Bundesministerium
für Wirtschaft
und Technologie

GnuPP für Einsteiger

Der Schnelleinstieg zum E-Mail-Verschlüsselungssystem GNU Privacy Projekt

Ihr freier Schlüssel zur E-Mail-Sicherheit!

Mit kompletter Software, Cartoons und Adele, dem E-Mail-Roboter

GnuPP für Einsteiger

Schnelleinstieg zum E-Mail-Verschlüsselungsprogramm GnuPP

Herausgegeben und gefördert vom
Bundesministerium für Wirtschaft und Technologie
Scharnhorststr. 34-37
10115 Berlin

Ansprechpartner:
Bundesministerium für Wirtschaft und Technologie
Referat Öffentlichkeitsarbeit

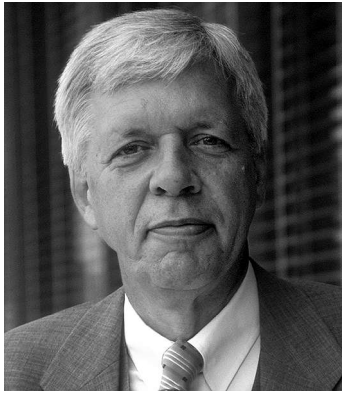
Impressum

Diese Seite darf nicht verändert werden.

Autor: Manfred J. Heinze, TextLab text+media
Beratung: Lutz Zolondz, G-N-U GmbH
Illustrationen: Karl Bihlmeier, Bihlmeier & Kramer GbR
Layout: Isabel Kramer, Bihlmeier & Kramer GbR
Fachtext: Dr. Francis Wray, e-mediate Ltd.
Redaktion: Ute Bahn, TextLab text+media

1. Auflage, März 2002

Wie das OpenSource-Kryptografieprogramm GnuPP selbst wurden
diese Texte nicht für Mathematiker, Geheimdienstler und
Kryptografen geschrieben, sondern für jedermann.



Sicherheit durch Offenheit

Liebe Anwender der Freien Software GnuPP,

bisher hat man oft versucht, Software dadurch zu schützen, dass man möglichst wenige Informationen darüber preisgab. Trotzdem werden immer wieder schwerwiegende Sicherheitslücken in solch geschlossenen Software-Systemen gefunden und zu Hackerangriffen missbraucht. Wir setzen deshalb auf „Sicherheit durch Offenheit". Denn die öffentliche Diskussion über erkannte Schwachstellen hilft, Sicherheitslecks schnell zu beseitigen oder gar nicht erst entstehen zu lassen.

Deshalb unterstützt das Bundesministerium für Wirtschaft und Technologie die Entwicklung des Open-Source-Verschlüsselungsprojektes „GNU Privacy Projekt" (GnuPP) . GnuPP ist eine sichere, einfache und kostenlose Verschlüsselungssoftware. Sie ermöglicht es jedem Bürger und jedem Unternehmen, seine Grundrechte auf vertrauliche Kommunikation über das Internet zu wahren und die Rechtsverbindlichkeit, Integrität und Authentizität der Kommunikation zu überprüfen.

Gerade für den Verkehr mit und zwischen den Behörden spielt das eine wichtige Rolle. Denn mit der flächendeckenden Einführung der digitalen Signatur in der Bundesverwaltung - wie sie die Bundesregierung beschlossen hat - können Bürgerinnen und Bürger ihren Rechts- und Geschäftsverkehr mit den Bundesbehörden künftig auch über das Internet sicher abwickeln.

Ich wünsche allen Anwendern von GnuPP eine lebhafte und sichere E-Mail-Kommunikation.

Werner Müller

Dr. Werner Müller
Bundesminister für Wirtschaft und Technologie.

1. Über dieses Handbuch

Das GnuPP-Anleitungs- und Übungsmaterial besteht aus drei Teilen:

dem gedruckten Schnelleinstieg, „GnuPP für Einsteiger", in dem Sie gerade lesen,

dem Handbuch „GnuPP für Durchblicker" im PDF-Format, das Sie auf der beiliegenden CD-ROM und nach der Installation von GnuPP auf Ihrer Festplatte finden,

dem GnuPP-Übungsroboter Adele, mit dem Sie die E-Mail-Ver- und –Entschlüsselung so oft üben können, wie Sie wollen. Um mit Adele zu üben, brauchen Sie eine Internet-Verbindung.

„GnuPP für Einsteiger" führt Sie kurz und knapp durch die Installation und die alltägliche Benutzung der GnuPP-Software. Der Zeitbedarf für das Durcharbeiten des Schnelleinstiegs hängt unter anderem davon ab, wie gut Sie sich mit Ihrem PC und Windows auskennen. In etwa sollten Sie sich eine halbe Stunde Zeit nehmen.

„GnuPP für Durchblicker" liefert Hintergrundwissen, das Ihnen die grundlegenden Mechanismen von GnuPP verdeutlicht und die etwas seltener benutzten Features erläutert. Das Handbuch liegt im PDF-Format vor, Sie können es auch ausdrucken.

Beide Handbuchteile können unabhängig voneinander benutzt werden. Zu Ihrem besseren Verständnis sollten Sie aber möglichst beide Teile in der angegebenen Reihenfolge lesen.

☞ **Diese Hand weist auf den Wechsel in das andere Buch hin**

Der GnuPP-Übungsroboter Adele steht Ihnen jederzeit im Internet zur Verfügung. Sie empfängt und sendet verschlüsselte E-Mails und entschlüsselt sie auch. Sie können also mit Adele einen kompletten Verschlüsselungsdialog so lange üben, bis Sie sich völlig mit dem Gebrauch der Software vertraut gemacht haben.

2. Was ist GnuPP?

GnuPP (GNU Privacy Projekt) ist eine vom Bundeswirtschaftsministerium geförderte E-Mail-Verschlüsselungssoftware. GnuPP bezeichnet das Gesamtpaket, das die Programme GnuPG, GPA, WinPT und andere Komponenten enthält.

Mit dem Verschlüsselungsprogramm GnuPG (GNU Privacy Guard) kann jedermann E-Mails sicher, einfach und kostenlos verschlüsseln. GnuPG kann ohne jede Restriktion privat oder kommerziell benutzt werden. Die Verschlüsselung von GnuPG ist extrem sicher und kann nach dem heutigen Stand von Forschung und Technik nicht gebrochen werden.

GnuPG ist Freie Software oder Open-Source-Software. Das bedeutet, dass jedermann das Recht hat, sie nach Belieben kommerziell oder privat zu nutzen. Jedermann soll und darf den Quellcode, also die eigentliche Programmierung des Programms, genau untersuchen.

Für eine Sicherheits-Software ist diese garantierte Transparenz des Quellcodes eine unverzichtbare Grundlage. Nur so lässt sich die Vertrauenswürdigkeit eines Programmes prüfen.

GnuPG ist vollständig kompatibel mit PGP

GnuPG basiert auf dem internationalen Standard OpenPGP (RFC 2440), ist vollständig kompatibel zu PGP und benutzt die gleiche Infrastruktur (Schlüsselserver etc).

PGP („Pretty Good Privacy") ist keine freie Software, sie wird seit mehreren Jahren nicht mehr unter der freien Softwarelizenz GNU General Public License (GNU GPL) vertrieben.

Weitere Informationen zu GnuPG und den Projekten der Bundesregierung zum Schutz des Internets finden Sie auf der Website sicherheit-im-internet.de des Bundeswirtschaftsministeriums.

3. Sie installieren GnuPP

Legen Sie die beiliegende CD-ROM in das CD-ROM-Laufwerk Ihres PCs. Öffnen Sie Ihren „Arbeitsplatz" und klicken Sie dort auf das CD-ROM-Icon mit dem Titel „GnuPP".

