

GPG-Einführung

Martin Schütte



13. April 2008

Einleitung
00

Verfahren
0000

Programme
000

Schlüsselverwaltung
000000

Passwörter
000

Ende
0000

Einleitung

Verfahren

Programme

Schlüsselverwaltung

Passwörter

Ende

Warum Kryptographie?

- **Vertraulichkeit**
Mail nur für Empfänger lesbar.
- **Integrität**
Keine Veränderung der Daten.
- **Authentizität**
Richtiger Absender bekannt.

Normale E-Mails garantieren keines der Ziele.

Welche Kryptographie?

There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files.

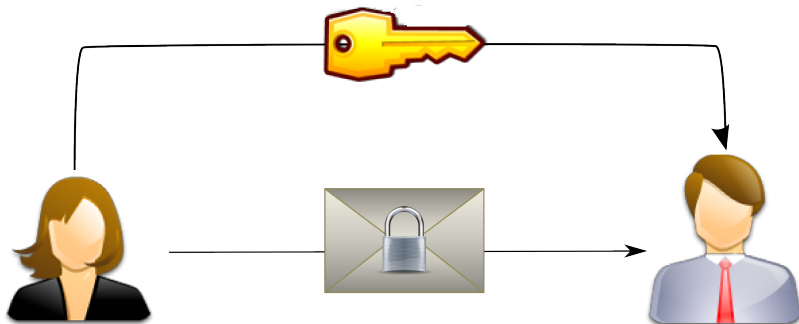
– Bruce Schneier, Applied Cryptography

GPG schützt vor Regierungen ...

... wenn ein paar Regeln beachtet werden.

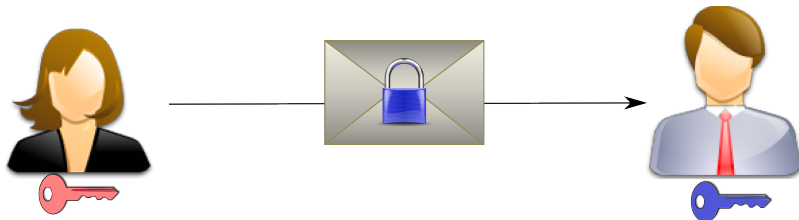
Symmetrische Verschlüsselung

- Ein Schlüssel zum ver- und entschlüsseln
- sichere Schlüssel: 128 bit lang
- + schnell
- Schlüsselverteilung



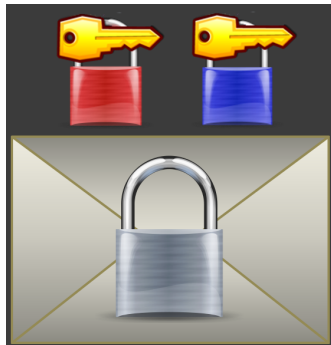
Asymmetrische/public key Verschlüsselung

- Jeder hat öffentlichen und privaten Schlüssel (zum ver- und entschlüsseln)
 - sichere Schlüssel: 2048 bit lang
- + öffentliche Schlüssel
- langsam



Hybride Verschlüsselung

- Erfolgsrezept für PGP
- Vorgehen:
 1. Schlüssel erzeugen
 2. symmetrisch verschlüsseln
 3. Schlüssel für alle Empfänger asymmetrisch verschlüsseln
 4. verschlüsselten Schlüssel und Nachricht verschicken
- vereint Vorteile

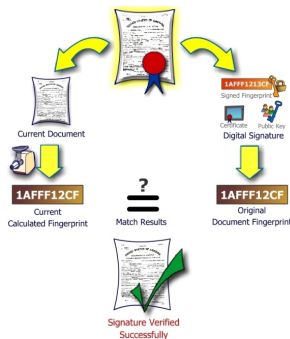


Signatur

Authentizität und Integrität sichern

1. Hash/Prüfsumme berechnen
2. mit eigenem privaten Schlüssel „verschlüsseln“
3. Hash an Nachricht anhängen (= Signatur)
4. mit öffentlichem Schlüssel überprüfen und vergleichen

Nicht nur für E-Mails, sondern auch für Software verbreitet.



PGP

Pretty Good Privacy

- 1991 von Philip Zimmermann geschrieben
- über BBSs, Usenet und Bücher verbreitet
- patentrechtliche, politische und wirtschaftliche Probleme
- viele Firmen: Viacrypt, PGP Inc., Network Associates/McAfee, PGP Corporation
- viele (parallele) Versionen: PGP/PGPi, 2.6.3, 4, 5.x, 6.x ff.



