray

Wie bereits in 4.3 beschrieben lassen sich alle PGP Funktionen über den Windows „Tray" abrufen.



Durch einfaches „klicken" der linken Maustaste auf das „Vorhängeschlosssymbol" rufen Sie obiges Menü auf, die Menüpunkte haben folgende Bedeutung:

Menüpunkt	***Funktion***
Beenden	Beendet PGPtray
Hilfe	Ruft PGP Hilfe auf. Installation der Hilfedateien ist notwendige Voraussetzung
Optionen	Hier können die PGP Grundeinstellungen vorgenommen werden
PGPnet	Dient zur Erzeugung einer sicheren Verbindung, auf Protokollebene, mit einem anderem Rechner
PGPkeys	Ruft die PGP Schlüsselverwaltung auf
PGPtools	Erzeug einen „Werkzeugkasten" mit verschiedenen nützlichen Funktionen auf dem „Desktop"
Aktuelles Fenster	Dient zum Ver- bzw. Entschlüsseln sowie dem Unterschreiben und der Prüfung von elektronischen Unterschrift eines Fensterinhalts
Zwischenablage	Dient zum Ver- bzw. Entschlüsseln sowie dem Unterschreiben und der Prüfung von elektronischen Unterschrift der Daten in der Zwischenablage

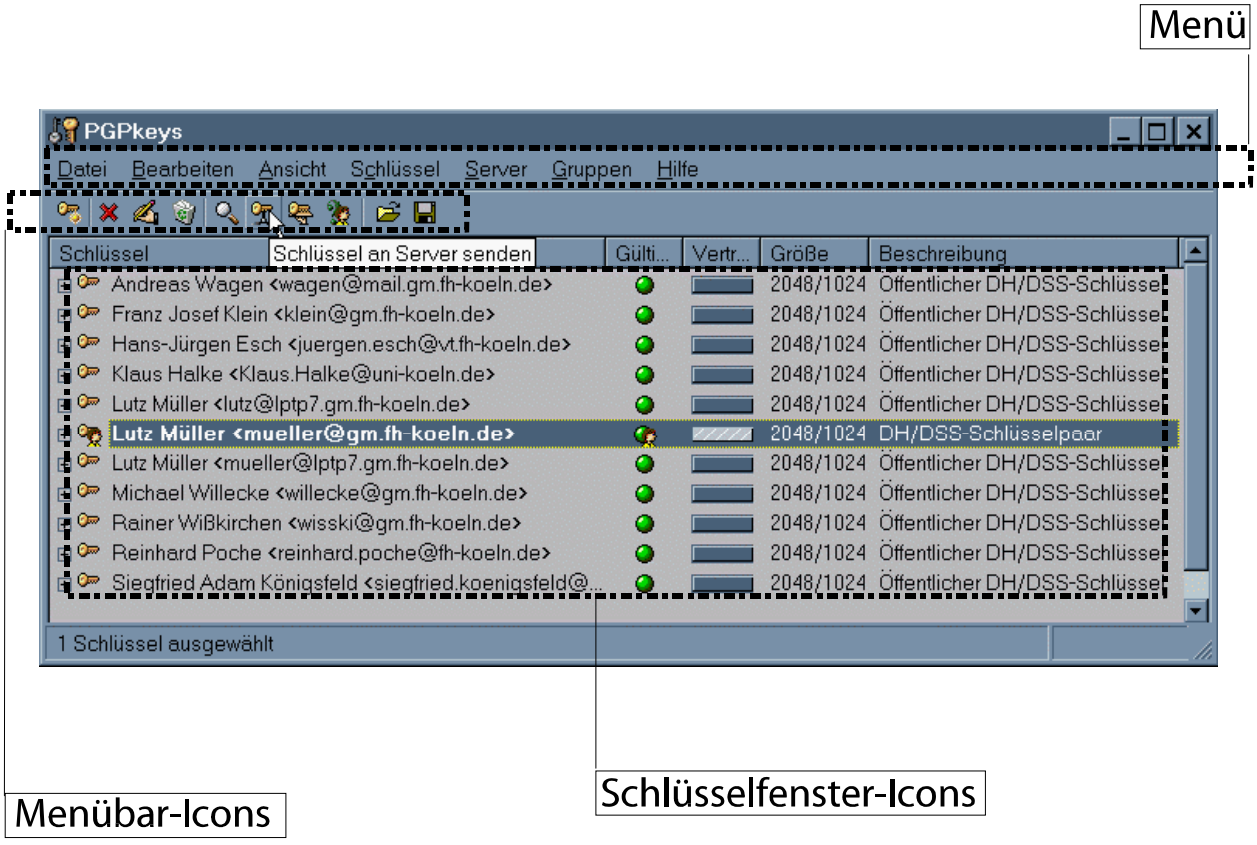
Nachfolgend sind obige Funktionen im einzelnen Beschreiben.

5.3 PGPnet



5.4 PGPkeys

PGPkeys dient hauptsächlich zur Schlüsselverwaltung. Wie Schlüssel verwaltet werden geht aus 5.1 hervor. Hier wird „nur“ allgemein auf die Bedienoberfläche von PGPkeys eingegangen. Die Erklärung der einzelnen Menüs erspare ich mir, der Anwender möge dazu mittels F1-Taste oder des Hilfe-Menü das Hilfssystem nutzen. Nachfolgend sind Funktionen der einzelnen Symbole erklärt.



5.4.1 Menübar-Icons

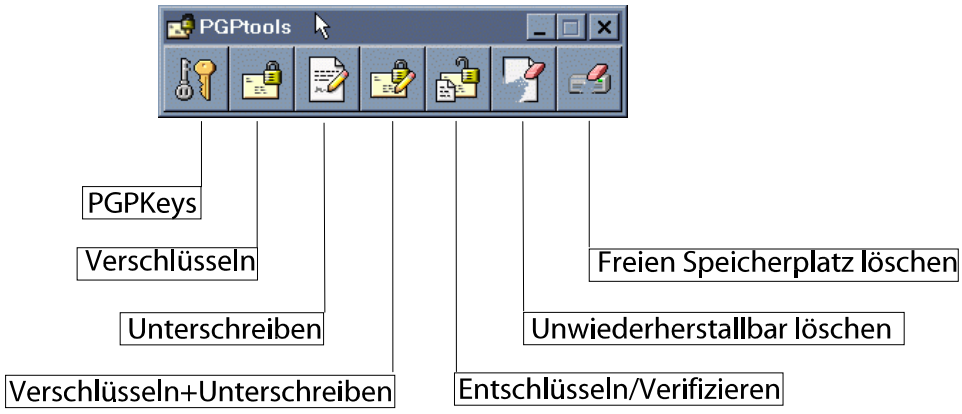
Icon	*Funktion*
	01. Öffnet den Assistenten zur Schlüsselerzeugung.
	02. Widerruft den ausgewählten Schlüssel oder Signatur und verhindert, dass jemand Daten für diesen Schlüssel verschlüsselt.
	03. Ermöglicht Ihnen, den ausgewählten Schlüssel zu signieren. Sie garantieren damit, dass der Schlüssel wirklich zur angegebenen Person gehört.
	04. Löscht den markierten Schlüssel, Signatur oder Foto.
	05. Öffnet den Schlüsselsuchdialog zur Suche von Schlüsseln im lokalen Schlüsselbund oder auf Keyservern.
	06. Sendet den ausgewählten Schlüssel zu einem Keyserver.
	07. Aktualisiert den ausgewählten Schlüssel vom Keyserver.
	08. Öffnet den Schlüsseleigenschaften-Dialog.
	09. Ermöglicht den Import eines Schlüssels in den lokalen Schlüsselbund.
	10. Exportiert den markierten Schlüssel in eine Datei.

5.4.2 Schlüsselfenster-Icons

Icon	*Funktion*
	01. Ein goldener Schlüssel und Kopf ist das Symbol für ein DH/DSS-Schlüsselpaar bestehend aus öffentlichem und privatem Schlüssel
	02. Ein einzelner goldener Schlüssel steht für einen öffentlichen DH-Schlüssel
	03. Ein grauer Schlüssel und ein Kopf stellen ein RSA-Schlüsselpaar dar, bestehend aus öffentlichen und privatem Schlüssel
	04. Ein einzelner grauer Schlüssel symbolisiert einen öffentlichen RSA-Schlüssel
	05. Abgelaufener Schüssel, das Verfalldatum wird bei der Schlüsselerzeugung festgelegt
	06. Ein Schlüssel, der zeitweise nicht zum Ver- und Entschlüsseln verfügbar ist, wird blass dargestellt
	07. Widerrufener Schlüssel
	08. Ein grüner Kreis mit Kopf ist das Symbol für Ihren eigenen Schlüssel
	09. Der grüne Kreis signalisiert Gültigkeit des Schlüssels. Ein roter Kreis in der ADK-Spalte (**A**dditional **D**ecryption **K**ey) bedeutet, dass der Schlüssel einen zusätzlichen Entschlüsselungsschlüssel hat
	10. Der graue Kreis bedeutet, dass der Schlüssel ungültig ist. In der ADK-Spalte bedeutet er, dass es für diesen Schüssel keinen zusätzlichen Entschlüsselungsschlüssel (ADK) gibt
	11. Karteikarte steht für den Besitzer des Schlüssels und die Namen und Emailadressen, die dem Schlüssel zugeordnet sind
	12. Ein Stift stellt die Signaturen von Zertifizierungsstellen und anderen PGP-Benutzern dar, die für die Echtheit des Schlüssel bürgen. • Ein rotes X symbolisiert eine widerrufene Signatur • Ein blasser Stift erscheint bei einer ungültigen Signatur • Ein blauer Pfeil heißt, dass die Signatur exportierbar ist
	13. Fotografische Benutzerkennung eines öffentlichen Schlüssels.
	14. Bei Ihrem eigenen Schlüssel ist der Balken gestreift. Unabhängig von Signaturen hat er volle Gültigkeit und volles Vertrauen.
	15. Der vollausgefüllte Balken steht für volle Gültigkeit oder volles Vertrauen in den Benutzer
	16. Ein halbausgefüllter Balken erscheint bei grundsätzlich gültigen Schlüsseln oder vertrauenswürdigen Personen
	17. Bei einem ungültigen Schlüssel oder einem nicht vertrauenswürdigem Benutzer ist der Balken leer

5.5 PGPTools

Sollten Sie via PGPtray die PGPtools starten zeigt ihnen PGP folgenden Wergzeugkasten auf der Schreibtischoberfläche.



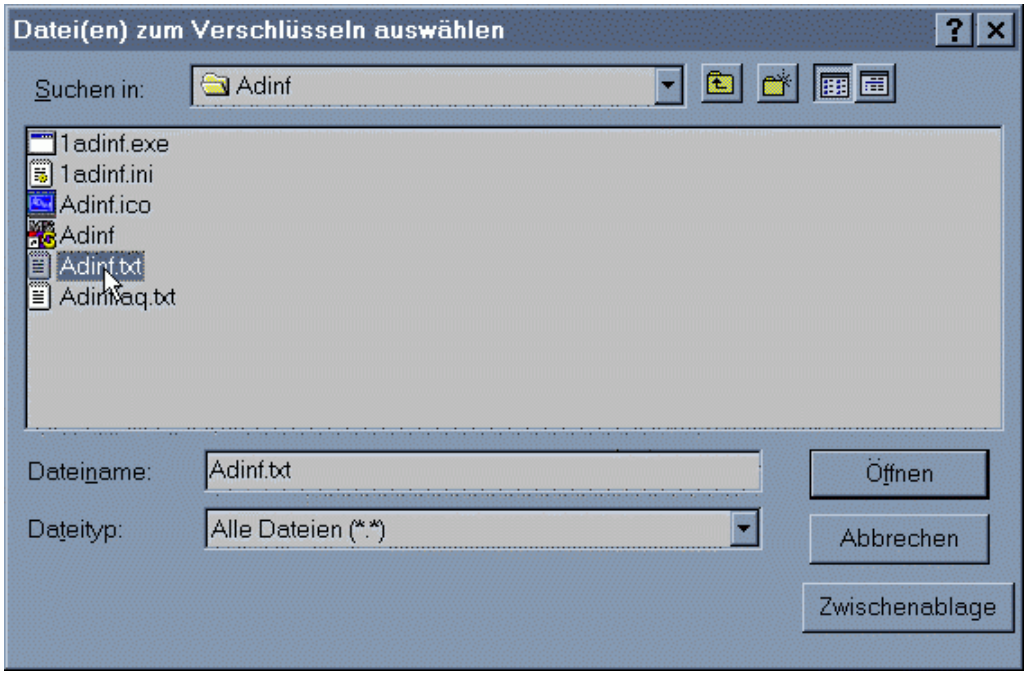
Dieser Werkzeugkasten ermöglicht Ihnen einen bequemen Einstieg in alle wichtigen PGP Funktionen. Ob Sie alle in 5.4 vorgestellten Funktionen via PGPtools nutzen, oder diese Funktionen über andere Wege ansprechen ist Ihre ganz persönliche Entscheidung.

5.5.1 PGPTools aufrufen

Wenn Sie mit dem Mauszeiger und der linken Maustaste PGPkeys ansprechen erhalten Sie die in 5.3 vorgestellte Möglichkeit der Schlüsselverwaltung.