Wenn sich das CD-ROM-Icon geöffnet hat, klicken Sie auf das Installations-Icon mit dem Titel „gnupp.1.1-de"

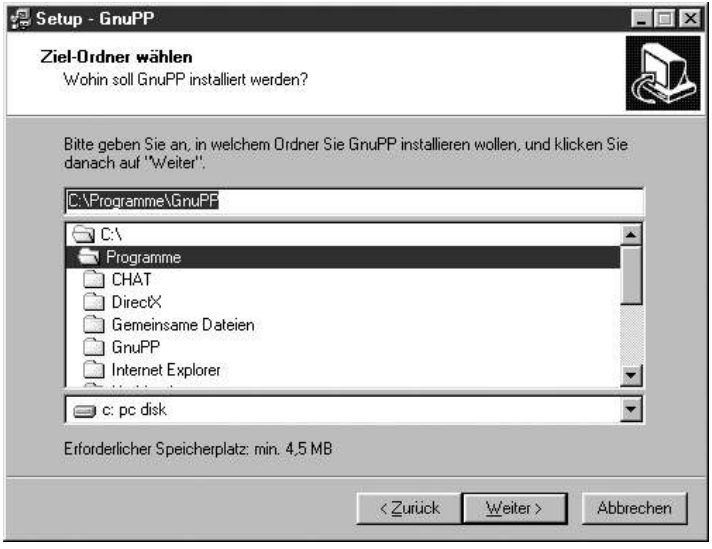
Die Frage, ob Sie das Programm installieren wollen, beantworten Sie mit [Ja].

Es begrüßt Sie dieser Screen:

Beenden Sie alle möglicherweise auf Ihrem Rechner laufenden Programme, und klicken Sie dann auf [Weiter].

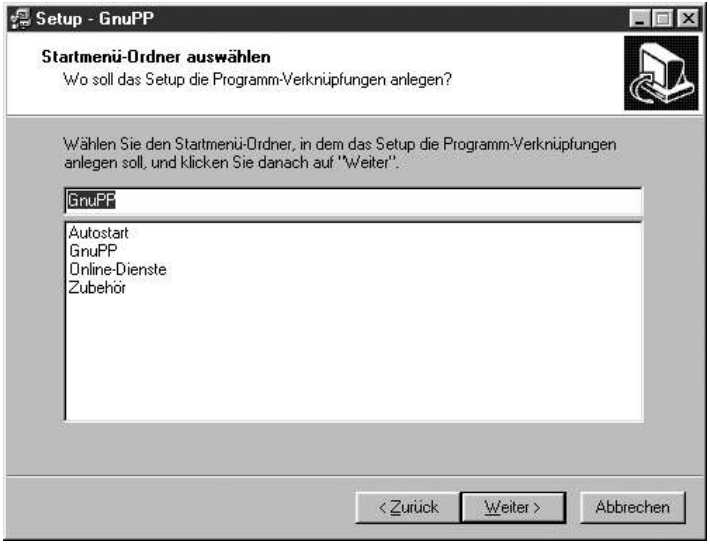
Lesen Sie die Lizenzvereinbarung und – wenn Sie ihr zustimmen – klicken Sie auf [Ja].

In der nun folgenden Dateiauswahl können Sie einen Ordner auf Ihrem PC aussuchen, in dem GnuPP installiert wird. Sie können auch einfach den voreingestellten Standard-Ordner C:\Programme\GnuPP nehmen.



Klicken Sie anschliessend auf [Weiter].

Das Programm legt nun ein Icon in das Windows Startup-Menü, damit Sie GnuPP einfacher starten können.



Am einfachsten übernehmen Sie die vorgeschlagene Einstellung und klicken dann auf [Weiter].

Anschließend werden alle bisherigen Eingaben noch einmal aufgelistet.
Wenn alles in Ordnung ist, klicken Sie auf [Installieren].

Nach kurzer Zeit ist die Installation beendet und dieser Dialog erscheint:

Klicken Sie auf [Fertigstellen] und lesen Sie die Informationen in der kurzen Readme-Datei.

Wenn Sie fertig sind, schließen Sie die Readme-Datei.

Das war's schon!

Sie haben GnuPP installiert und können es gleich zum ersten Mal starten.

Vorher sollten Sie aber im Handbuch „GnuPP für Durchblicker" (PDF-Datei) die Kapitel 3 und 4 lesen. Wir erklären dort den genialen Trick, mit dem GnuPP Ihre E-Mails sicher und bequem verschlüsselt. GnuPP funktioniert zwar auch, ohne dass Sie verstehen warum, aber im Gegensatz zu anderen PC-Programmen wollen Sie GnuPP schließlich Ihre geheime Korrespondenz anvertrauen. Da sollten Sie schon wissen, was vor sich geht.

Außerdem ist die ganze Angelegenheit ziemlich spannend...

Weiter geben wir Ihnen einige Tipps, mit denen Sie sich einen sicheren und trotzdem leicht zu merkenden Passwortsatz ausdenken können.

☞ **Lesen Sie jetzt im Handbuch die Kapitel 3 und 4, und lesen Sie erst danach hier weiter.**

4. Sie erzeugen Ihr Schlüsselpaar

Nachdem Sie gelesen haben, warum GnuPG so sicher ist und wie ein guter Passwortsatz als Schutz für Ihren geheimen Schlüssel entsteht, werden wir Ihr Schlüsselpaar erzeugen.

Eigentlich müsste man so einen wichtigen Schritt ein paar Mal üben können....

Und genau das können Sie auch tun: Sie können den gesamten Ablauf der Schlüsselerzeugung, Verschlüsselung und Entschlüsselung durchspielen, so oft Sie wollen, bis Sie ganz sicher sind.

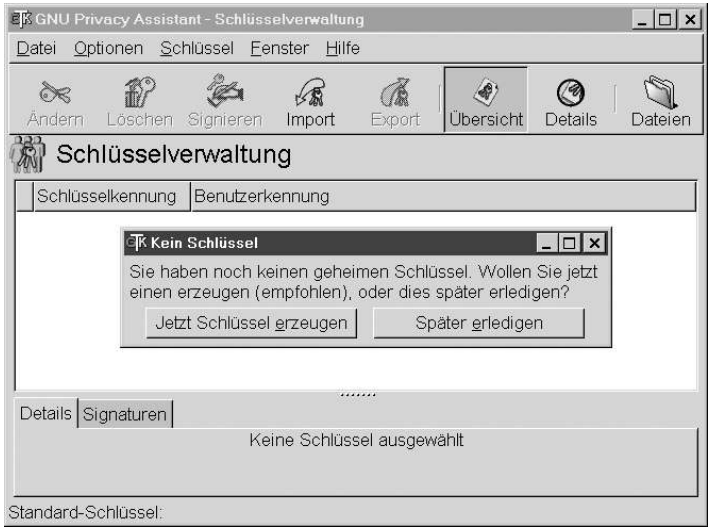
Ihr Vertrauen in GnuPP wird sich durch diese "Trockenübung" festigen, und die "heisse Phase" der Schlüsselerzeugung wird danach kein Problem mehr sein.

Ihr Partner bei diesen Übungen wird Adele sein.

Adele ist ein Testserver, den die Firma G-N-U GmbH – einer der Entwickler von GnuPP – bereitstellt. Mit Hilfe von Adele können Sie Ihre Schlüssel, die wir gleich erzeugen werden, ausprobieren und testen, bevor Sie damit Ernst machen. Doch dazu später mehr.

Los geht's!

Öffnen Sie das Windows Startmenü, dort den Ordner Programme\GnuPP und schließlich das Programm GNU Privacy Assistant. Daraufhin sehen Sie diesen Dialog:



Klicken Sie auf
[Jetzt Schlüssel erzeugen].