OpenPGP/GnuPG

- Standardisierung
 - 1996 RFC 1991 „PGP Message Exchange Formats“
 - 1998 RFC 2440 „OpenPGP Message Format“
 - 2007 RFC 4880 „OpenPGP Message Format“
- offener Standard, nur freie Algorithmen
- verschiedene Programme möglich

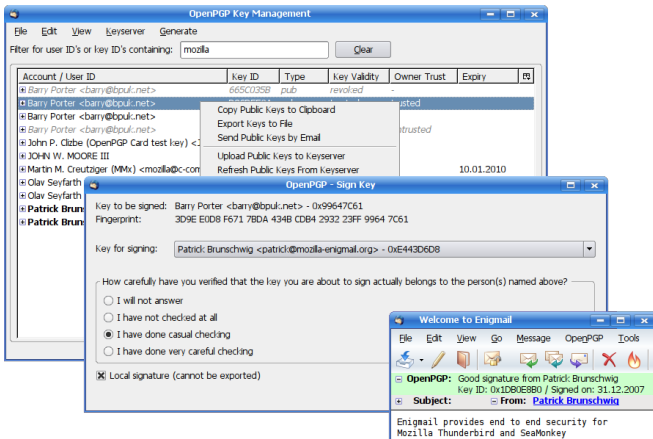
OpenPGP/GnuPG

- Standardisierung
 - 1996 RFC 1991 „PGP Message Exchange Formats“
 - 1998 RFC 2440 „OpenPGP Message Format“
 - 2007 RFC 4880 „OpenPGP Message Format“
- offener Standard, nur freie Algorithmen
- verschiedene Programme möglich
- GPG: „GNU Privacy Guard“



Enigmail

- graphische Oberfläche für GPG
- Add-On für Mozilla Thunderbird und Seamonkey



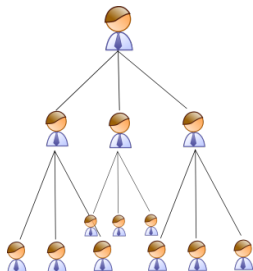
Wie Identität sicherstellen?

- Jeder kann eigenen GPG-Schlüssel mit Inhaber „Martin Schütte“ erstellen und verbreiten
 - Verfahren zur Zuordnung Schlüssel ↔ Person nötig
- ⇒ Schlüssel signieren/beglaubigen lassen

X.509/Public Key Infrastruktur

- Vertrauen in zentrale Stellen
 - Zertifizierungsstellen signieren Schlüssel
- ⇒ Hierarchie von Zertifizierungsstellen

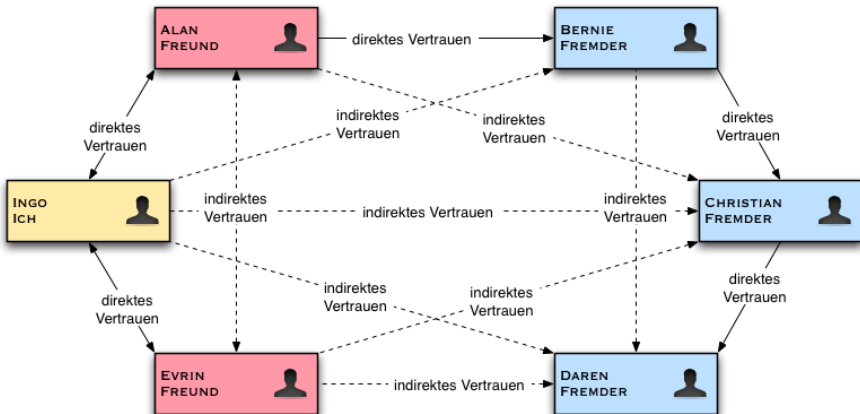
Benutzt für X.509-Zertifikate
(SSL, TLS und S/MIME-Mailverschlüsselung).



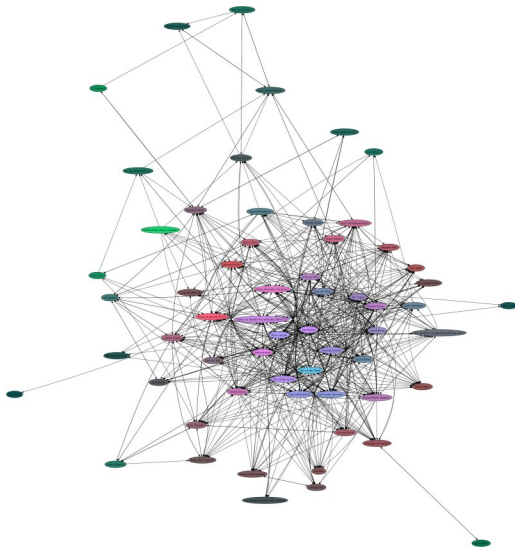
Web of Trust

- Vertrauen in andere Nutzer
 - dezentral aus vielen 1:1-Signaturen
- ⇒ Vertrauens-„Pfade“ durchs Netz