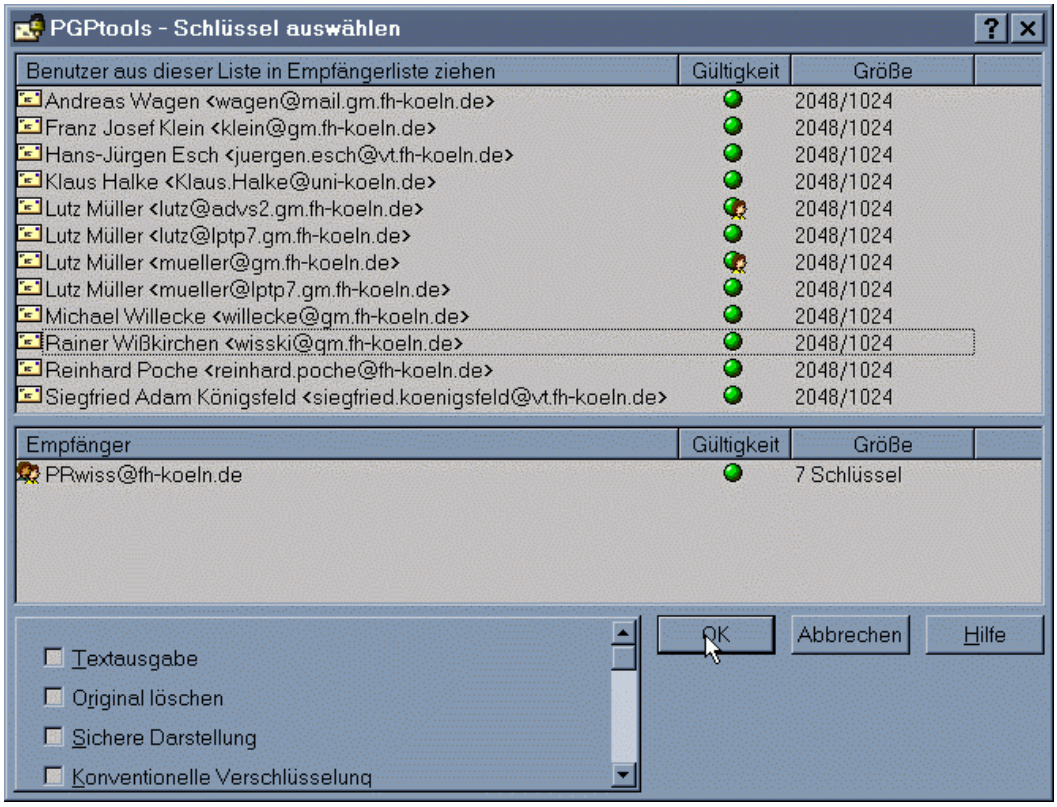
5.5.2 PGPTools - Verschlüsseln aufrufen

Mit dieser Funktion können Daten verschlüsselt werden. Nach anklicken des „Verschlüsseln“ – Symbols öffnet PGPtools nachfolgendes Fenster.



Hier können eine oder mehrer Dateien die verschlüsselt werden sollen, aus einem vorher bestimmten Pfad, durch eine Markierung mit der linken Maustaste ausgewählt werden. Nach der erfolgten Auswahl bestätigen Sie bitte mit dem [Öffnen] Knopf.

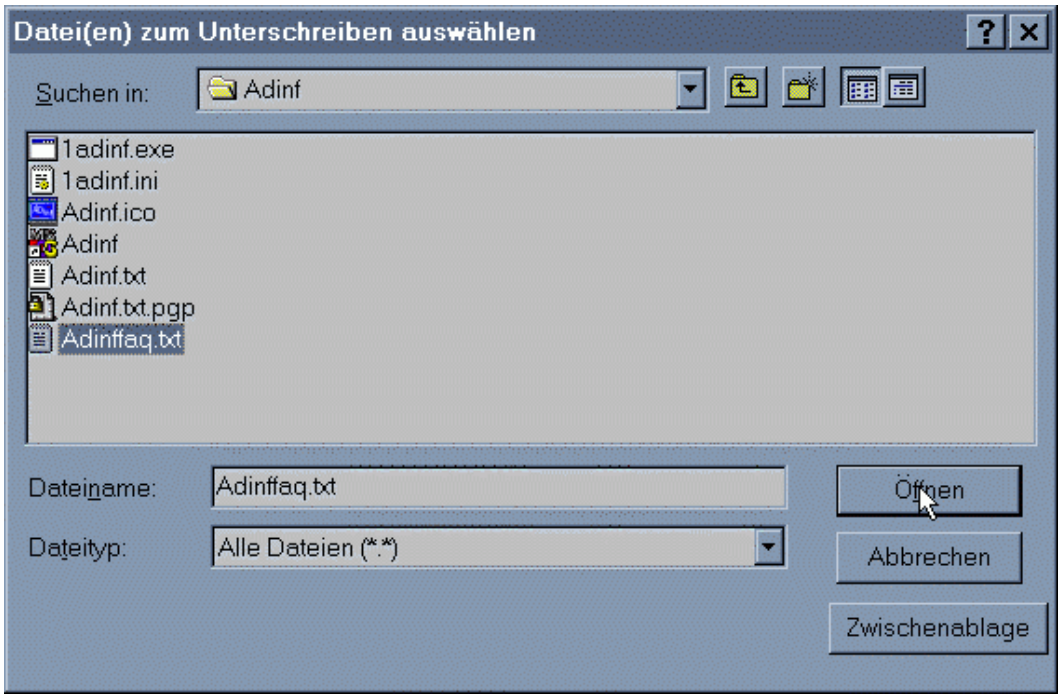
PGP „weiß“ nun welche Dateien es bearbeiten soll und öffnet das nächste Fenster.



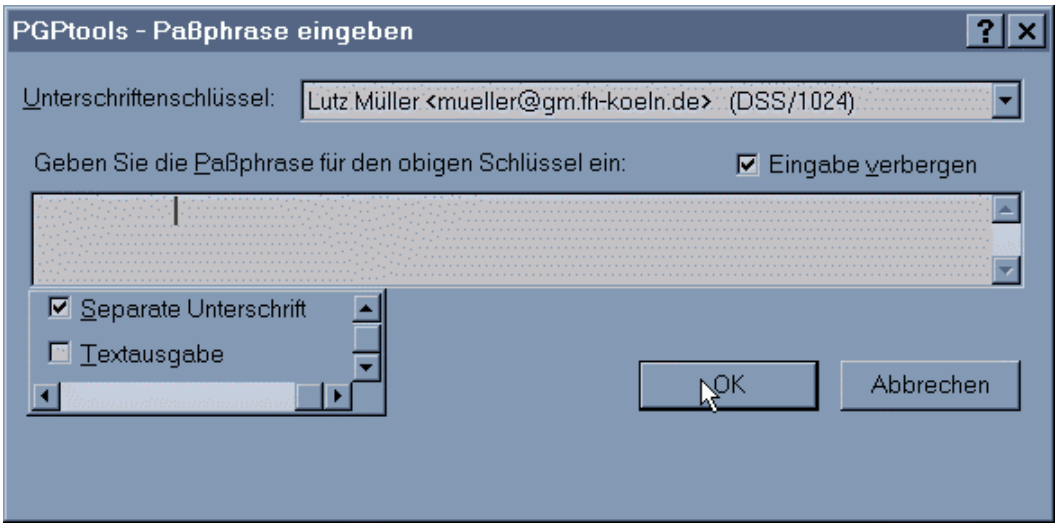
Nach dem „Was wird verschlüsselt“ folgt zwangsläufig „Für wenn wird verschlüsselt“. Logischerweise kann PGP nur mit den öffentlichen Schlüsseln arbeiten die es kennt. Anzumerken ist, dass für das „reine“ Verschlüsseln nicht Ihr privater Schlüssel benötigt wird, und dass wenn Sie sich denn nicht selber in die Empfängerliste eingetragen haben, eine Entschlüsselung der Dateien von Ihnen persönlich nicht vorgenommen werden kann.

5.5.3 PGPTools - Unterschreiben aufrufen

Elektronisch Unterschreiben ist auch eine wesentliche Funktion von PGP. Nach anklicken des entsprechenden Knopfes erscheint nachfolgendes Fenster.



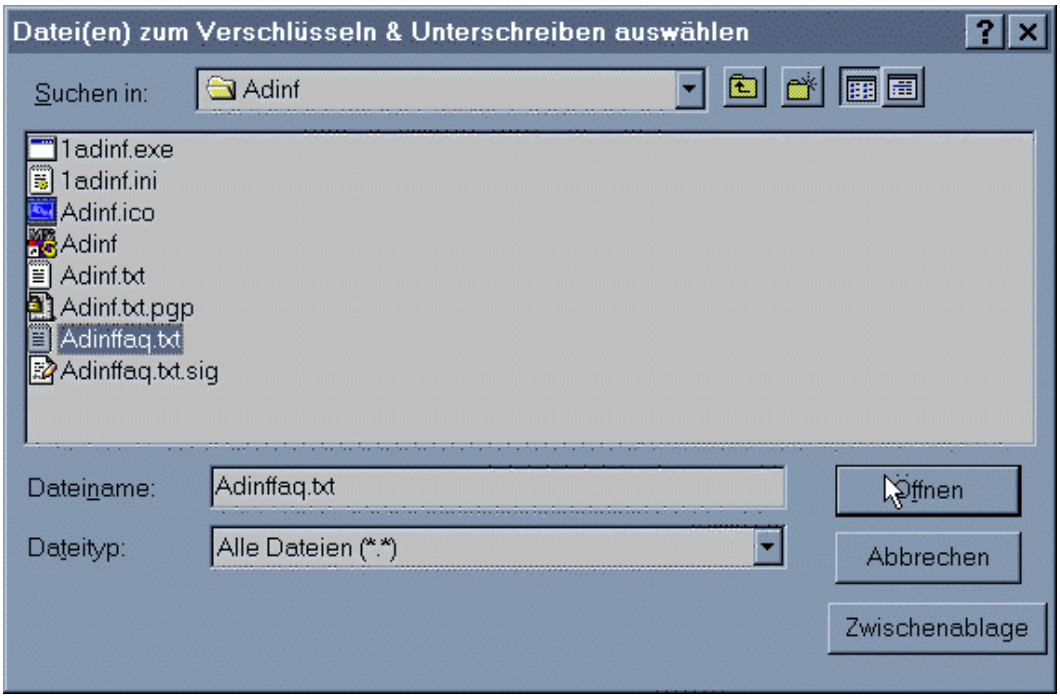
Hier können eine oder mehrer Dateien die elektronisch unterschrieben werden sollen, aus einem vorher bestimmten Pfad, durch eine Markierung mit der linken Maustaste ausgewählt werden. Nach der erfolgten Auswahl bestätigen Sie bitte mit dem [Öffnen] Knopf. PGP „weiß“ nun welche Dateien es bearbeiten soll und PGP öffnet daraufhin das nächste Fenster.



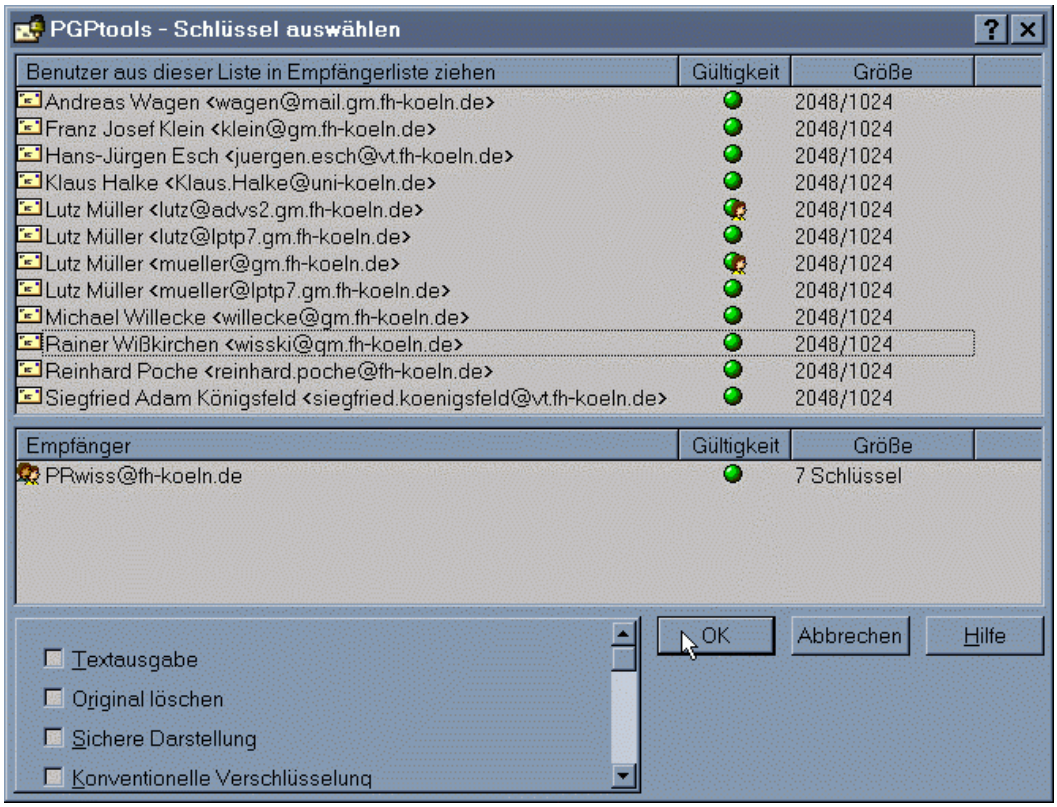
Huch, warum wird hier keine Empfängerliste dargestellt ? Antwort: Weil zum „reinen“ elektronischen unterschreiben ausschließlich Ihr privater Schlüssel benötigt wird. Nach der Eingabe Ihrer Passphrase kann PGP mit Ihrem privaten Schlüssel die vorher ausgewählten Dateien signieren. Wichtig ist dabei, dass Sie PGP mitteilen ob die Signatur in einer separaten Datei abgespeichert werden soll oder an die bestehenden Daten angehängt wird. Gerade bei Dateien die mit „normalen“ Büroanwendungen wie z.B. Word, Excel usw. erstellt wurden ist es wichtig, dass Sie die Option „Separate Unterschrift“ nutzen.