Wenn Sie die Schlüsselerzeugung zunächst einmal testen wollen, dann können Sie im nun folgenden Fenster einen beliebigen Namen eingeben, z.B. „Mustermann".

Oder Sie können auch gleich Ernst machen und Ihren richtigen Namen eingeben.

Klicken Sie auf [Weiter], wenn Sie fertig sind.

Als nächstens geben Sie Ihre eigene E-Mail-Adresse an.

Wieder gilt: Sie können die Schlüsselerzeugung zunächst einmal mit irgendeiner ausgedachten E-Mail-Adresse durchtesten, z.B. f.mustermann@firma.de

Oder Sie können auch gleich Ihre echte E-Mail-Adresse eingeben.

Klicken Sie auf [Weiter], wenn Sie die E-Mail-Adresse eingegeben haben.

Anschliessend können Sie einen Kommentar zum Schlüssel eingeben, als z.B. "Schlüssel für Büro-E-Mail". Dieser Kommentar ist nur für Sie sichtbar und wird einem Dritten nicht angezeigt.

Klicken Sie anschliessend auf [Weiter].

Jetzt folgt der wichtigste Teil: die Eingabe Ihres Passwortsatzes.

Erinnern Sie sich an das Kapitel 4, „Der Passwort-Satz" im Handbuch „GnuPP für Durchblicker" das Sie eben durchgelesen haben? Wir haben Ihnen dort einige Tipps zur Erzeugung eines sicheren Passwortsatzes gegeben.

Dann sollten Sie nun einen geheimen, einfach zu merkenden und schwer zu knackenden Passwortsatz parat haben und hier eintragen.

Falls der Passwortsatz nicht sicher genug sein sollte, werden Sie darauf hingewiesen.

Auch an dieser Stelle können Sie – wenn Sie wollen – zunächst einen Test-Passwortsatz eingeben oder auch gleich „Ernst machen".

Wenn Sie Ihren geheimen Passwortsatz zweimal eingegeben haben, klicken Sie auf [Weiter].

Im nächsten Dialog werden Sie gebeten, eine Sicherheitskopie Ihres Schlüssels anzulegen. Tun Sie das jetzt, auch wenn Sie den Ablauf nur üben:

Speichern Sie die Sicherungskopien auf einer Diskette, die Sie sicher verwahren können. Auf einer Diskette, die Sie an einem sicheren Ort aufheben, ist Ihr geheimer Schlüssel wesentlich besser geschützt als auf der Festplatte Ihres PCs.

Wenn Sie keine Sicherungskopie angelegt haben, werden Sie an mehreren Stellen – z.B. bei einem neuen Programmstart – daran erinnert.

Fertig? Dann klicken Sie auf [Fertig] und Ihre Schlüssel werden endgültig erzeugt.

Wenn der PC Ihre Schlüssel berechnet hat, erscheint dieser Hinweis.

In der Mitte des Fensters – hinter dem Symbol der doppelten Schlüssel – sehen Sie Ihr soeben erzeugtes Schlüsselpaar.

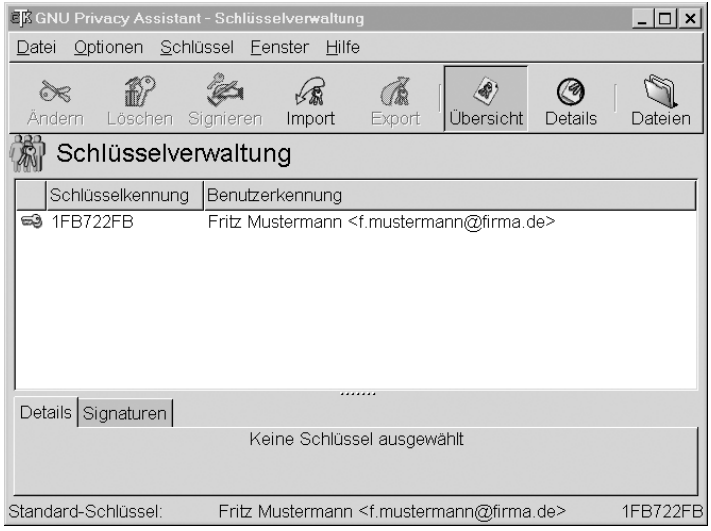
Wenn Sie Ihr Schlüsselpaar anklicken, sehen Sie einige Details, die Sie gleich nachlesen können.

Was bedeuten die Anmerkungen über Ihren Schlüssel?
Ihr Schlüssel ist unbegrenzt gültig d.h., er hat kein „eingebautes Verfallsdatum". Man kann die Gültigkeit nachträglich verändern – mehr dazu später.

Ein Schlüssel mit einer Länge von 1024 Bit ist ein sehr sicherer Schlüssel, der trotzdem nicht zuviel Rechenpower auf Ihrem Computer beansprucht.

Klicken Sie nun auf [Schliessen].

Voila - Ihre Schlüssel sind fertig! Und so sehen sie aus:



Damit ist die Installation von GnuPP und die Erzeugung Ihres Schlüsselpaares abgeschlossen. Sie besitzen nun einen einmaligen und extrem sicheren digitalen Schlüssel.

☞ **Lesen Sie nun im Handbuch Kapitel 5 „Schlüssel im Detail" weiter. Sie können dieses Kapitel jetzt lesen oder später, wenn Sie diese Informationen benötigen.**

5. Sie veröffentlichen Ihren Schlüssel per E-Mail

Beim täglichen Gebrauch von GnuPP ist es sehr praktisch, dass Sie es beim Ver- und Entschlüsseln stets nur mit den „ungeheimen" öffentlichen Schlüsseln zu tun haben. Solange Ihr eigener geheimer Schlüssel und der ihn schützende Passwortsatz sicher sind, brauchen Sie sich um weitere Geheimhaltung keine Sorgen zu machen.

Jedermann darf und soll Ihren öffentlichen Schlüssel haben, und Sie können und sollen öffentliche Schlüssel von Ihren Korrespondenzpartnern haben – je mehr, desto besser.

Denn:

Um sichere E-Mails austauschen zu können, müssen beide Partner jeweils den öffentlichen Schlüssel des anderen besitzen und benutzen.

Wenn Sie also an jemanden verschlüsselte E-Mails schicken wollen, müssen Sie dessen öffentlichen Schlüssel haben und zum Verschlüsseln benutzen.

Wenn – andersherum – jemand Ihnen verschlüsselte E-Mails schicken will, muss er Ihren öffentlichen Schlüssel haben und zum Verschlüsseln benutzen.

Deshalb werden Sie nun Ihren öffentlichen Schlüssel öffentlich zugänglich machen. Je nachdem, wie gross der Kreis Ihrer Korrespondenzpartner ist, gibt es zwei Möglichkeiten:

direkt per E-Mail an bestimmte Korrespondenzpartner

oder auf einem Schlüsselserver – weltweit für jedermann zugänglich

Die erste Möglichkeit, Ihren öffentlichen Schlüssel zu verbreiten, besteht wie gesagt darin, dass Sie ihn per E-Mail an einen oder mehrere Korrespondenzpartner schicken.

Zum Üben dieses Vorgangs kommt nun Adele ins Spiel:

Adele ist ein sehr netter E-Mail-Roboter, mit dem Sie zwanglos korrespondieren können. Weil man gewöhnlich mit einer klugen und netten jungen Dame lieber korrespondiert als mit einem Stück Software (was Adele in Wirklichkeit natürlich ist), haben wir sie uns so vorgestellt:

Adele schicken Sie zunächst Ihren öffentlichen Schlüssel. Wenn Adele Ihren Schlüssel empfangen hat, verschlüsselt sie damit eine E-Mail an Sie und sendet sie zurück.