Web of Trust



Web of Trust



Keysigning-Party

- Kultiges Zusammensitzen und gemeinsames Murmeln magischer Zahlen. (laut Fachbegriffe der Informatik)
 - persönliches Treffen, ohne Computer (!)
 - Vergleich von PGP-Schlüssel-Identität mit (amtlichem) Ausweis
 - Gegenseitiges Signieren der Schlüssel
- ⇒ Web of Trust wächst



© Noirin Plunkett

Keyserver

- Ziel: öffentliche Schlüssel verfügbar machen
- einfach Signaturen anhängen
- wie großes „Telephonbuch“ für 2,5 Mio. PGP-Schlüssel
- alle können Schlüssel/Signaturen lesen und hinzufügen
(aber Löschen praktisch nicht möglich)

Schlüssel-Widerruf/Revocation

- falls Schlüssel gestohlen/gebrochen/verloren
 - muss mit dem Schlüssel selbst signiert werden
- ⇒ Sofort nach Schlüsselerzeugung anlegen
und für den Notfall verwahren

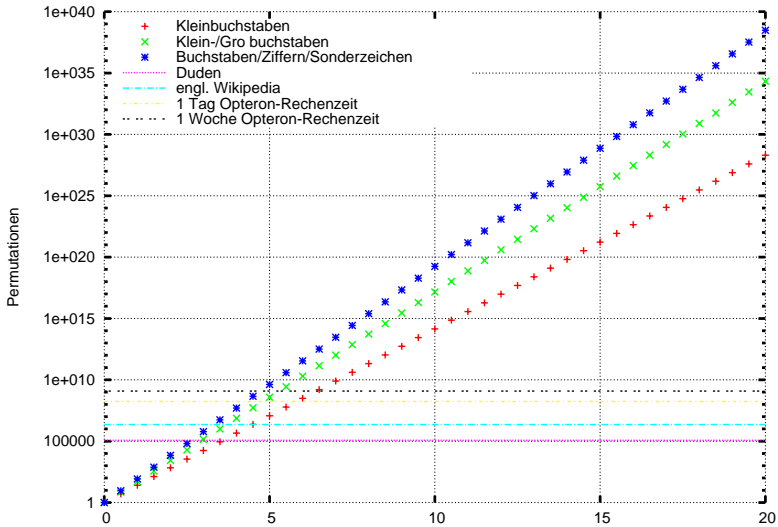
Mantra/Passphrase/Passwort

- Verschlüsselung sicher
 - Schwächstes Glied der Kette: privater Schlüssel
- ⇒ Schutz mit Passphrase
- ⇒ gute Passphrase/Passwörter nötig

Mantra/Passphrase/Passwort

- Ziel: hohe Entropie (\approx Zufälligkeit)
also viele Möglichkeiten, großer Suchraum
- Ideal: 128 bit Entropie, d. h. $2^{128} \approx 10^{38}$ Möglichkeiten
(also so stark wie die Verschlüsselungselbst; nicht realistisch)
- Normaler Text hat nur 1,x Bits Entropie pro Buchstabe
- deshalb Ziffern und Sonderzeichen benutzen
- Tabu: einfache Wörter, Zitate, Verse

Mantra/Passphrase/Passwort



Fazit

- technische Probleme gelöst
- GPG funktioniert
- Enigmail setzt GUI drauf
- noch einfacher wird es nicht