5.5.4 PGPTools - Verschlüsseln+Unterschreiben aufrufen

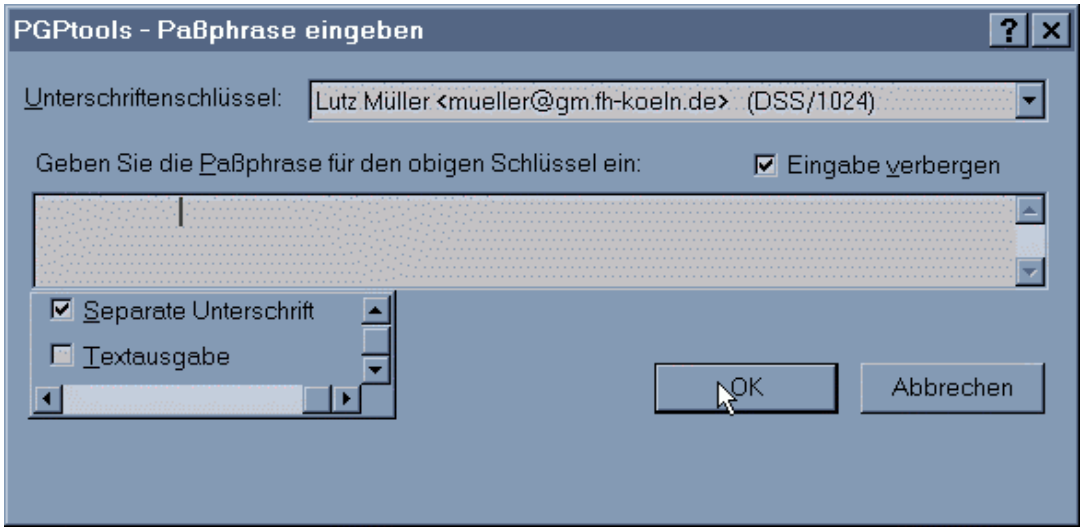
Wir haben bisher das Verschlüsseln und elektronisches Unterschreiben als getrennte Funktionen kennen gelernt. Selbstverständlich kann PGP beide Funktionen auch gleichzeitig durchführen. Nach dem anklicken des entsprechenden Symbol aus dem PGP Werkzeugkasten erscheint nachfolgendes Fenster.



Auch hier sind die Dateien auszuwählen die Sie verschlüsseln/unterschreiben möchten. Nach der Auswahl bestätigen Sie bitte mit [Öffnen].



Für das Verschlüsseln benötigt PGP die Empfänger ID's. Diese sind in der Regel identisch mit den Email–Adressen der Empfänger.



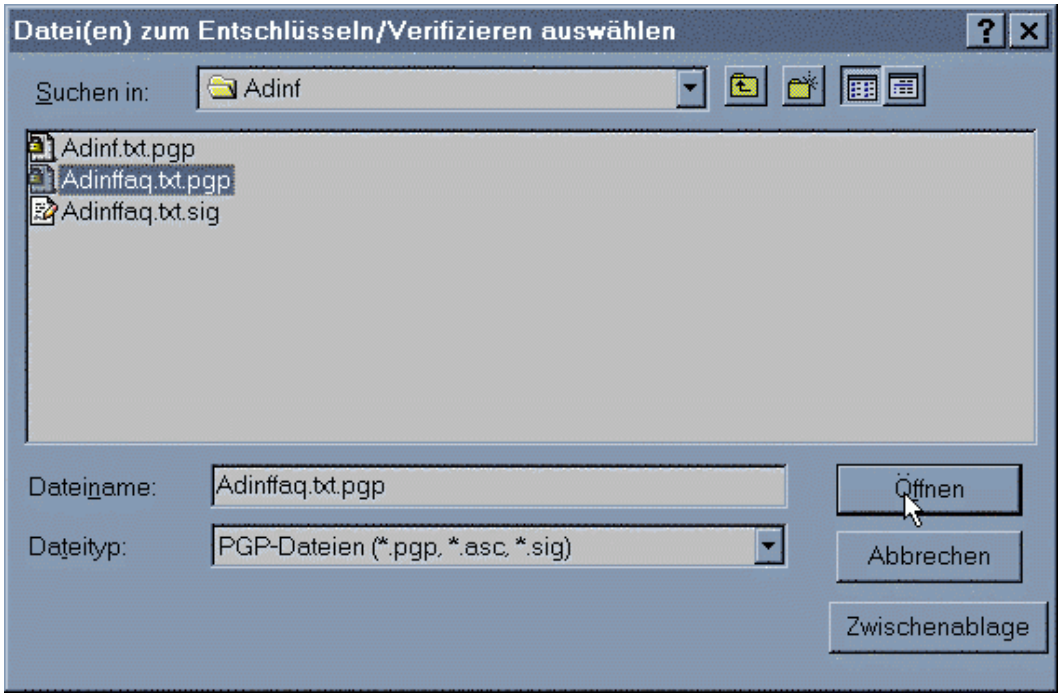
Die Eingabe der Passphrase wird gebraucht, damit PGP die ausgewählten Dateien elektronisch Unterschreiben (signieren) kann.

5.5.5 PGPTools - Entschlüsseln/Verifizieren aufrufen

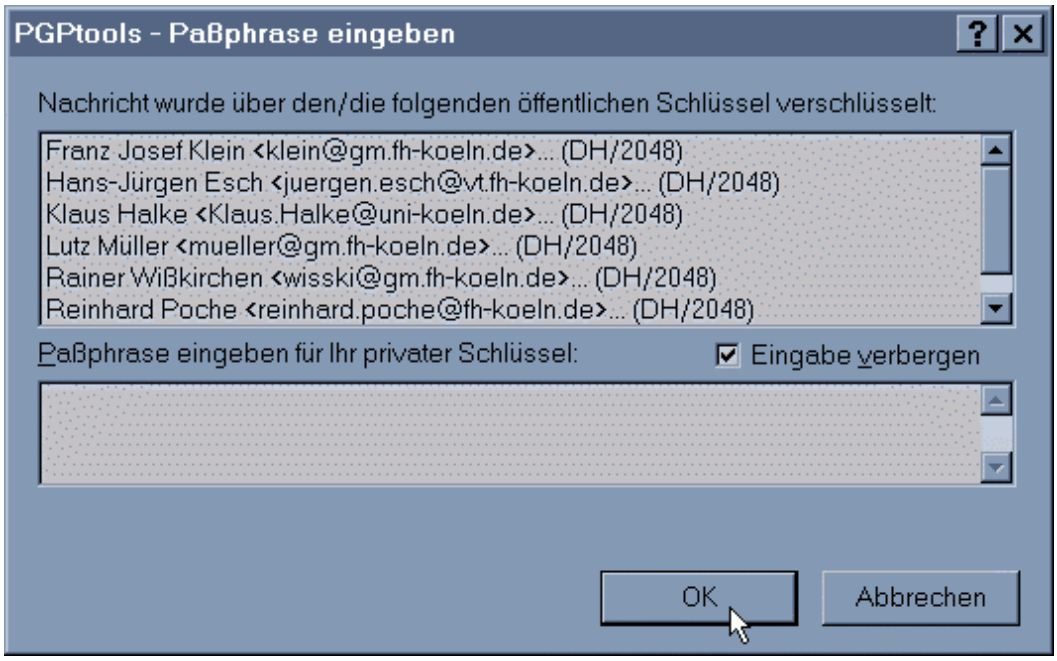
Die „Umkehrfunktion“ Entschlüsseln/Verifizieren wird aufgerufen um die „Klartext“-Daten zu erhalten bzw. um eine elektronische Unterschrift zu überprüfen.

Es werden folgende Dateiformate unterstützt:

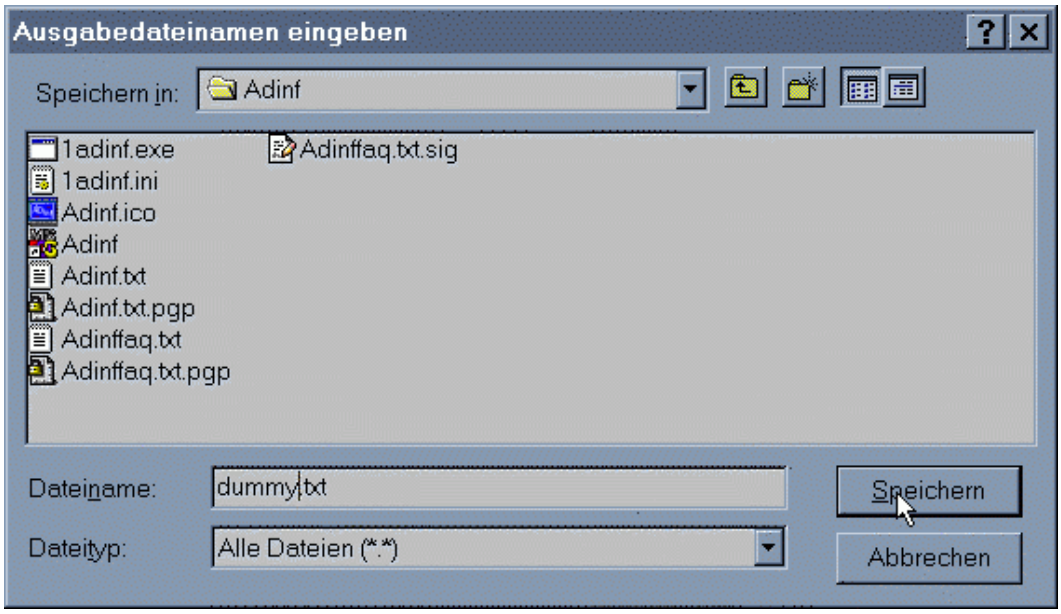
Dateiart	***Bemerkung***
*.pgp	Verschlüsselte Dateien die auch zusätzlich signiert sein können im binären Format
*.asc	Verschlüsselte Dateien die auch zusätzlich signiert sein können im Textformat. Dieses Format benötigt ca. 30% mehr Platz auf dem Datenträger als das binäre Format. Vorteile hat *.asc beim versenden von Daten via Email
*.sig	Beinhaltet Daten zum prüfen der elektronischen Unterschrift (Signature) von Dateien



In diesem Fenster erfolgt das obligatorische auswählen der von PGP zu bearbeitenden Dateien.



Da die ausgewählte Datei „addinffaq.txt.pgp“ verschlüsselt ist benötigt PGP eine Passphrase um mit dem entsprechenden privaten Schlüssel arbeiten zu können.



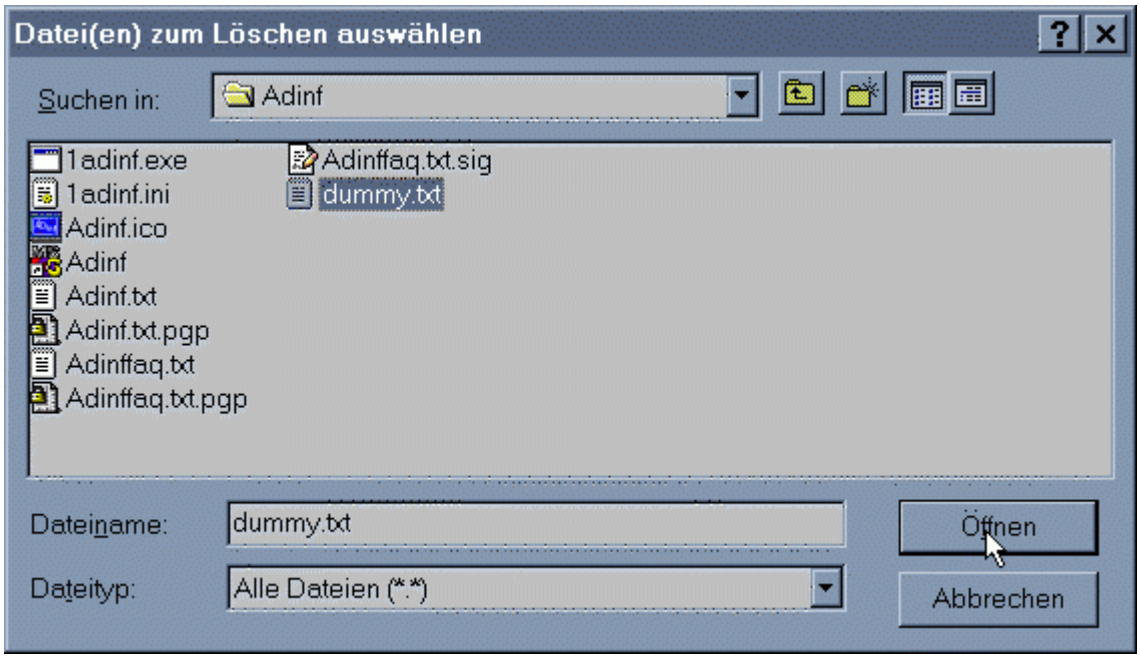
PGP bemerkt dass sich die original „addinffaq.txt“ Datei in dem Arbeitsverzeichnis befindet. Um keine Daten zu überschreiben lässt PGP die Vergabe eines „neuen“ Dateinamen zu.