Diese Antwort von Adele entschlüsseln Sie mit Ihrem eigenen geheimen Schlüssel. Damit Sie wiederum Adele verschlüsselt antworten können, legt Adele ihren eigenen öffentlichen Schlüssel bei.

Adele verhält sich also genau wie ein richtiger Korrespondenzpartner. Allerdings sind Adeles E-Mails leider bei weitem nicht so interessant wie die Ihrer echten Korrespondenzpartner. Andererseits können Sie mit Adele so oft üben, wie Sie wollen – was Ihnen ein menschlicher Adressat wahrscheinlich ziemlich übel nehmen würde.

Wir exportieren also nun Ihren öffentlichen Schlüssel, kopieren ihn in eine E-Mail und senden diese an Adele.

Die hier zuerst gezeigte Möglichkeit funktioniert immer, selbst wenn Sie – z.B. wenn Sie einen E-Mail-Service im Web verwenden – keine Dateien anhängen können. Zudem bekommen Sie so Ihren Schlüssel zum ersten Mal zu Gesicht und wissen, was sich dahinter verbirgt und woraus der Schlüssel eigentlich besteht.

Und so geht's:
Zuerst klicken Sie auf [Export] in der Iconleiste und dann in dem sich öffnenden Dialog auf [Exportieren in Datei]. Wählen Sie mit [Durchsuchen...] einen geeigneten Ordner auf Ihrem PC, z.B. C:\Eigene Dateien\ und speichern Sie den Schlüssel dort z.B. als „mein_key.asc".

Wenn der Schlüssel auf Ihrer Festplatte gespeichert ist, können Sie den Dialog „Schlüssel exportieren" mit [OK] schließen.

Klicken Sie sich dann bis zu dem Ordner durch, in dem Sie Ihren Schlüssel gespeichert haben. Nun öffnen Sie den Schlüssel mit einem Texteditor, z.B. mit Notepad. Sie sehen Ihren öffentlichen Schlüssel im Texteditor so, wie er wirklich aussieht – ein ziemlich wirrer Text- und Zahlenblock:

arkieren Sie den gesamten Schlüssel von

```
-----BEGIN PGP PUBLIC
KEY BLOCK-----
```

bis

```
-----END PGP PUBLIC
KEY BLOCK-----
```

und kopieren Sie ihn mit dem Menübefehl oder mit dem Tastaturkürzel Strg C. Damit haben Sie den Schlüssel in den Speicher Ihres Rechners – bei Windows Zwischenablage genannt – kopiert.

Nun starten Sie Ihr E-Mail-Programm – es spielt keine Rolle, welches Sie benutzen – und fügen Ihren öffentlichen Schlüssel in eine leere E-Mail ein. Der Tastaturbefehl zum Einfügen („Paste") lautet bei Windows **Strg V.**

Diesen Vorgang – Kopieren und Einfügen – kennen Sie sicher als „Copy & Paste"

Adressieren Sie nun diese E-Mail an adele@gnupp.de
und schreiben in die Betreff-Zeile:

mein öffentlicher Schlüssel

So etwa sollte Ihre E-Mail nun aussehen:

To: adele@gnupp.de
From: Fritz Mustermann <f.mustermann@firma.de>
Subject: mein öffentlicher Schlüssel
Cc:
Bcc:
Attached:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.0.6 (MingW32)
Comment: Weitere Infos: siehe http://www.gnupg.org

mQGiBDxDH0wRBACS+IsOvXkh/QzjY65v+IrsNvxEIE4XECHZM4Qv8FoLa7rRO9J+
jVhq4KPseNvoYIzqrv7/M/byGHKIX59ZLRefkxJq59IK2w4jjGJ5Ex0IrKka6J1I
+w0nTByqF6pyobLZ47GwlXy7ZmlmFPR3OGHm+IoAOQH4or9SVvlBwFJ/wwCg05sa
m18TGEIlsORWdrUfWbjS0ZcD/AqRHPSviJzPrrrsw+mYNujVgDz4nKBkyu//uGMR
tpw3Nu143UfF4B5X0XTqfSYDeVacuplboJaHF7iT5ipKXMsINo17yoglVpR4uOx3
gyv42VaJkrjRLSIb991MbitwOU6UvjtqZ7+gLGxbfSI3pZoK/A7395GCz+VNj+C/
hdW2A/9qOvkM1jly/7voxrMeCv3mwz09v2EW/c0akq4WRKCEAe9ncjoij6LXDMrk
zmvpvRpiaqZFHt4/wb9dG8ZPjmi/hM8tKs0S9Y0oOihF32aqnwAC59LePQpfbuHr
iPCSclv0DZ1mNm7Wczk6Xf6Wa3TCwkgppIY9PHcrzA+nQIO4MbQ5RnJpdHogTXVz
dGVybWFubiAoVGVzdHNjaGzDvHNzZWwpIDxmLm11c3RIcm1hbm5AZmlybWEuZGU+
iFcEExECABcFAjxDH0wFCwcKAwQDFQMCAxYCAQIXgAAKCRDxggWdE2OJPThNAKDF
lfAal53Osv38jr+QX/PWUwOIXQCfTgamdbbAxE0zgzGaut3uGtzN6eW5AQ0EPEMf
VhAEAJCFm094JP1oc3mCCzGusGDY8HtpMH12270x7XnubVamLRd3KO+mw220B1Ds
jYmuEZjy1c1DW9eOXu1N/rORIUMRLyVGOyVGXXp1nNQchgbiUesYMKCc16Axi45R
f/40242gmQjWa/DeJ8yD7cyOD3BfKYyi5dMrp/QDnWQl4/xfAAMFA/9PE9YL+uKY
hY6CoRpFNQOwlvb4wkolzThmL01CmeOrvHrSQFdyTJO2tftqjt7Tl6eZaN0e8lpP
xOrsoQR1hwUcevfFLo8sphl7kqD7Nl3n7i7nlC7c/2O3b4qTamoEgZpoypkOjShp
lBRbcjrhqtRxdW5sEYNn+06d5b3M1ZfQXYhGBBgRAgAGBQI8Qx9WAAoJEPGCBZ0T
Y4k9vWYAnjNbspcK4JjUu+dKw8kg2iCDAK5XAJ9Th6rkFRLw4qFfSZ8SMsnaBJKS
+Q==
=BB1w
-----END PGP PUBLIC KEY BLOCK-----
```

Schicken Sie die E-Mail an Adele nun ab. Nur zur Vorsicht: natürlich sollten Ihre E-Mails **nicht** f.mustermann@firma.de als Absender haben, sondern Ihre eigene E-Mail-Adresse. Denn sonst werden sie nie Antwort von Adele bekommen...

Genauso gehen Sie vor, wenn Sie Ihren Schlüssel an eine echte E-Mail-Adresse senden. Natürlich können Sie dann auch noch ein paar erklärende Sätze dazuschreiben. Adele braucht diese Erklärung nicht, denn sie ist zu nichts anderem als zu diesem Zweck programmiert worden.
Fassen wir kurz zusammen:
Sie haben Ihren öffentlichen Schlüssel per E-Mail an einen Korrespondenzpartner geschickt.

☞ **Im Handbuch „GnuPP für Durchblicker" Kapitel 7 beschreiben wir, wie Sie Ihren Schlüssel auch als Dateianhang versenden.**

Das ist oftmals das gebräuchlichere Verfahren. Wir haben Ihnen hier die „Copy&Paste"-Methode zuerst vorgestellt, weil sie transparenter und leichter nachzuvollziehen ist..
Sie können dieses Kapitel jetzt lesen oder später, wenn Sie diese Funktion benötigen.

6. Sie veröffentlichen Ihren Schlüssel per Keyserver

Diese Möglichkeit bietet sich eigentlich immer an, selbst wenn Sie nur mit wenigen Partnern verschlüsselte E-Mails austauschen. Ihr Schlüssel ist dann sozusagen „stets griffbereit" auf einem Server im Internet vorhanden.

Klicken Sie Ihren Schlüssel an, und klicken Sie dann auf die Taste [Export]

Wie Sie sehen, ist ein Key Server bereits voreingestellt. Wenn Sie auf [OK] klicken, wird der Schlüssel auf den Server geschickt und von dort aus an die anderen, weltweit verbundenen Key Server weitergereicht. Jedermann kann ihn von dort herunterladen und dazu benutzen, Ihnen eine sichere E-Mail zu schreiben.

Wenn Sie den Ablauf im Moment nur testen, dann schicken Sie den Übungs-Schlüssel nicht ab.
Er ist wertlos und kann praktisch nicht mehr vom Schlüsselserver entfernt werden. Sie glauben nicht, wieviele Testkeys mit Namen wie „Julius Caesar", „Helmut Kohl" oder "Bill Clinton" dort herumliegen – schon seit Jahren....

Fassen wir kurz zusammen:
Sie wissen nun, wie Sie Ihren Schlüssel auf einen Schlüsselserver im Internet schicken können.

☞ **Wie Sie den Schlüssel eines Partners auf den Schlüsselservern suchen und finden, beschreiben wir im Handbuch „GnuPP für Durchblicker" Kapitel 6. Sie können dieses Kapitel jetzt lesen oder später, wenn Sie diese Funktion benötigen.**

7. Sie entschlüsseln eine E-Mail

Adele erhält nun Ihren öffentlichen Schlüssel, verschüsselt damit eine E-Mail und sendet sie an Sie zurück. Nach kurzer Zeit erhalten Sie Adeles Antwort.

So sieht sie aus:

To:
f.mustermann@firma.de
From:
adele<adele@gnupp.de>
Subject: Verschluesselte Antwort