- bleibt: soziales Problem
- Möglichkeit muss auch genutzt werden

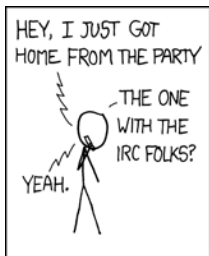
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGiBEfG/6ERBADpOMTBq50Fqceur3pEF5TWvBilCL5Ygxuf/o8z8Wrmu30upJKqZhEVsLPeGRNICURfOLW
l/jPBr54WNL7x05fzzVQUwzkzcrvniY5ieghnXaEdv8wdiQKn4am2HaNr46uSdQqNuOP3fk3705SM0ggMni
eWpDGHQ1PYpBSORA+mpwCg7nUpWTjmqvq0ZA0iA0bIiJX7WeKd/1mkJG9jledW1RnGSnlj3fC6yMYh1kukQ
sk+7qA/jn+MpaJF8+v8exCW4N7Adg0IHGHQFAG4BrhFLKtItpjSfE00L2FLfwCvMYODYawlTw0+hHrJwsY2E
IbyPk+7im6Yte3jXJFTaJk5cTVqIgn/rg8t2QBFRaWUz+Pd24U+4xATWA/9zbF0oLQU0uhHs07xRpHPH6j
41pqrLMCeDkp/0b0zvgZ9JVE/FhmXMaQEDkK7ShMGrJTVMBLpvpAgg6SJ+F6zjWnEzHiOm3DxhL5aTZYYJw
mI6bksf4lrVX/zNfolNgshvGQSoFq1LuhPjYnBfnTFU2Xer4TFH+ZnLdySidkXArQnTWfYdGluIFNjaM08d
HRlIDxtYXJ0aw5AbXNjaHvldHRlLm5hbWU+iGYEEExECACYFAkfHABACGyMFCQlMAYAGCwkIBwMCBBUCCAME
FgIDAQIEAQIXgAAKRCctvboushHY2U2GAJ9pvx0MJX+4BLTrmnlUcqr4iOYBACGoiiz3lsjqseD41GNfo0
gU/b2uYeOLE1hcnRpbIBTY2jDvHROZSA8bXNjaHvldHRAcnoudW5pLXBvdHNkYW0uZGU+iGYEEExECACYFAk
fG//sCGyMFCQlMAYAGCwkIBwMCBBUCCAMEFgIDAQIEAQIXgAAKRCctvboushHY2YevAJ4hSpfPL8gNCp5eD
W3Ft01ic3fqwAcfcgAyK3b9Vc7tZnYSMD8qjke86dS0JU1hcnRpbIBTY2jDvHROZSA8aW5mb0Btc2NodWV0
dGUubmFtZT6IaQQTEQIAKQIbIwUJCWYBgAYLCQgHawIEFQIIAwQWAgMBAh4BAheABQJHxwAzAhkBAa0JEK2
9ui6yEdjZsnYAniqtbwxq/Xjyp8LRp3jHPTAGZLcXAJ9jaK8RrYiNeZGUW5gCjddLZssaGrkCDQRHxv+hEA
gA6qCEeICPgXERvAcW32+CFENEID0yhw5AowuSnVguOmLmG1LVjdfifyju/prLehejtzwr9MTeOKL2if8t
mz05EmLp4wTeUtTlVTsigpF3gII/SP9/OpktORwuBsOSX50EcparkW3h6LV2oOTSDK67Q2zXHOq+vMVnz0L
pr79/z5KRr6ZpnwSpylve5t12pAj0sc99IGiUYECLdiAMf8PNT0909AZCiiVqlp4ZSIIlNGkHcQtSv8yFjd
IM0Ah7+qo35fuieBq3JcbK8xS0ok0K0nOC4wKz1g0T5RPwsmiPMIEdb29YEK51yEPCVL7IbZgBBXyXzkvKm
2jQxJYY9ABdwADBQf+IphzjV9uTAyD3jgJyQPxU8le23ml9/H8cSfzYcMdnz1UAblRp3HavSzVfXktTczB9
1Iqw2MRZHiY/2Y48+gU780N4FHMHKwP4PcLl/uZaqT8Mg3SMzdfQBCWJG8dLBrOurrKHtrGaCyqzWD9S3yi
VU3qEYE9l715thm5EgpbIWcVYTWABWuBkkZAg5qBn1Vm4ffMYJscYmT/I5oY/BPjExh/JmfFEnWjEyXGFG1
1M0dvhNmQakXRb8oKF2uRt/pd4jQLS1d7qwjeY35vMvKK+t5QsmLt0IUDQexW60HudK+703TQaC+KVkuL1C
+KXwjH5xDtcbNhmKWjBtVOCR+2X4hPBBGrAgAPBQJHxv+hAhsMBQkJZgGAAA0JEK29ui6yEdjZ+LsAnRStD
3g0eGgbLlp8maJn8cD/199AAJ9/uE4qYppsK4VMeGdelFNGe8p79w===OIL0

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

Links/Quellen

- GnuPG
 - Enigmail
 - Keyserver pgpkeys.pca.dfn.de
 - Keysigning Party HOWTO
 - Phil Zimmermann
 - How PGP works
 - Stephen Levy, *Crypto*, 2001
-
- Bilder jeweils mit Link zur Quelle
 - Cliparts von Wikimedia Commons
 - Rest: © Martin Schütte



👤🔇 xkcd