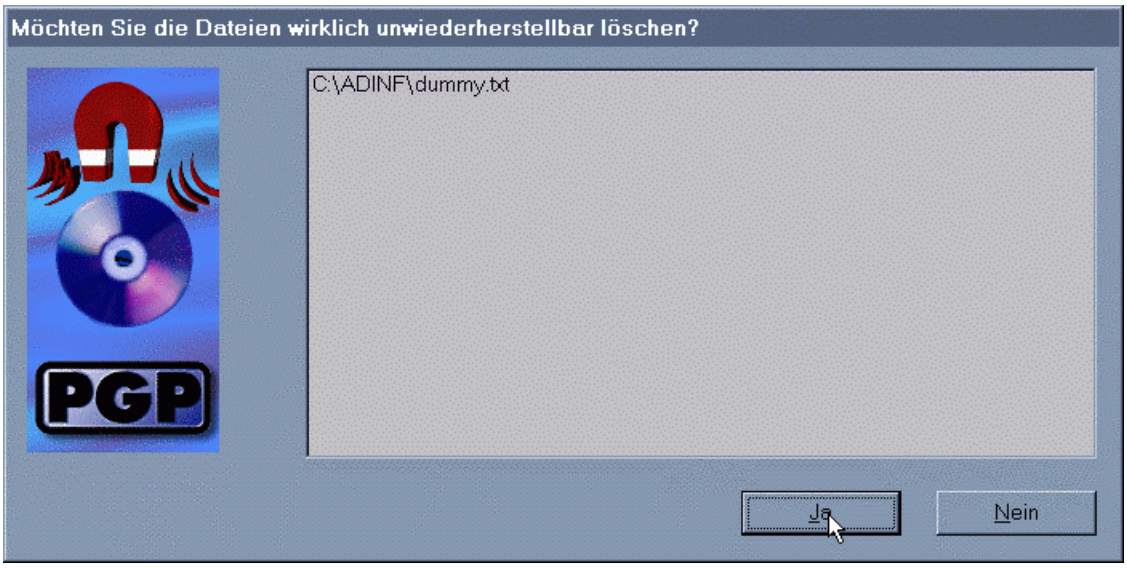
Nach dem Entschlüsseln der Datei wird in diesem Fenster die Gültigkeit der Signature angezeigt.

5.5.6 PGPTools - Unwiederherstallbar löschen aufrufen

In 5.5.5 wurde die unheimlich geheime Datei „dummy.txt“ aus verschlüsselten Daten erzeugt. Angesichts der enormen Wichtigkeit dieser Datei bietet sich eine „unwiederherstellbare“ Löschung dieser Datei an.



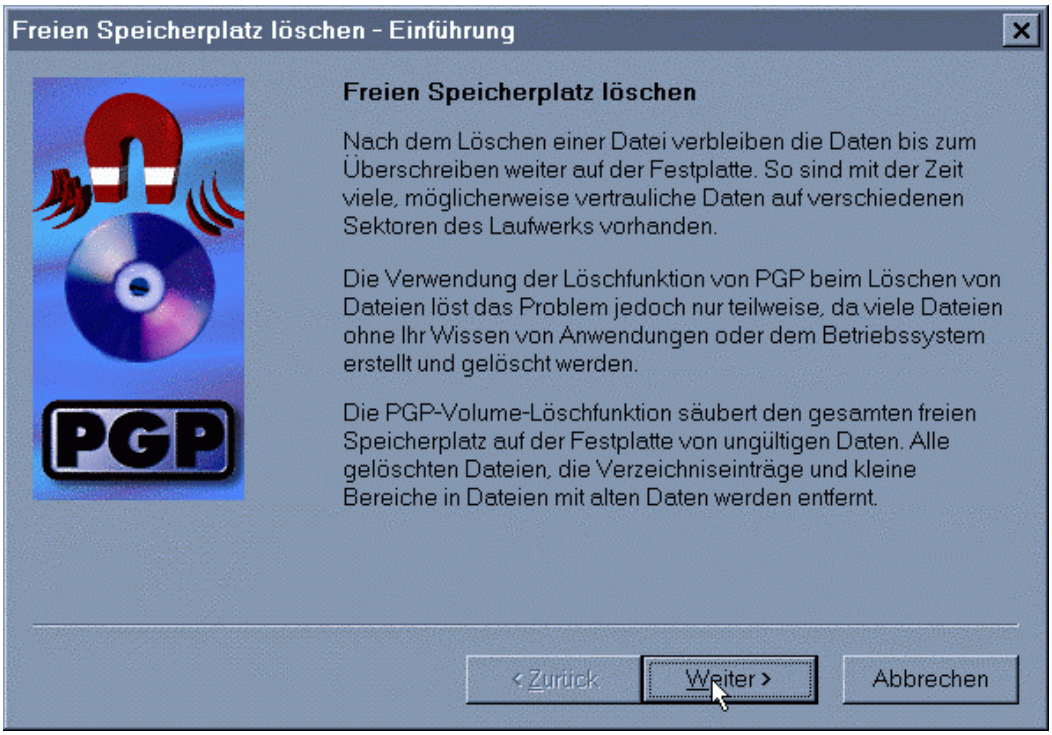
In diesem Fenster können Sie als Anwender die Dateien auswählen die „Unwiederherstellbar“ gelöscht werden sollen. Mit [Öffnen] bestätigen Sie die Auswahl.



Eine Sicherheitsabfrage ist notwendig, weil PGP mindestens so gut löscht das Sie mit „Hausmitteln“ niemals mehr die Daten rekonstruieren könnten. Ob diese Art der Datenlöschung allen möglichen Rekonstruktionsverfahren trotzt ist mir nicht bekannt.

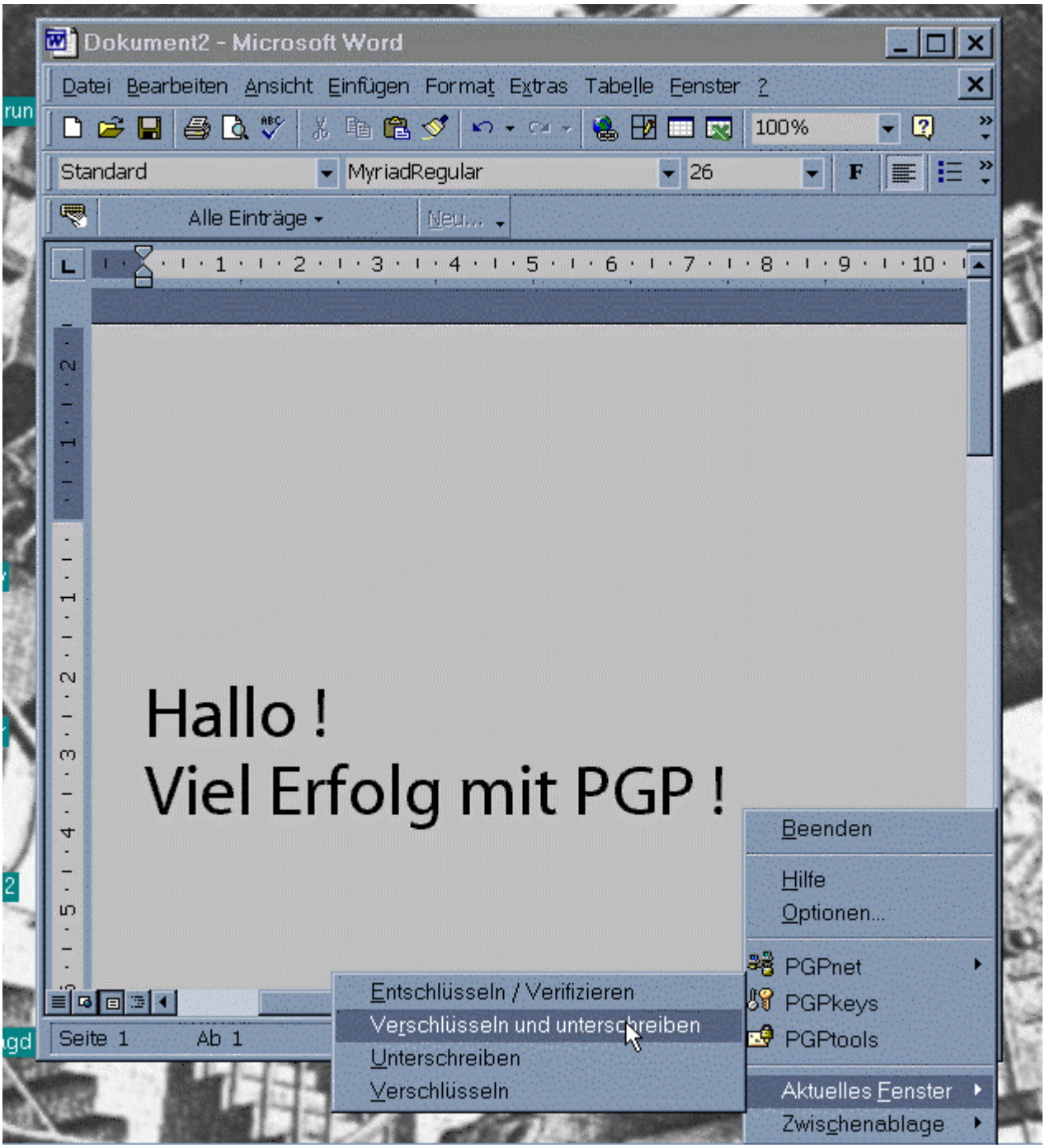
5.5.7 PGPTools - Freien Speicherplatz löschen aufrufen

Analog zu 5.5.6 bietet PGPtools auch die Möglichkeit das Filesystem Ihres Windows PC von Datenmüll, der einem Angreifer dennoch nützlich werden könnte, zu befreien. Auch hier ist meine ganz persönliche Meinung, dass wenn Sie diesen Sicherheitsstandard überhaupt benötigen, sollte als Alternative ein verschlüsseltes Dateisystem eingesetzt werden..

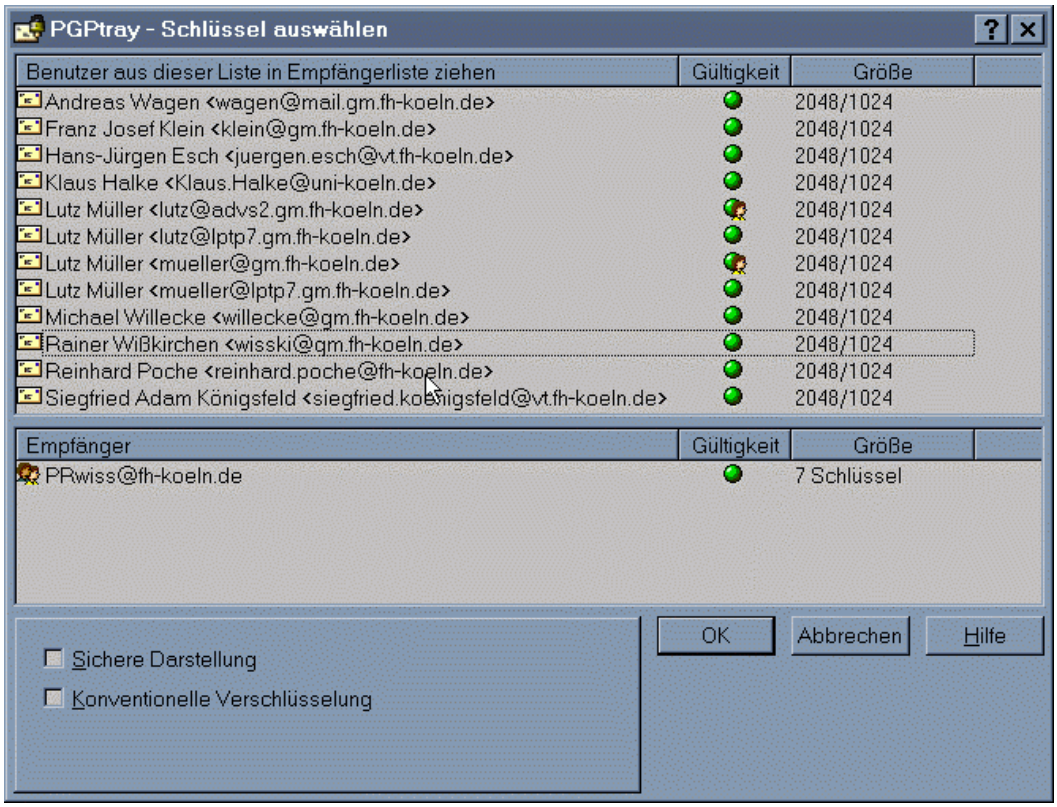


5.6 Aktuelles Fenster

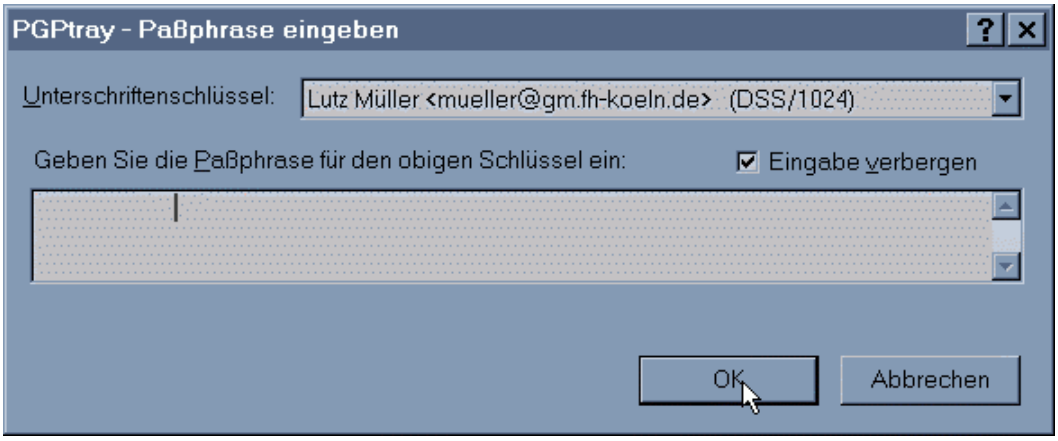
In 5.5 haben wir uns mit der Bearbeitung von Dateien mittels PGP beschäftigt. PGP kann aber nicht „nur“ auf Dateiebene Daten verschlüsseln/entschlüsseln/signieren sondern, was manchmal sehr nützlich sein kann, (wenn z.B. Ihr Email Programm keine PGP Erweiterung besitzt) auch dieselben Funktionen auf ganze Fensterinhalte anwenden. Um PGP auf diese Weise zu nutzen geht man wie folgt vor:



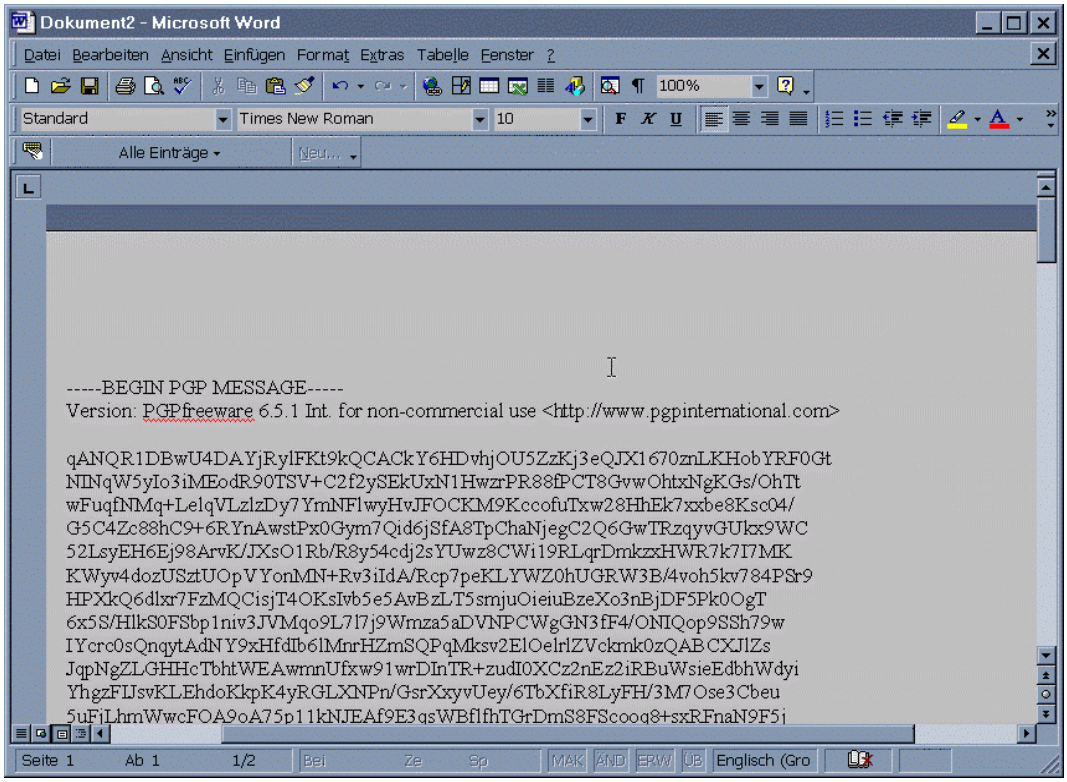
Bringen Sie zunächst das Fenster dessen Inhalt Sie verschlüsselt möchten in den Vordergrund der Windows Schreibtischoberfläche. Danach rufen Sie bitte mit **PGPtray⇒Aktuelles Fenster⇒Verschlüsseln und unterschreiben** die gleichlautende Funktion auf.



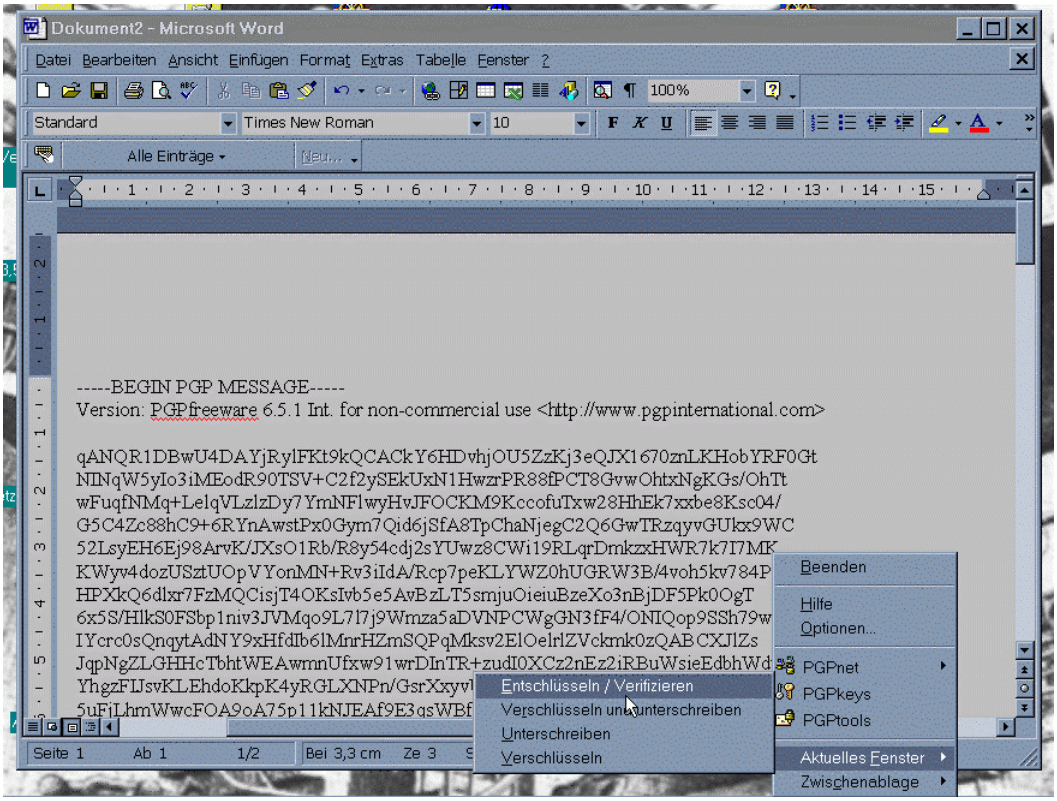
Da Sie u.a. auch verschlüsseln möchten benötigt PGP die öffentlichen Schlüssel der Empfänger.



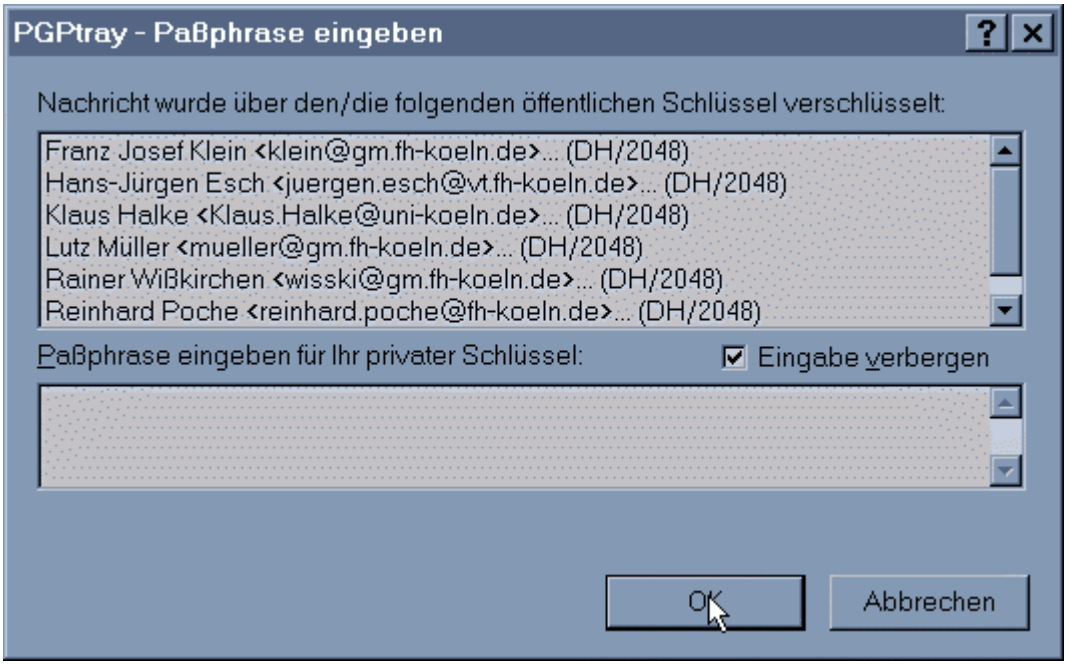
Ihr privater Schlüssel ist PGP nur dann zugänglich, nachdem Sie Ihre Passphrase eingegeben haben. Nach dem Sie mit [OK] bestätigt haben liegen die verschlüsselten und signierten Daten in dem oben ausgewählten Fenster vor.



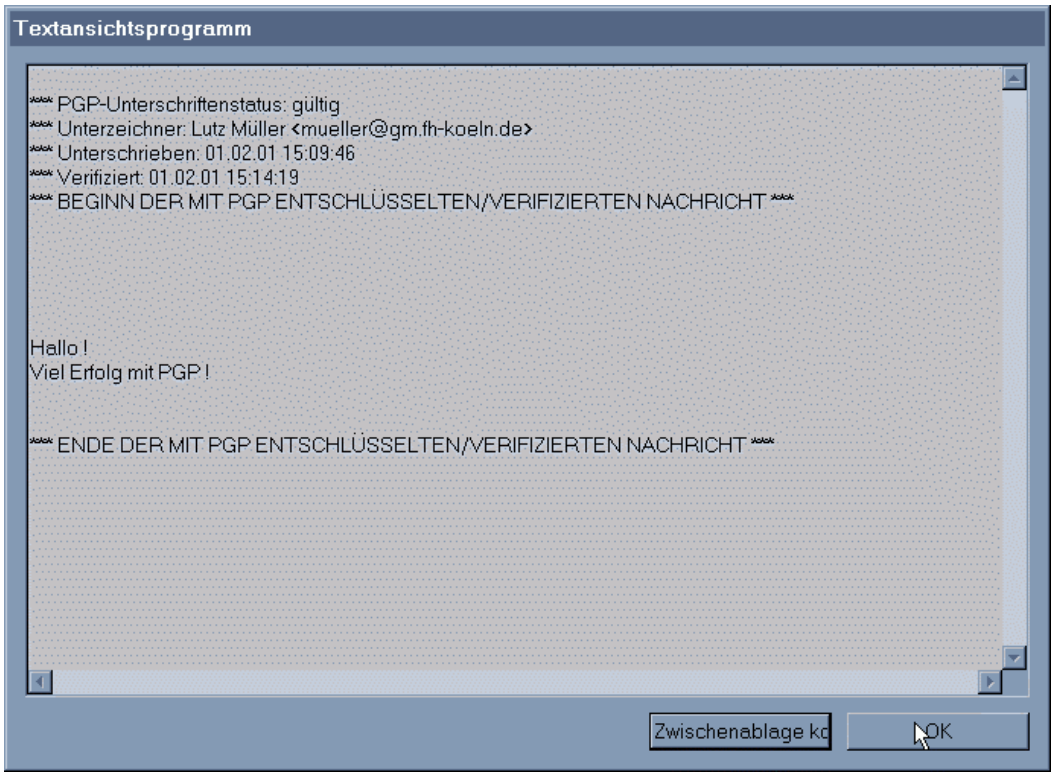
Sie sehen nun die verschlüsselten und signierten Daten in Ihrer aktuellen Anwendung. Zur Übung wird nun dieses „Datenkauderwelsch“ zurück in den Klartext umgewandelt. Dazu geht man wie folgt vor.



Nach dem Sie das Fenster dessen Inhalt Sie Entschlüssel/Verifizieren wollen in den Vordergrund der Schreibtischoberfläche gebracht haben, wählen Sie bitte via PGPtray die oben dargestellte Funktion aus.



PGP erkennt, dass das Fenster u.a. auch Verschlüsselt wurde und fordert Sie nun zur Eingabe der Passphrase auf. (Noch mal: Diese Passphrase wird benötigt, um Ihren privaten Schlüssel PGP zugänglich zumachen)

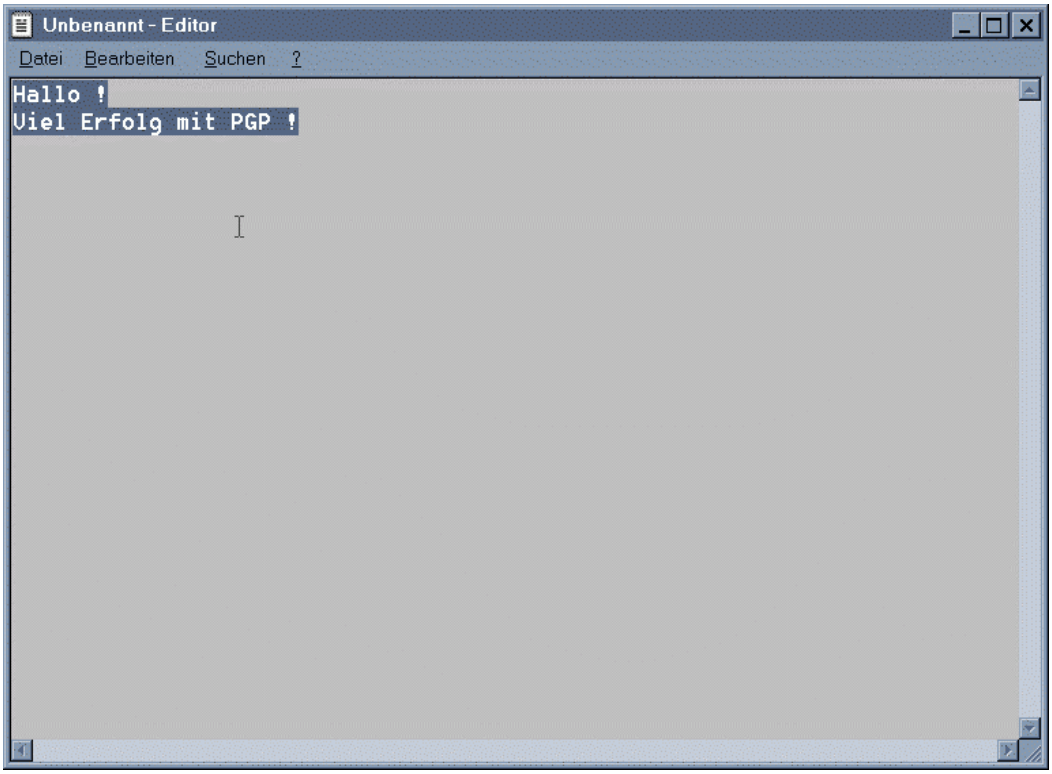


Sie erkennen nun den Klartext der „Fensterdaten“ der bei Bedarf in die Zwischenablage kopiert werden kann. Hieraus ist auch ersichtlich, dass diese Daten von einer bestimmten Person signiert wurden.