```
----BEGIN PGP MESSAGE-----
Version: GnuPG v1.0.1 (GNU/Linux)
Comment: For info see http://www.gnupg.org


hQEOAwuiAEB5WiClEAP/Whx+O/DbrJ97DEa+s9q4sOwWZ9tGq7fV1UwL2/qE8pe6
5Mr/77y6C7Uc2kQUSI06+NpV4J4Y9HINkWskn7M3UBhFHY6sRPF9Ks4wseHM0klI
qj0uLw/+2ylbCchTMoAAPgPVvtGp2aEfiRJItVJjLk96eb6qqATlHmcAgwQ26XoD
...
ssp3BSvr7UZdFHKhIKGjDf9dJuP9VFbmyhLvBeUfpo+O1+dd8CO0JOGZAoBGiY7a
TvFz2NTqLhtWoH897Wu31tzYt41P08PsIqq94Bp6yQO6zoI22vJ0Q8jwVfFqHkaR
9Djp34LyqkyAVHcw25KtCtGEYadBdqI0aHJ0ddQanxOfu7UG0Es6/ugtwmfQX/aZ
c03tyh6DNhWPs9UTZBQwNdk=
=C3TI
-----END PGP MESSAGE-----
```

(Aus Gründen der Übersichtlichkeit haben wir den Verschlüsselungsblock stark gekürzt)

.

Diese E-Mail werden Sie nun mit dem Programm WinPT entschlüsseln.

WinPT ist ein sogenanntes "Frontend" für GnuPG. Es dient zur eigentlichen Ver- und Entschlüsselung der E-Mails und zur Erzeugung und Überprüfung von digitalen Unterschriften. Und zwar – und das ist einer seiner Vorteile – mit jedem beliebigen E-Mail-Programm.

Für bestimmte E-Mail-Programme – z.B. MS Outlook für Windows, gibt es außerdem spezielle GnuPP-PlugIns, mit denen die Ver- und Entschlüsselung direkt im jeweiligen E-Mailer erledigt werden kann.

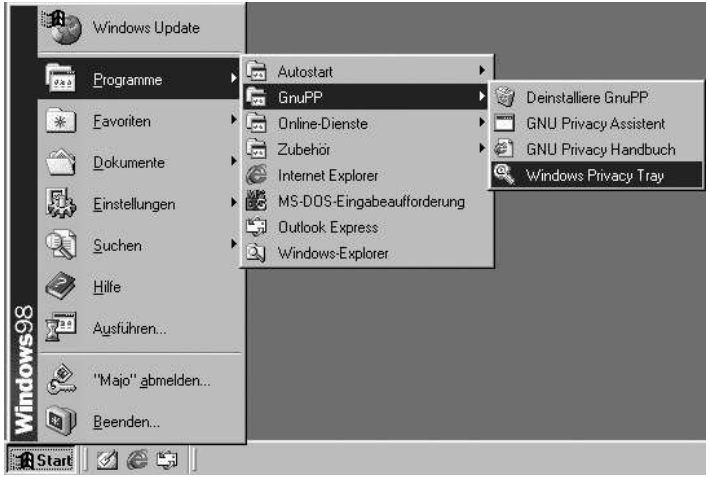
☞ **Hinweise zu diesen Lösungen finden Sie im Handbuch „GnuPP für Durchblicker" Kapitel 8. Sie können dieses Kapitel jetzt lesen oder später, wenn Sie diese Funktion benötigen.**

WinPT hat dagegen den Vorteil, dass es nicht mit einem bestimmten, sondern mit jedem E-Mail-Programm funktioniert. Es erledigt nämlich die Ver- und Entschlüsselung einfach im Speicher des Rechners. Das bedeutet, dass man den Text, der ver- oder entschlüsselt werden soll, zunächst in die Zwischenablage des Rechners kopieren muss.

Markieren Sie den gesamten Text aus Adeles E-Mail und kopieren Sie ihn mit dem entsprechenden Menübefehl oder Tastaturkürzel (z.B. Strg C bei Windows).

Damit haben Sie den Schlüssel in den Speicher Ihres Rechners – bei Windows Zwischenablage oder Clipboard genannt – kopiert.

Starten Sie nun WinPT aus dem Windows-Startmenü:

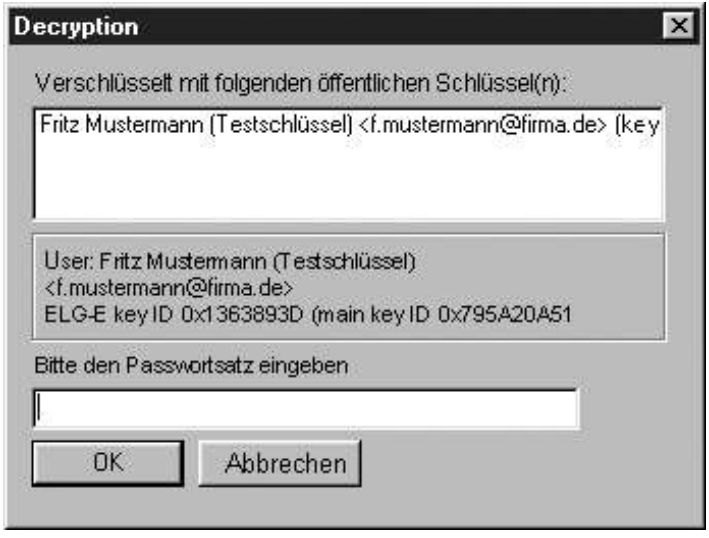


Während WinPT startet, erscheint kurz ein Hinweis darauf, dass das Programm die bereits vorhandenen Schlüssel einlädt.

Nachdem das Programm gestartet wurde, sehen Sie unten rechts in der Windows-Taskleiste dieses Schlüssel-Icon:

Klicken Sie mit der rechten Maustaste auf dieses Icon. Daraufhin öffnet sich das WinPT-Menü. Hier klicken Sie auf [Zwischenablage] und dann auf [Entschlüsseln/Überprüfen].

Es erscheint dieser Dialog: Geben Sie nun Ihren geheimen Passwortsatz ein. GnuPG entschlüsselt nun Adeles E-Mail.



Kurz darauf erscheint dieser Hinweis:

Der entschlüsselte Text befindet sich jetzt wieder im Windows-Clipboard, genau wie beim Verschlüsseln. Kopieren Sie ihn mit Einfügen [Strg + V] in den Texteditor oder auch in Ihr E-Mail-Programm.

Die entschlüsselte Antwort von Adele sieht so aus:

```
Hallo Herr Mustermann,

hier ist die verschluesselte Antwort auf
Ihre mail.