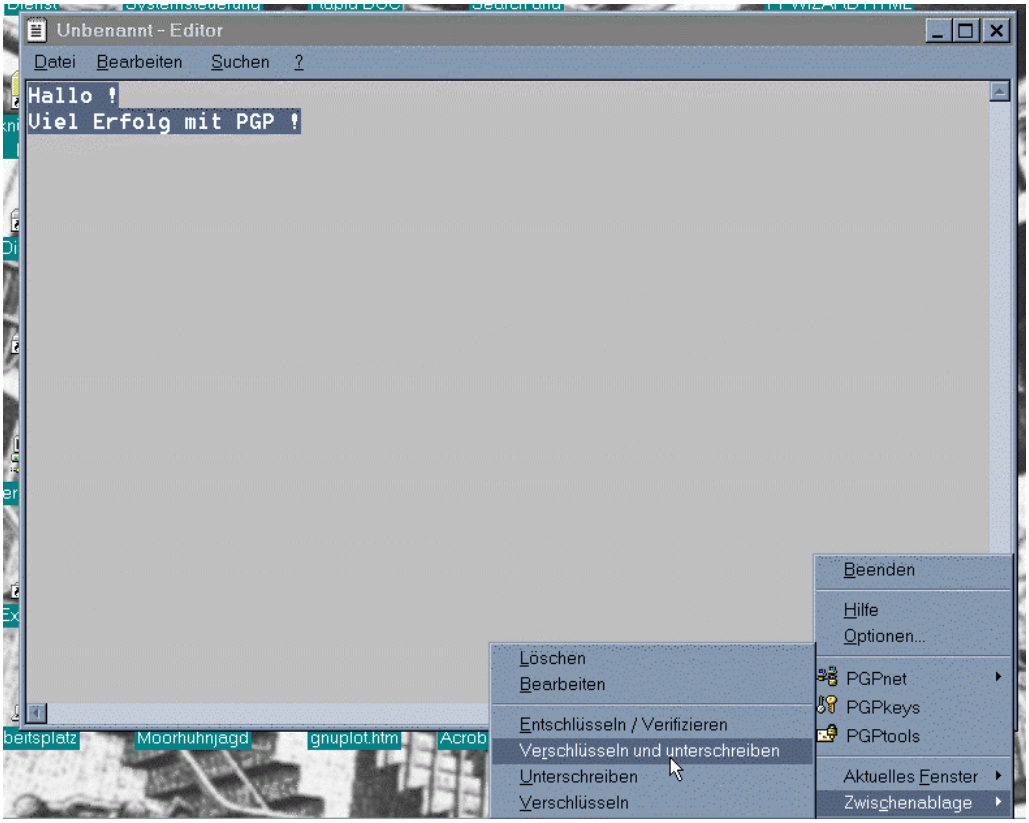
Es sei noch erwähnt das die Funktionen „Aktuelles Fenster unterschreiben“ bzw. „Aktuelles Fenster verschlüsseln“ zur Verfügung stehen. Die Erklärung dieser einzelnen Schritte erspare ich, weil die hier vorgestellte Funktion „Aktuelles Fenster verschlüsseln/unterschreiben“ beides beinhaltet.

5.7 Zwischenablage

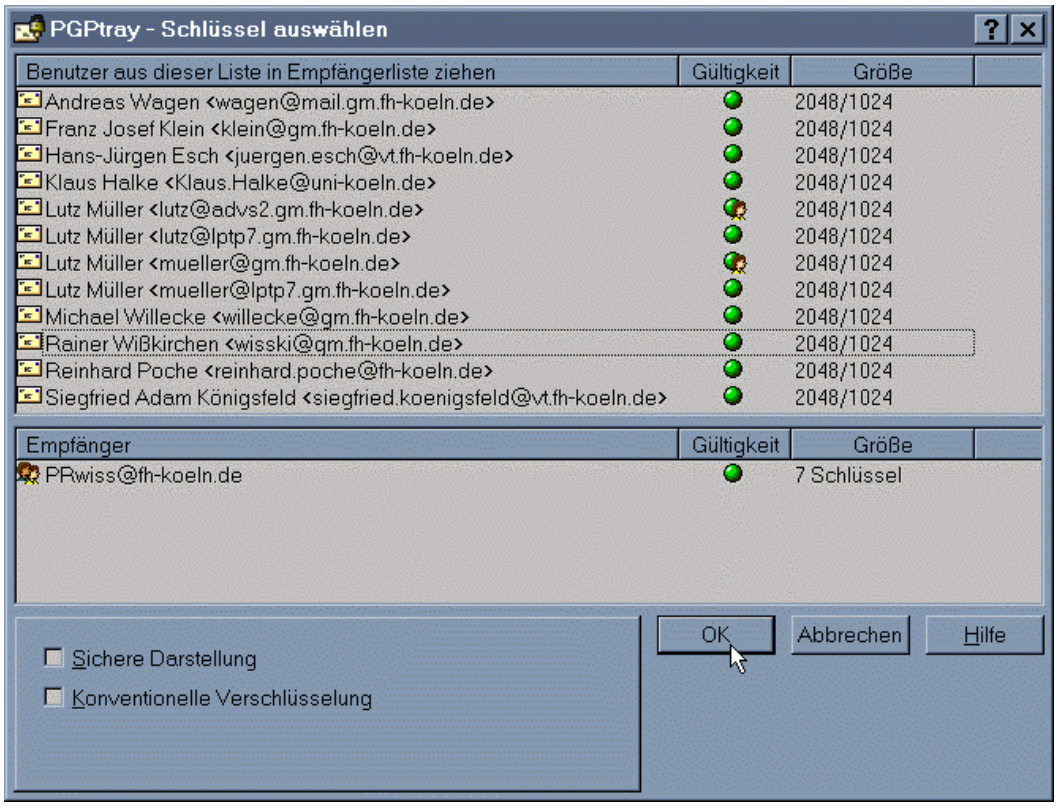
Im Zusammenspiel von PGP und der Windows Zwischenablage geht man wie folgt vor.



Markieren Sie den Text innerhalb der Anwendung mit der Maus bzw. [Strg-A]. Rufen Sie danach bitte [Strg-C] bzw. via Menü die Kopierfunktion auf. Nach Ausführen dieser Funktion stehen die markierten Daten in der Zwischenablage zur weiteren Bearbeitung bereit.

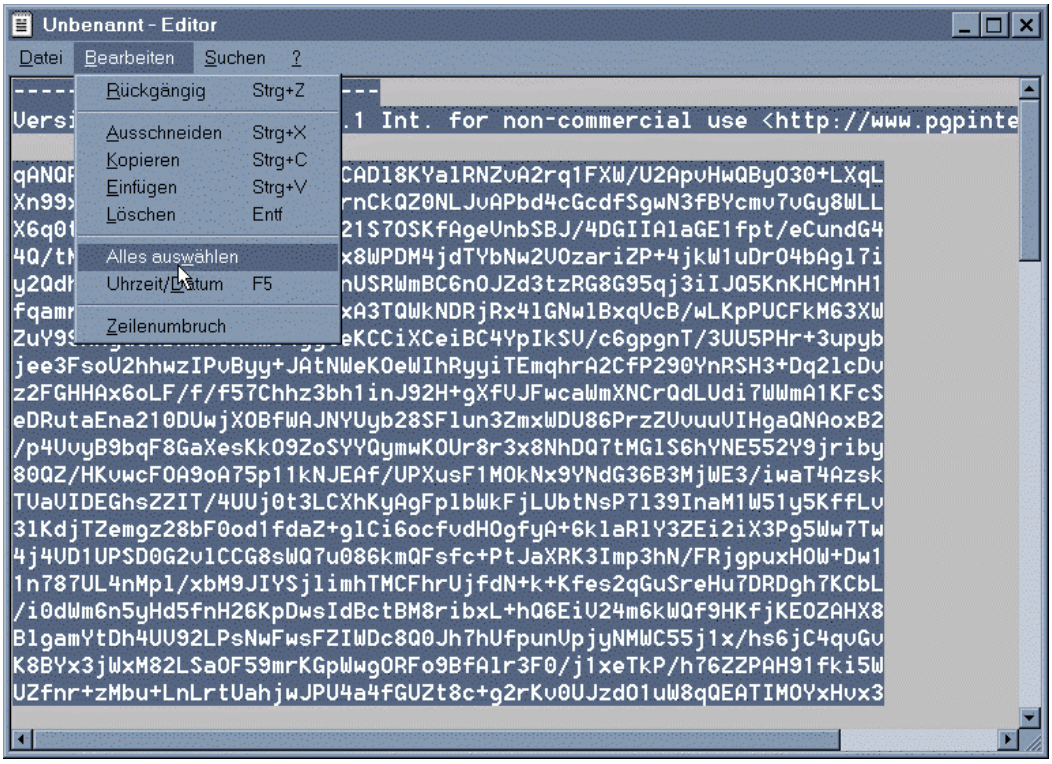


„Wie gehabt“ rufen Sie bitte mit **PGPtray⇒Zwischenablage⇒Verschlüsseln und unterschreiben** die gleichlautende Funktion auf.

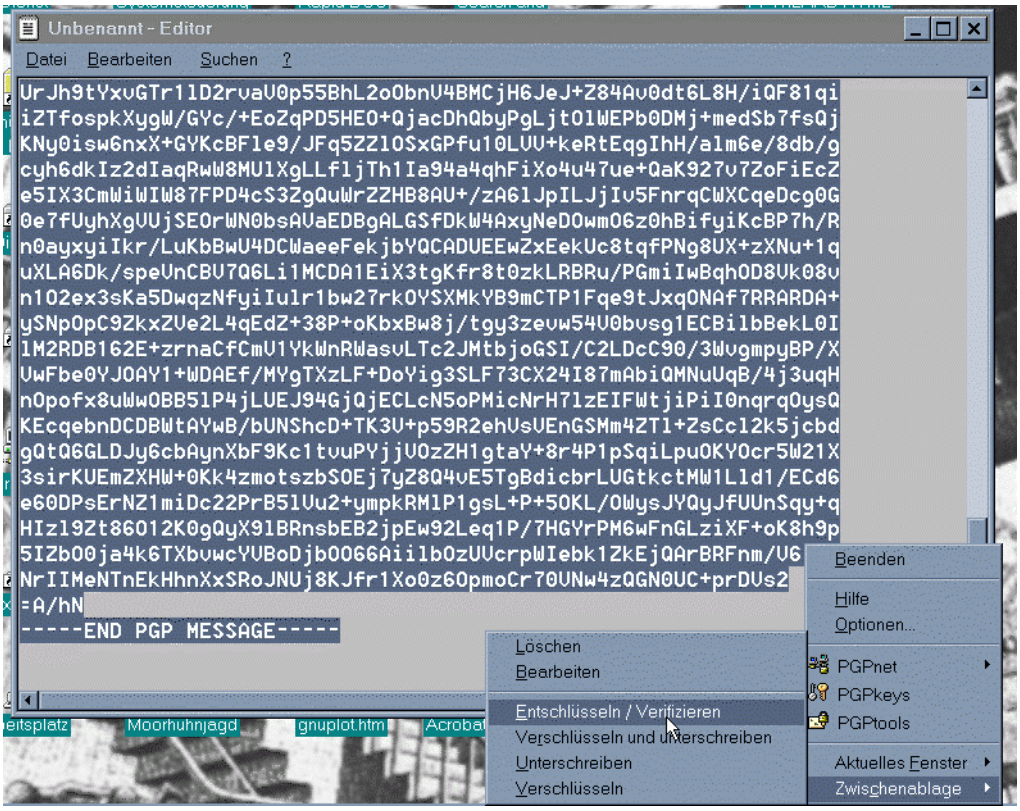


Da Sie auch verschlüsseln möchten benötigt PGP die öffentlichen Schlüssel der Empfänger sowie Ihre Passphrase (deren Eingabedarstellung ersehen Sie aus 5.6). Nach erfolgreicher Verschlüsselung und Signatur der Daten in der Zwischenablage können diese mit [Strg-V] bzw. Einfügen als „Verschlüsselten-Text“ in die Anwendung zurückgeschrieben werden.

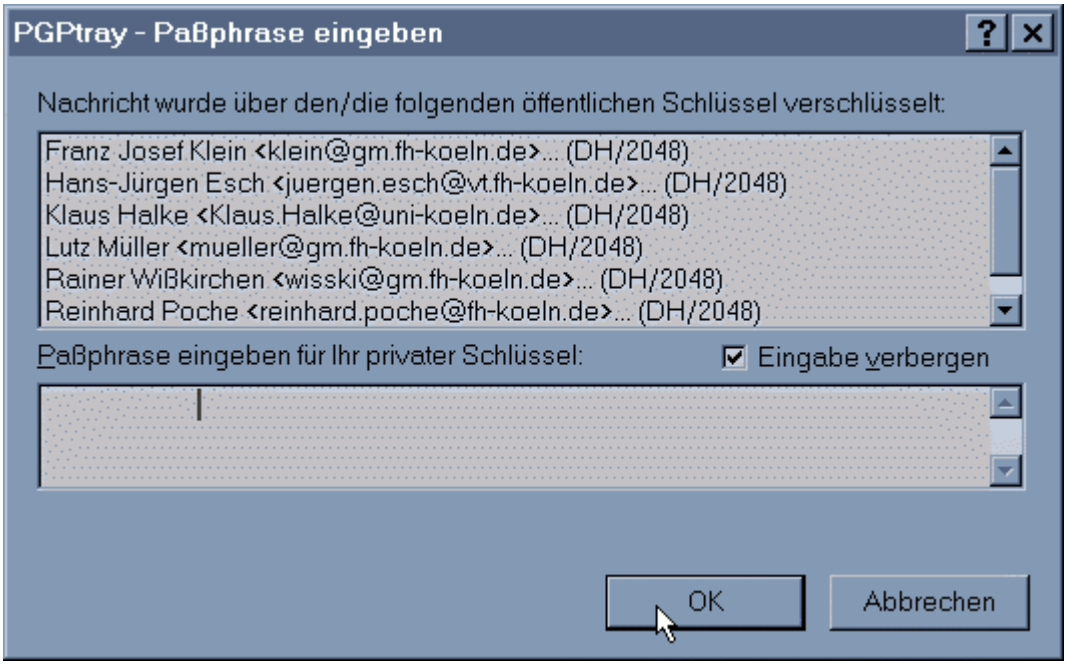
Wenn Sie daraus dann erneut Klartext machen möchten gehen Sie bitte wie folgt beschrieben vor:



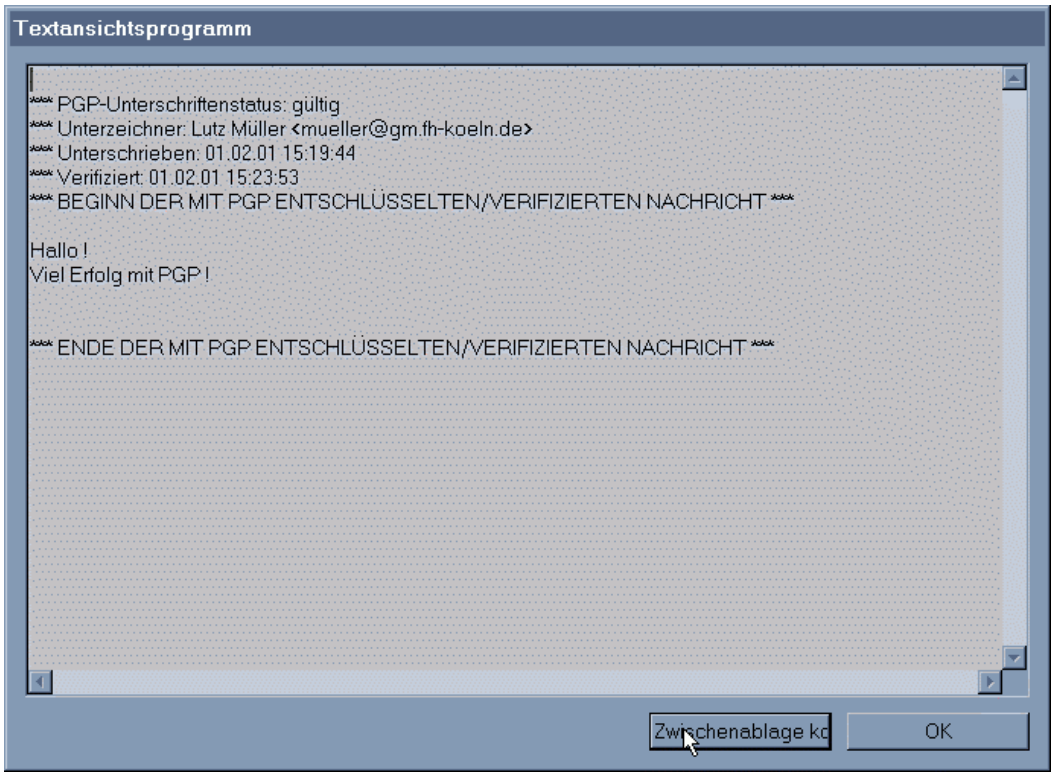
Das Markieren des verschlüsselten Textes ist mit der Maus bzw. mit [Strg-A] zu erreichen. Wenn im weiteren Verlauf der Bearbeitung [Strg-C] bzw. die Kopieren Funktion ausgeführt wird „landen" diese Daten in der Zwischenablage.



Mit oben dargestellter PGPtray Funktion starten Sie den Entschlüsseln/Verifizieren Vorgang.



Die Eingabe Ihrer Passphrase ist zum Entschlüsseln unbedingt notwendig.

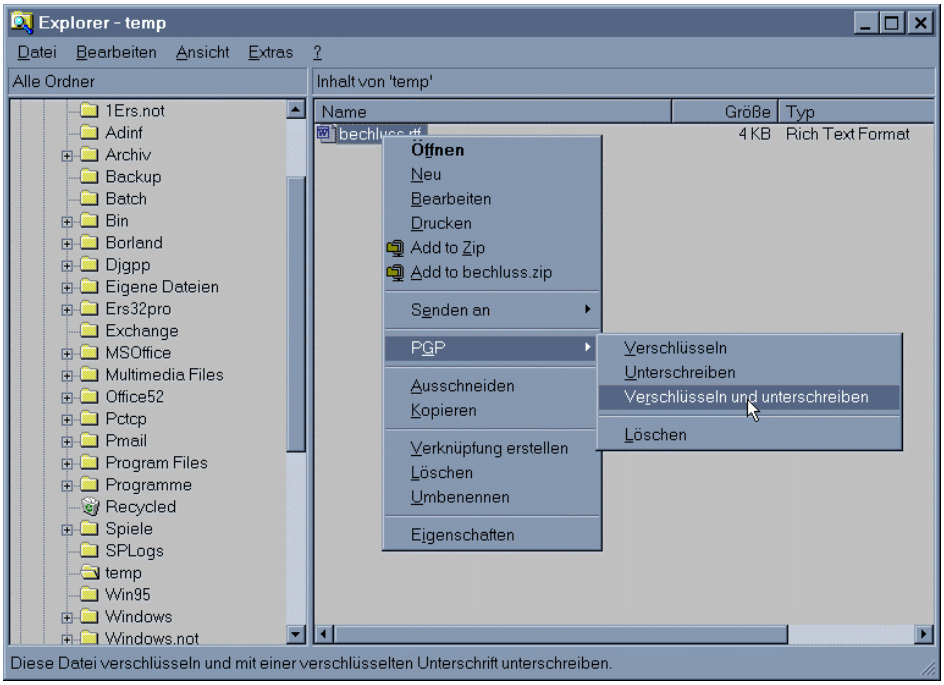


Und siehe da, der Klartext erscheint erneut im PGP-Textansicht-Fenster. Wenn [Zwischenablage kopieren] ausgeführt wird schreibt Windows oben angezeigte Daten in die Zwischenablage. Damit stehen diese Daten dann fast allen Windowsanwendungen zur Verfügung.

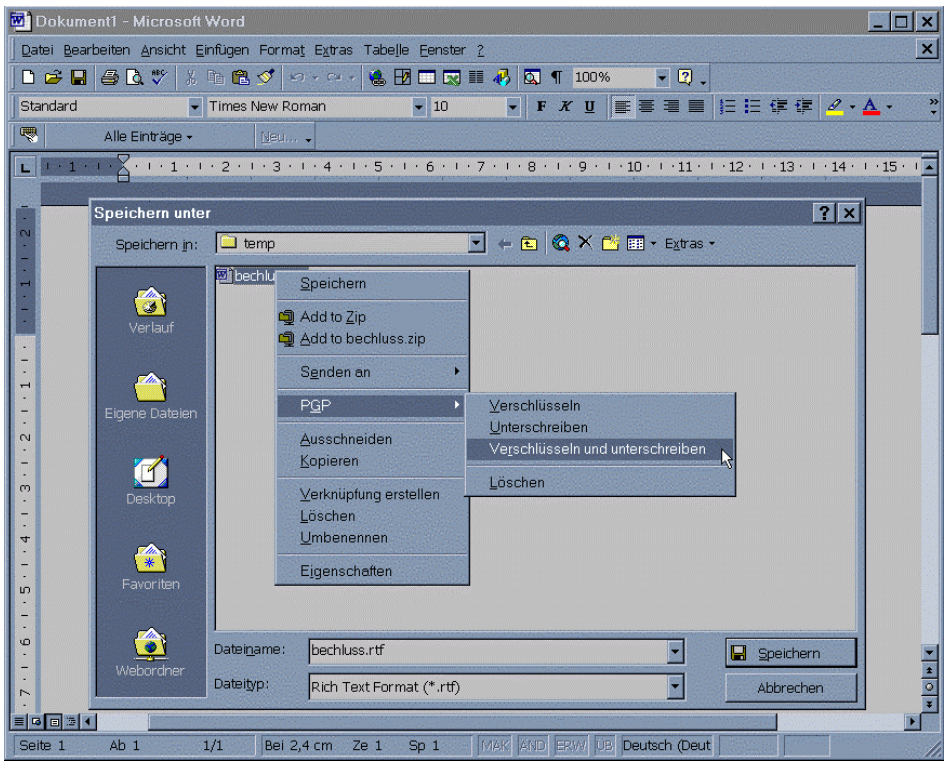
5.8 PGP und Standardanwendungen

Vorstehend erläuterte PGP Funktionen können unter MS Windows 9x/NT/2000 auch aus (fast) allen modernen Anwendungen heraus aufgerufen werden.

Nachfolgend zwei Beispiele:



Hier sehen Sie die Darstellung der PGP Anwendung „innerhalb“ des Explorers von Windows 95.



Hier die moderne Variante der Zusammenarbeit PGP mit MS Winword 2000.

Bedient wird dieses m.E. recht bequeme Arbeiten innerhalb von Anwendungen indem man mit der **linken** Maustaste, in dem entsprechenden Fenster der Anwendung, die Datei(en) markiert die zur Bearbeitung mit PGP vorgesehen sind. Wenn danach sofort die **rechte** Maustaste betätigt wird, öffnet sich ein sog. „pull down Menu" in dem u.a. auch die wichtigsten PGP-Funktionen zur Verfügung stehen. Diese Anwendung unterscheidet sich nicht wesentlich von dem was in 5.5 beschrieben wurde, darum erspare ich Ihnen und mir eine weitere Darstellung der Zusammenhänge.

6.PGP Kurzeinführung für Ungeduldige

Nachfolgend ein „Kochrezept“ zur kurzen Einführung von PGP auf Windows PC.

- Besorgen Sie sich die notwendige Software via http://www.pgpi.org . Achten Sie darauf das Sie sich eine „deutschsprachige internationale“ Version herunterladen, und dass Sie diese Freeware Version nicht für dienstliche Belange einsetzen können. Erkundigungen nach PGP Lizenzen für dienstliche Anwendungen richten Sie bitte an die Fachleute der ZI oder „besuchen“ Sie die Website http://www.pgp.com/international/germany/ . Wenn Sie PGP „innerhalb“ des Netscape Messager anwenden möchten, benötigen Sie nach das entsprechende „Plugin“, welches Sie unter http://bear-software.freeservers.com/downloads.html erhalten

- Installieren Sie PGP mit den notwendigen „Plugin“

- Erzeugen Sie sich das unbedingt notwendige „eigene“ Schlüsselpaar. In erster Näherung ist die Voreinstellung DH/DSS 2028/1024 Bit ok. Beachten Sie aber das in Zukunft wahrscheinlich ein RSA Schlüsselpaar Verwendung findet

- Spielen Sie mit PGP ! D.h. verschlüsseln und signieren Sie Dateien und Emails erst einmal mal für den eigenen Gebrauch

- Fragen sie bei unserer ZI nach ob mittlerweile eine Zertifizierungsstelle an unserer Fachhochschule besteht. Wenn ja, lassen Sie sich dort Ihren öffentlichen Schlüssel signieren

- Tauschen Sie mit Ihren Kommunikationspartnern öffentliche Schlüssel aus. Zunächst via Diskette oder Email später evtl. via internen und externen Schlüsselservern aus

- Prüfen Sie die erhaltene öffentliche Schlüssel indem Sie die Signaturen dieser Schlüssel überprüfen. Dazu benötigen Sie den öffentlichen Schlüssel der Zertifizierungsstelle, oder überzeugen sich z.B. via telefonischer Rückfrage von der Richtigkeit der „Fingerabdrücke“

- Nutzen Sie PGP so oft wie möglich um Erfahrungen mit diesem Produkt zu sammeln

- Vergessen Sie Ihre Passphrase nicht

- Verlieren Sie Ihr Schlüsselpaar nicht

- Signieren Sie keine öffentliche Schlüssel anderer Leute weil Sie dritten Personen einen Gefallen erweisen wollen

7.Glossar

3DES

3DES Triple-DES erhöht die Sicherheit vom normalen DES-Verfahren, indem die Daten mit doppelter (112 Bit) oder dreifacher (168 Bit) Schlüssellänge verschlüsselt werden.

ADK

Bedeutet Additional Decryption Key. Wird dieser Schlüssel angewendet kann eine „dritte Person", in der Regel ist dass der Sicherheitsbeauftragte, Ihre Daten entschlüsseln.

CA

Die Certificate Authority ist eine Zertifizierungsstelle, die digitale Verschlüsselungen zur Übermittlung vertraulicher Daten, zum Schutz vor Manipulationen und zur Identitätsprüfung des Urhebers vergibt. Siehe auch Digitale Signatur.

CAST

Beim Algorithmus CAST, der vermutlich nach seinen Autoren Carlisle Adams und Stafford Tavares benannt wurde, handelt es sich um ein relativ neues Verfahren für das symmetrisches Verschlüsseln. PGP ab Version 5.0 nutzt die kostenfrei verfügbare konkrete Realisierung CAST-128 (auch CAST5 genannt) mit 128-Bit-Schlüsseln.

DES

Ein symmetrisches Verschlüsselungsverfahren DES steht für Data Enryption Standard und ist ein normiertes Verfahren zur Verschlüsselung von Daten. DES ist zwar weit verbreitet, allerdings nicht mehr zeitgemäß aufgrund der geringen Schlüsselgröße von 56 Bit.