Anbei der public key von adele@gnupp.de,
dem freundlichen E-Mail-Roboter, als Anlage.

Viele Gruesse,
adele@gnupp.de
```

Der Textblock, der darauf folgt, ist der öffentliche Schlüssel von Adele.

Wir werden anschliessend diesen öffentlichen Schlüssel importieren und an Ihrem Schlüsselbund befestigen. So können Sie ihn jederzeit zum Entschlüsseln der Nachrichten Ihres Korrespondenz-partners benutzen.

Fassen wir kurz zusammen:

1. Sie haben eine verschlüsselte E-Mail mit Ihrem geheimen Schlüssel entschlüsselt.
2. Der Korrespondenzpartner hat seinen eigenen öffentlichen Schlüssel beigelegt, damit Sie ihm antworten können.

8. Sie befestigen einen Schlüssel am Schlüsselbund

Ihr Korrespondenzpartner muß nicht etwa jedes Mal seinen Schlüssel mitschicken, wenn er Ihnen verschlüsselt schreibt. Sie bewahren seinen öffentlichen Schlüssel einfach an Ihrem GnuPG-„Schlüsselbund" auf.

1. Möglichkeit:
Um einen öffentlichen Schlüssel zu importieren (an Ihrem Schlüsselbund zu befestigen), speichern Sie ihn am einfachsten als Textblock ab, so wie Sie es vorhin schon bei Ihrem eigenen Schlüssel getan haben.

Also:

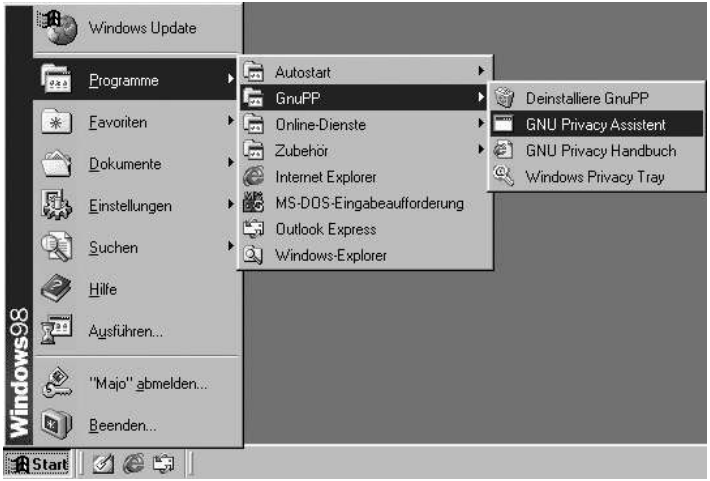
markieren Sie den öffentlichen Schlüssel, den Sie von Ihrem Korrespondenzpartner erhalten haben, von

```
-----BEGIN PGP PUBLIC
KEY BLOCK-----
```
bis
```
-----END PGP PUBLIC
KEY BLOCK-----
```

und setzen ihn mit Copy & Paste in einen Texteditor ein. Speichern Sie den Schlüssel unter einem Namen in einem Ordner, den Sie leicht wiederfinden, z.B. als „adeles_key" im Verzeichnis C:\Eigene Dateien.

2. Möglichkeit:
Der Schlüssel liegt der E-Mail als Dateianhang bei. Welches E-Mail-Programm Sie auch immer benutzen, Sie können stets Dateianhänge („Attachments") auf Ihrer Festplatte abspeichern. Tun Sie das jetzt (am besten wieder in einem Ordner, den Sie leicht wiederfinden,unter z.B. C:\Eigene Dateien).

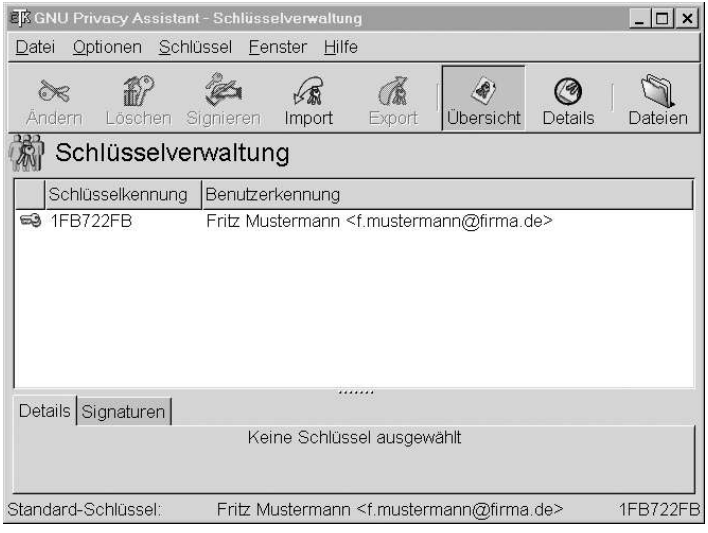
Ob Sie nun den Schlüssel als Text oder als E-Mail-Anhang abgespeichert haben, ist egal: in beiden Fällen importieren Sie diesen abgespeicherten Schlüssel in den GnuPG-„Schlüsselbund".



Und zwar so:

Starten Sie den GNU Privacy Assistant im Windows-Menü, falls Sie ihn in der letzten Übung ausgeschaltet haben.

Wenn der GNU Privacy Assistant läuft, klicken Sie auf die Schaltfläche Import, suchen den eben abgespeicherten Schlüssel und laden ihn. Der importierte Schlüssel wird nun im GNU Privacy Assistant angezeigt:



Damit haben Sie einen fremden öffentlichen Schlüssel – in diesem Beispiel den von Adele – importiert und an Ihrem Schlüsselbund befestigt. Sie können diesen Schlüssel jederzeit benutzen, um verschlüsselte Nachrichten an den Besitzer dieses Schlüssels zu senden.

Bevor wir weitermachen, eine wichtige Frage:
woher wissen Sie eigentlich, dass der fremde öffentliche Schlüssel wirklich von Adele stammt? Man kann E-Mails auch unter falschem Namen versenden – die Absenderangabe besagt eigentlich gar nichts.

Wie können Sie also sichergehen, dass ein Schlüssel auch wirklich seinem Absender gehört ?

☞ **Diese Kernfrage besprechen wir im Handbuch „GnuPP für Durchblicker" Kapitel 9: „Die Schlüsselprüfung". Lesen Sie jetzt dort weiter, bevor Sie danach an dieser Stelle fortfahren.**

Sie haben in Kapitel 9 des Handbuchs „GnuPP für Durchblicker" gelesen, wie man sich von der Echtheit eines Schlüsselss überzeugt und ihn dann mit seinem eigenen geheimen Schlüssel signiert.

In Kapitel 10 des Handbuchs „GnuPP für Durchblicker" besprechen wir, wie man nicht nur einen Schlüssel, sondern auch eine komplette E-Mail-Nachricht signieren kann. Das bedeutet, daß man die E-Mail mit einer Art elektronischem Siegel versieht.

Der Text ist dann zwar noch für jeden lesbar, aber der Empfänger kann sicher sein, daß die E-Mail unterwegs nicht manipuliert oder verändert wurde.

Die Überprüfung einer solchen Signatur ist sehr einfach. Sie müssen dazu natürlich den öffentlichen Schlüssel des Absenders bereits an Ihrem GnuPP-Schlüsselbund befestigt haben, wie in Kapitel 8 besprochen.

Wenn Sie eine signierte E-Mail erhalten, sehen Sie, daß der Text am Anfang und Ende von einer Signatur eingerahmt ist.

Sie beginnt mit

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

und endet unter der E-Mail-Nachricht mit