DH

Unsymmetrisches Verschlüsselungsverfahren benannt nach Diffie-Hellman. Eine Alternative zu RSA

DSA

Unsymmetrisches Verschlüsselungsverfahren. Der Digital Signature Algorithm (DSA) wurde vom National Institute of Standards and Technology (NIST) im Rahmen des Digital Signature Standard (DSS) veröffentlicht, der selbst Teil des US-Regierungsprojektes Capstone ist. DSS wurde vom NIST in Zusammenarbeit mit der NSA ausgewählt, um einen elektronischen Unterschriftenstandard für die US-Behörden zu erhalten. Dieser Standard wurde am 19. Mai 1994 veröffentlicht.

DSS

Verfahren zur Erstellung elektronischer Unterschriften. Digital Signature Standard (DSS), siehe auch DSA

Einweg-Hashfunktionen

Mit diesen Funktionen wird das Hash-Komprimat aus einer Nachricht bzw. einer Datei erzeugt. PGP ab Version 5.0 unterstützt Einweg-Hashfunktionen nach den Verfahren MD5, SHA-1 und RIPEMD-160.

ElGamal

Dieses unsymmetrische Verschlüsselungsverfahren ist nach seinem Erfinder Taher ElGamal benannt. PGP ab Version 5.0 unterstützt dieses Verfahren.

Fingerabdruck (Fingerprint)

Jeder PGP Schlüssel trägt einen einmaligen Fingerabdruck. Es ist eine zufällige Zeichenfolge, die es nur einmal gibt und einen Schlüssel eindeutig kennzeichnet. Anhand eines Fingerabdruckes kann man die „Richtigkeit" eines Schlüssel prüfen. z.B. A sendet B seinen privaten PGP Schlüssel via Email. Nach erhalt der Email kann B telefonisch A Kontakten und anhand durchgesagter „Codewörter", die als ganzes eben den Fingerabdruck wiedergeben, die „Richtigkeit" des privaten Schlüssels von A überprüfen. Dieses Verfahren gilt als „unsicherer" als der persönliche Austausch von Schlüsseldaten oder die Verwendung eines „sicheren" Schlüsselservers.

GnuPG

GnuPG bedeutet „Gnu Privacy Guard", übersetz also „Gnu-Wächter für Privatsphäre", wobei das Akronym „Gnu" für „Gnu is not Unix" steht". GnuPG ist eine freie Implementation des OpenPGP-Standards, der aus dem Datenformat von PGP 5.x/6.x entwickelt wurde. Es ist derzeit unter den meisten Unix-Varianten und Windows 95/98/NT einsetzbar. PGP und GnuPG sind kompatibel.

Hash-Komprimat

Ein Bestandteil der elektronischen Unterschrift. Eine Hash-Funktion wandelt eine Nachricht, eindeutig und nicht verwechselbar, in ein nur dieser Nachricht zu ort bares Hash-Komprimat. Dieses Hash-Komprimat kann man sich durchaus als „digitalen Fingerabdruck" einer Nachricht vorstellen. Zur Bildung eines Hash-Komprimats benutz PGP sog. Hash-Funktionen nach **MD5**, **SHA-1** oder **RIPEMD-160**.

Hybride Verschlüsselung

Ist eine Kombination der unsymmetrischen mit der symmetrischen Verschlüsselung. Es wird ein geheimer und einmaliger Sitzungsschlüssel erzeugt, mit diesem werden die Daten symmetrisch Verschlüsselt. Der Sitzungsschlüssel selber wird unsymmetrisch verschlüsselt. Mit diesem „Trick" erreicht man den Geschwindigkeitsvorteil der symmetrischen Verfahren und die Anwenderfreundlichkeit der unsymmetrischen Verfahren.

IDEA

Ein symmetrisches Verschlüsselungsverfahren. DEA steht für International Data Encryption Algorithm und ist ein block-orientierter, konventioneller Verschlüsselungsalgorithmus, der an Eidgenössischen Technischen Hochschule der Schweiz entwickelt wurde. Das IDEA Verfahren gilt als „Sicher" und wird von PGP verwendet.

Kryptanalyse

Methoden und Verfahren, um verschlüsselte Daten ohne vorherige Kenntnis des Schlüssels zu entschlüsseln.

Kryptographie

Die praktische Anwendung der Kryptologie.

Kryptologie

Die Wissenschaft vom Verschlüsseln von Informationen. Nicht alle Länder, wie z.B. China oder auch Frankreich, erlauben verschlüsselte Übertragungen. Telefon, Fax oder Internet-Daten sind davon betroffen. Siehe auch Seite „Verschlüsselung/Kryptographie".

Mantra

Ein anderes Wort für die PGP Passphrase.

MD5

MD5, das MD steht für Message Digest, ist ein Verfahren um aus einer Nachricht ein Hash-Komprimat zu bilden. Dieser „Fingerabdruck" einer Nachricht hat die Länge von 128 Bit. Das Verfahren MD5 stammt von Ronald Rivest und wurde 1992 im RFC 1321: The MD5 Message-Digest Algorithm beschrieben. PGP arbeitet u.a. mit MD5.

NSA

Die National Security Agency ist ein amerikanischer Geheimdienst, größer als die CIA, die keiner demokratischen Kontrolle unterworfen ist. Ihr jährlicher Etat wird auf 10 bis 15 Milliarden Dollar für 60 000 bis 100 000 Mitarbeitern geschätzt. Die NSA-Zentrale befindet sich seit 1957 auf der Armee-Basis Fort Meade in Maryland. Zusammen mit anderen UK/USA-Staaten betreibt die NSA den internationaler Abhörring ECHELON.

PGP

Steht für Pretty Good Privacy und ist ein Programm zur Verschlüsselung von Emails. Im Email-Bereich ist PGP mittlerweile zu einem Quasi-Standard geworden und wird von sehr vielen Leuten eingesetzt. PGP setzt intern mehrerer Verschlüsselungsverfahren ein.

PGP - Öffentlicher Schlüssel (public key)

Ein wesentlicher Bestandteil unsymmetrischen Verfahren. Der öffentliche Schlüssel wird benötigt um:

- Daten für einen bestimmten Empfänger zu verschlüsseln
- Daten die mit einer elektronischen Unterschrift versehen zu auf Echtheit zu überprüfen

PGP - Passphrase

Eine Passphrase ist ähnlich einem Passwort, nur dass man hier ganze Sätze (Phrasen) inklusive Sonderzeichen und Leerzeichen angeben werden können, z.B. „Ich trinke gerne Bier". Eine Passphrase ist aufwendiger zu „knacken" und somit sicherer als ein Passwort. Beim Verschlüsselungsprogramm PGP wird dies auch als „Mantra" bezeichnet.

PGP - Schlüsselkennungen

Jeder PGP-Schlüssel hat zusätzlich zum Namen und der Email-Adresse eine Kennung, die aus den Schlüsseldaten abgeleitet wird.

PGP - Schlüsselzertifikate

Ein Schlüsselzertifikat enthält den öffentlichen Schlüssel. Dieser Eintrag besteht aus mehreren langen Zahlen. Hinzu kommt ein Texteintrag, der angibt, wem dieser Schlüssel gehört.

PGP Netz des Vertauens (Web auf Trust)

Eine Möglichkeit um über Vertrauensgerade von Unterzeichnern von öffentlichen Schlüssel deren Echtheit zu Überprüfen.

Primzahl

Eine Primzahl ist eines Zahl die im Bereich der ganzen Zahlen nur durch die Zahl 1, oder durch sich selber ohne Rest teilbar ist. Große Primzahlen spielen bei Verschlüsselungsverfahren eine wesentliche Rolle.

Privater Schlüssel (privat key)

Ein wesentlicher Bestandteil von unsymmetrischen Verfahren. Der **geheime** private Schlüssel wird benötigt um:

- Daten die mit dem entsprechenden öffentliches Schlüssel verschlüsselt wurden zu entschlüsseln
- Daten mit einer elektronischen Unterschrift zu versehen

RIPEMD-160

Ist ein Verfahren welches eine Einweg-Hash-Funktion definiert die ein Hash-Komprimat von 160 Bit Länge erzeugt. RIPEMD-160 wurde entwickelt von Hans Dobbertin, Antoon Bosselaers und Bart Preneel. PGP an Version 5.0 unterstützt dieses Verfahren.

RSA

Steht für Rivest, Shamir und Adleman, die diesen Algorithmus zur Verschlüsselung von Daten entwickelt haben. Bei diesem Verfahren werden zwei große Primzahlen zu einer noch größeren Primzahl verknüpft, die dann als Schlüssel dienen kann. RSA arbeitet mit öffentlichen Schlüsseln (Public-Keys) und gilt als sehr sicher. RSA ist in den USA patentiert, darf aber frei genutzt werden. Das Patent ist im Jahr 2000 abgelaufen.

Schlüssel

Als Schlüssel bezeichnet man eine Einheit von digitalen Daten von bestimmter Länge. Ein Schlüssel wird verwendet um zusammen mit einem Verschlüsselungsverfahren um einen Datei, Email oder Filesystem zu verschlüsseln bzw. zu entschlüsseln.

Schlüsselmanagement

Die Erzeugung, Übertragung neuer Schlüssel, und die Verwaltung bestehender Schlüssel wird mit diesem Begriff bezeichnet. Das Schlüsselmanagement kann auch von einer Schlüssel-Zertifizierungsstelle unterstützt werden.

SHA-1

Ist der Secure Hash Algorithm. Es handelt sich hierbei um eine Einweg-Hash-Funktion zur Erzeugung eines Hash-Komprimats mit 160 Bit Länge. PGP unterstützt dieses Verfahren.

Signature

- Einige Zeilen Text, die Namen, Firma, Adresse, Telefon/Fax, oft auch einen guten Spruch des Autors am Ende eines Emails oder eines News-Artikels.
- Elektronische Unterschrift, die den Unterschreibenden als Urheber bestätigt. Eine elektronische Unterschrift kann an den Inhalt eines Dokumentes (z.B. Text einer Email, Überweisungsauftrag, öffentlicher PGP-Schlüssel) gekoppelt werden. Ändert einer das Dokument, passt die elektronische Unterschrift nicht mehr zu dem ursprünglichen Dokument, zu dem die Unterschrift gemacht wurde. Jede Änderung des Dokumentes lässt die elektronische Unterschrift ungültig werden.

Steganografie

Verschlüsselung von Daten in sogenannten Trägerdateien. In unauffälligen Sound-, Text- oder Grafikdateien werden Botschaften versteckt. Einer verschlüsselten Email sieht man an, dass hier etwas verschlüsselt wurde. Wer aber denkt schon bei einer Email mit harmlosen Inhalt daran, dass in der mitgeschickten Bilddatei die eigentliche Information versteckt ist. Besonders sicher, weil von einem Angreifer erst einmal nicht erkannt, ist die Anwendung der Steganografie zusammen mit modernen Verschlüsselungsverfahren.

Symmetrische Verschlüsselung

Beim Ver- und Entschlüsseln wird derselbe Schlüssel verwendet. Vorteil: Sehr schnell und effizient. Nachteil: Es gibt nur einen Schlüssel, dieser muss auf einem „geheimen" Weg zwischen Sender und Empfänger der verschlüsselten Nachricht ausgetauscht werden.

Unsymmetrische Verschlüsselung

Unsymmetrische Verfahren beruhen darauf, dass man unterschiedliche Schlüssel zum Ver- und, Entschlüsseln verwendet. Zum Verschlüsseln wird ein öffentlicher (public key) Schlüssel verwendet. Das Entschlüsseln kann dann nur durch einen privaten (privat key) Schlüssel erfolgen. Somit ist ein Schlüssel immer frei zugänglich, mit dem man aber die Nachricht nicht wieder entschlüsseln kann. Das Prinzip der unsymmetrischen Verschlüsselung beruht darauf, dass es mathematische Verschlüsselungsfunktionen gibt, von denen man aber praktisch nicht die geeignete Entschlüsselungsfunktion ableiten kann. Man spricht in diesem Zusammenhang auch von „Falltürfunktionen".

Zufallszahl

Das wesentliche Merkmal einer Zufallszahl ist dass diese nicht berechnet werden kann. „Richtige" Zufallszahlen können auf dem PC nur durch menschliches Zutun, z.B. durch wahlloses bewegen der Maus bzw. durch ganz spezielle Einsteckkarten erzeugt werden. Zufallszahlen spielen eine große Rolle bei diversen Verschlüsselungsverfahren.

8. Quellenangaben

8.1 Konventionelle Quellen

- Addision-Wesley, „Datenkommunikation und elektronische Post“ von Plattner/Lanz/Lubich/Müller/Walter
- c’t 2/2001 S.60, „Wer braucht digitale Signaturen ?“ von Stefan Krempl
- Spektrum der Wissenschaft 12/1988 S.8, „Die Geschichte der legendären ENIGMA“ von Dewdney
- Spektrum der Wissenschaft 1/1989 S.6, „Über moderne Computer-Verschlüsselungsmethoden“ von Dewdney
- Springer Lehrbuch, „Kryptologie“ von Bauer

8.2 Internet Quellen

- http://www.heise.de/ct/pgpCA/default.shtml
- http://www.helmbold.de/pgp/pgp6.5/anleitung.htm
- http://www.iiv.de/obertfk/vereine/fbo/helpdesk/kurse/pgp/index.html
- http://www.informatik.uni-rostock.de/~kleinau/diplom/index.html
- http://www.informatik.uni-rostock.de/~kleinau/diplom/index.html
- http://www.nordrhein-westfalen.datenschutz.de/fachbereich/fach_7_3_2.html
- http://www.pgp.com/international/germany/
- http://www.pgpi.org/doc/faq/pgpi/de/
- http://www.thomas-kriener.de/wpf/pgp/