```
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.0.6 (MingW32) - WinPT 0.4.0
Comment: Weitere Infos: siehe
http://www.gnupg.org
iEYEARECAAYFAjxeqy0ACgkQcwePex+3Ivs79wCfW8u
ytRsEXgzCrfPnjGrDDtb7
QZIAn17B8l8gFQ3WIUUDCMfA5cQajHcm
=O6lY
-----END PGP SIGNATURE-----
```

Markieren Sie den gesamten Text von `BEGIN PGP SIGNED MESSAGE` bis `END PGP SIGNATURE` und kopieren Sie ihn mit Crtl+C in die Zwischenablage.

Nun fahren Sie genauso fort wie bei der Entschlüsselung einer E-Mail, wie wir es in Kapitel 7 dieses Handbuchs besprochen haben:

Sie öffnen WinPT aus der Windows-Taskleiste und wählen Decrypt/Verify.

Es sollte dann die Meldung

```
Signature good -
Signed by .....
```

angezeigt werden.
Falls Sie aber die Meldung

`Bad signature`
oder `Überprüfung fehlgeschlagen`
erhalten, wurde die Nachricht bei der Übertragung verändert. Aufgrund der technischen Gegebenheiten im Internet ist es nicht auszuschließen, daß die E-Mail durch eine fehlerhafte Übertragung verändert wurde. Das ist zunächst der wahrscheinlichste Fall. Es kann jedoch auch bedeuten, dass der Text nachträglich verändert wurde.

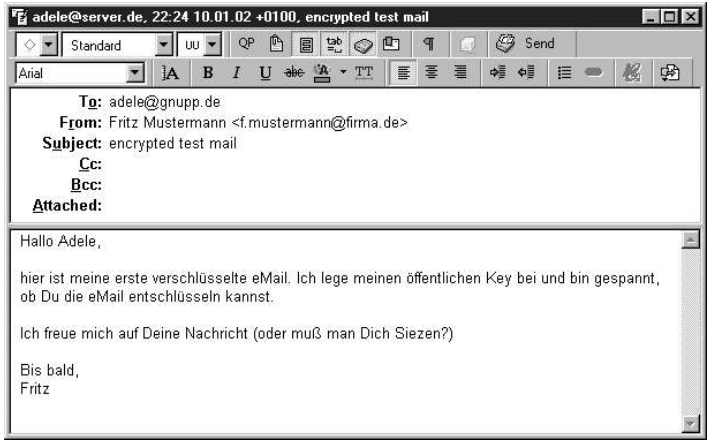
☞ **Wie Sie in einem solchen Fall vorgehen sollten, erfahren Sie im Handbuch GnuPP für Durchblicker" Kapitel 10. „E-Mails signieren". Lesen Sie jetzt dort weiter, bevor Sie danach an dieser Stelle fortfahren.**

9. Sie verschlüsseln eine E-Mail

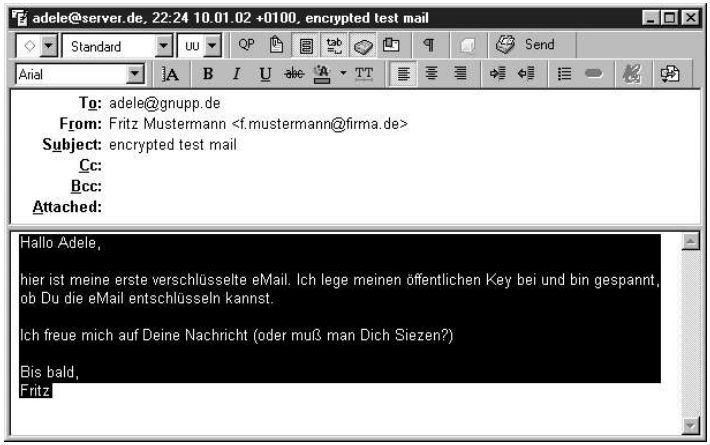
Jetzt wird es nochmal spannend:

Sie verschlüsseln eine E-Mail und senden sie an Adele. Wenn Sie einen ebenso geduldigen menschlichen Korrespondenzpartner haben, dann senden Sie Ihre E-Mail eben an diesen.

Starten Sie nun Ihr E-Mail-Programm. Schreiben Sie eine Nachricht – es ist egal, was: Adele kann nicht wirklich lesen....

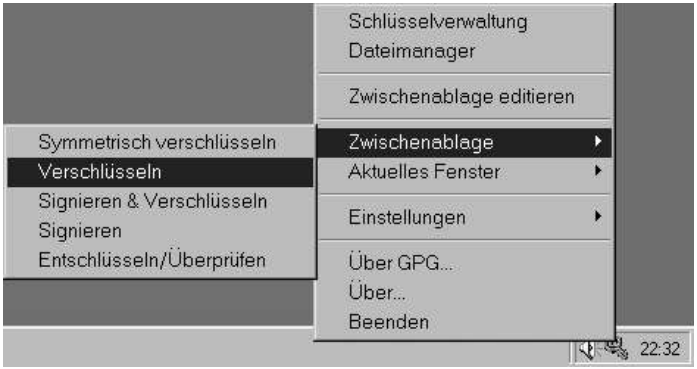


Nun markieren Sie den gesamten Text und kopieren Sie ihn mit dem entsprechenden Menübefehl oder Tastaturkürzel Ihres Betriebssystems (z.B. Strg+C bei Windows). Damit haben Sie den Text in den Speicher Ihres Rechners – bei Windows Zwischenablage oder Clipboard genannt – kopiert.



Klicken Sie nun mit der rechten Maustaste auf auf das WinPT-Icon unten rechts in der Windows-Task.

In der WinPT-Befehlsleiste klicken Sie auf [Zwischenablage] und dann auf [Verschlüsseln].



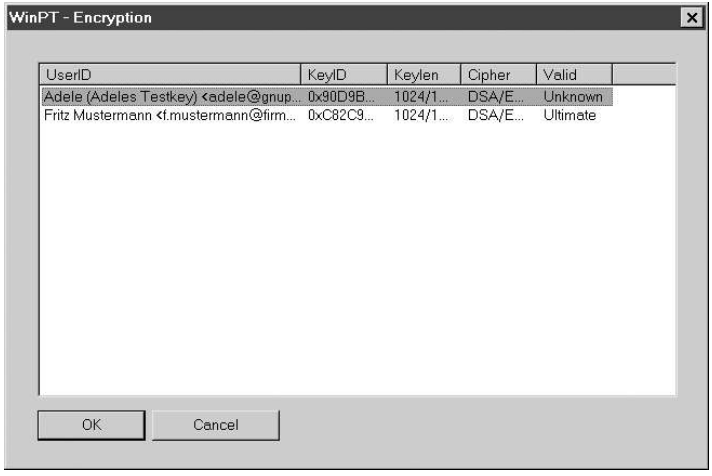
Daraufhin öffnet sich ein Fenster mit den Schlüsseln, die Sie an Ihrem Schlüsselbund haben. In unserem Beispiel sind das Adeles Schlüssel, den sie Ihnen vorhin geschickt hat, und Ihr eigener Schlüssel, den Sie in Kapitel 2 erzeugt haben.

Klicken Sie auf Adeles Schlüssel, denn damit muss die Nachricht ja verschlüsselt werden,

Sie erinnern sich an den Grundsatz:

Wenn Sie an jemanden verschlüsselte E-Mails schicken wollen, müssen Sie dessen öffentlichen Schlüssel haben und zum Verschlüsseln benutzen.

Klicken Sie den öffentlichen Schlüssel Ihres Korrespondenzpartners an und anschließend auf [OK].

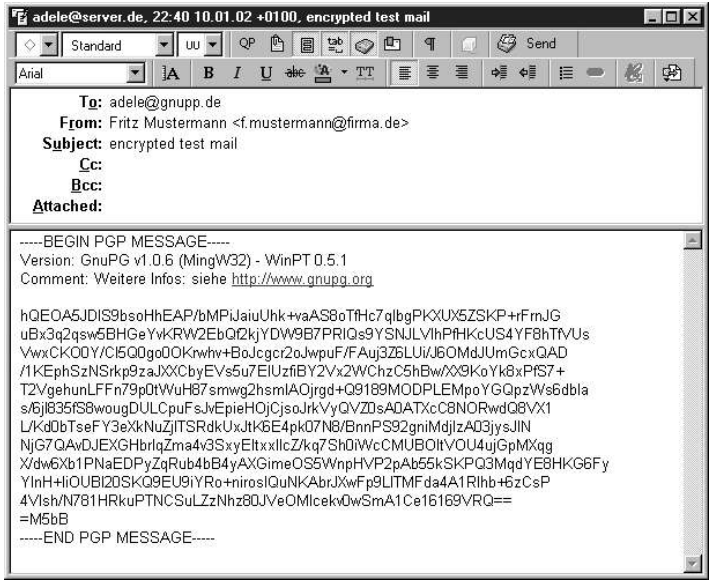


Jetzt wird Ihre Nachricht verschlüsselt. Nach kurzer Zeit erscheint diese Meldung:

Klicken Sie auf OK.

Die verschlüsselte Nachricht befindet sich noch in der Zwischenablage (Clipboard) und kann nun mühelos in das E-Mail-Fenster hineinkopiert werden. Löschen Sie den unverschlüsselten Text oder kopieren die den Inhalt der Zwischenablage einfach darüber.

So ähnlich sollte das Ergebnis aussehen:



Senden Sie nun Ihre E-Mail wieder an Adele.
Nur zur Vorsicht: natürlich sollten Ihre E-Mails **nicht** f.mustermann@firma.de als Absender haben, sondern Ihre eigene E-Mail-Adresse. Denn sonst werden sie nie Antwort von Adele bekommen...

Herzlichen Glückwunsch!
Sie haben Ihre erste E-Mail verschlüsselt!

Wie Sie Ihre E-Mails verschlüsselt archivieren

Eine Einstellung müssen Sie noch vornehmen, damit Sie Ihre E-Mails verschlüsselt aufbewahren können. Natürlich können Sie einfach eine Klartext-Version Ihrer Texte aufbewahren, aber das wäre eigentlich nicht angebracht. Wenn Ihre Mitteilung geheimhaltungsbedürftig war, sollte sie auch nicht im Klartext auf Ihrem Rechner gespeichert sein. Also sollte immer ein Kopie der verschlüsselten E-Mail aufbewahrt werden.

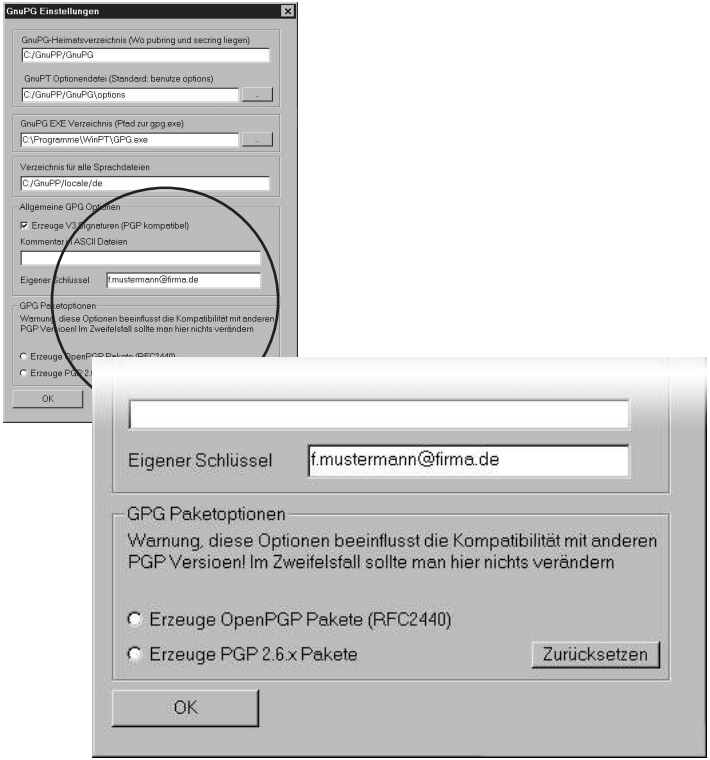
Sie ahnen das Problem: zum Entschlüsseln der archivierten E-Mails braucht man den geheimen Schlüssel des Empfängers – und den haben Sie nicht und werden Sie nie haben....

Also was tun?

Ganz einfach – GnuPP legt einfach eine Archiv-Kopie Ihres Textes ab, die mit Ihrem eigenen öffentlichen Schlüssel verschlüsselt ist! So können Sie den Text auch später noch einfach mit Ihrem eigenen Geheimschlüssel wieder lesbar machen.

Da GnuPP nicht wissen kann, welchen Schlüssel Sie benutzen – Sie können ja auch mehrere haben – müssen Sie dem Programm dies mitteilen.

Um diese Option zu nutzen, genügt ein Mausklick: öffnen Sie WinPT, dann das Untermenü „Einstellungen" und dort „GPG"



In dem Einstellungsfenster, das sich nun öffnet, tragen Sie unter „Eigener Schlüssel" Ihren Schlüssel ein, und zwar einfach mit der dazugehörigen E-Mail-Adresse.

Fassen wir kurz zusammen:

1. Sie haben mit dem öffentlichen Schlüssel Ihres Partners eine E-Mail verschlüsselt und ihm damit geantwortet.
2. Sie haben GnuPP mitgeteilt, daß es Archiv-Kopien Ihrer E-Mails ablegen soll, die mit Ihrem eigenen Schlüssel verschlüsselt sind.

Das war's! Willkommen in der Welt der freien und sicheren E-Mail-Verschlüsselung!

☞ **Lesen Sie nun die Kapitel 10 bis 12 im Handbuch „GnuPP für Durchblicker". Sie erfahren dort unter anderem, wie man E-Mails signiert und einen bereits vorhandenen Geheimschlüssel (z.B. aus PGP) in GnuPG importiert und verwendet.**

☞ **Im Kapitel 13 des Handbuchs „Gnupp für Durchblicker"** können Sie weiterhin in zwei spannenden Kapiteln lesen, warum GnuPG nicht zu knacken ist - jedenfalls nicht in den nächsten paar Milliarden Jahren.

Und Sie können lesen, wie die geheimnisvolle Mathematik hinter GnuPP wirklich funktoniert.

Genau wie das OpenSource-Kryptografieprogramm GnuPP wurden diese Texte nicht geschrieben für Mathematiker, Geheimdienstler und Kryptografen, sondern

☞ **für jedermann.**

Herausgegeben und gefördert vom
Bundesministerium für Wirtschaft und Technologie

www.gnupp.de

Projektleitung:
G-N-U GmbH
EDV-Dienstleistungen
E-Mail: info@g-n-u.de
WWW: http://www.g-n-u.de

Redaktion:
TextLAb
text + medien
http://www.textlab.de