PGP und GnuPG

„Eine E-Mail ist wie eine Postkarte, die jeder mitlesen kann. Stecken Sie Ihre Briefe nicht in einen Umschlag?“

Andre Meister andre.meister@student.hu-berlin.de 0x05CE2461

Gliederung

- Umfrage
- Definition, Einsatz
- Funktionsweise
- Beispiele
- Geschichte
  - PGP, Krypto-Debatte
  - OpenPGP, GnuPG
- Fazit, (Anmerkungen ?)

Definition, Einsatz

- Pretty Good Privacy, GNU Privacy Guard
- OpenPGP Standard (RFC 2440)
- verschlüsseln, entschlüsseln, signieren
- E-Mails, Dateien, HDD, Instant Messaging
- Schneier: „Assuming you trust IDEA, PGP is the closest you're likely to get to military-grade encryption.“

Funktionsweise

- Asymmetrisches Verschlüsselungsverfahren
  - privater + öffentlicher Schlüssel (RSA/DSA)
- Ver-/Entschlüsseln
  - asymmetrisch verschlüsselter Session-Key
  - symmetrisch verschlüsselte Nachricht
- Signaturen: Hash -> RSA/DSA
- Fingerprint, Web-of-Trust
- Anwendung spielend einfach

Beispiel E-Mail

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.6 (GNU/Linux)

hQEMAzaHe2yX25NHAQf/YwKuXANld7XfcxVJolRm5uT7YpKWte5TE0unP7JofiUV
R5oy6i/vfNbVtWNKL16WLfGbXwezrJz5PbFYK0n8xJE4mZlfTPLl6YT5Y8E+RmAb
ZiNSLjaye/PbVfhQGfzZL1NvV0vyE6v5nlF6zbn7aM6ukE+uWPvcF0WTPm8cASye
6IRa5aYEwBJqidrtZ1HWpznDjjXD2YDlY8lthY3jqaQjUpXZVkGEo3Zgsi9hksg8
SyD9N2JEw3IkRaU1txgT82uxtrO3R13qWnEAgtuzDUW9YTOXXNZbUd0Kra4dmiNQ
Skthne+il2TwEXyqOhDLoVsnhH7SAgolg5A5I9YXjcnqjXMNUiymOx/sJBK0iBxl
Hw9QiqMXXpjlVUW7N09oTt6JQ3Y32WwOU+fguIAf9X4dttd3lnma1J5hUXw+uQ46
mGBJPtLUmzjhqKbC3c5J6N0u6MVEcApGBz1WAe39GfmQHbXz4Jntbat5mlmZ0brs
QHthACAJcyHSFFKHjUjAiSXTVyPIg4+KqUlOikqTTUw2+EOcniKk1r1deFCgQkoF
tY7U67k05BDuJMua7A3lzQbWZyLr3fNlnGZ6l+eAtxAj0DptKQXpUxgGqjxi/g5O
EVkeqiNpHDTQ0HbEPgs1EAC0BJpKacdyY8ja/zJgEVlcdp0aQz74ZqksZ2A/PcVB
+s0CEJyFF4nrnys3knZp64mKVbnpi6Ec9rYbnrPM2Zqn5ocXrd9x7fBnjkBS5kEq
rZ4edNCiM6YBaNxsksHsFqPwypv3Aqn2MMuKqNvRqBdJXwonyH5UFE2ofW9J/kgE
iyAY8fv5moNo8odRhgv5n253MnjltB0EgkwbikOnCqQ0/BBObK7TCv39Of4Th/u1
z7mXS3pk7pEun7EY610ZS+2obOKorl1Wam3dhBEef2JEzbYyadMS+5X3PDc/1xg7
Xsl4Q8swsJYGXX90BYJqRM9zJ13n/N4eUI43WyDJGeyO/L2gRek7QPq4P/YYSP9x
r+7WE1G4EUrdy+uF8U59ylS8xwKRJVdZ9SsMdYtXjcQqgVtVO1SkcbKC1cLTOzoL
3BBAoaINkVzCWJNnkRWOjsSwXlsLkqIN3+lod7zXZoBmnsj1KcWuaUnHXfp4UTJG
Mjih8mj5Ke8DcydsI34PYmQeD5eDYb8EYN0CDrDPnZ394nFh8grUSXy80dOOUOeG
SacFB/zyYjcT7bY5e5zCzIFIG8YfSM/+YZVk7xqdHa1vp7mcy5sTbrBiPvzQkbiA
ifXf80ZKJSxZD+Eex1HC8F6HKOo9RoxctRV1Pf/iKcNDeNX+ar58r1gi8Ie/fOmT
a2aUsUuhhdT/GV3Ui66UhWqnDO6zxqVOtVyWQ74yga0Ep9S9IemgiRgRvrJ+Ny46
Sl+hJtKv2fk//MxkTGVtle12J95Vhs0QzxQ9Qi2d30rnpsH9J5nM813MzL2Na4zl
kOPZAaYYjV6zD5UMKowSNBthVQOuK18Uw4ENcDBr8RdO9oYMQkqe8yQDV6FUyTDB
WgIOC1GfOHw+V5TFOiajr/exkZEOyBvva+DsSxaUPOzyasR406EhL9W6qJbn9uUw
5LDg+wsK93BG3slVN33CCcR8eJs72hxm6tR8URqyyu7a/pYh8v6Yuqwe72mM+huc
voPcrFCOhMceXuBgneBXx4T1WuCcYAR0e5DF5swMRP9IM35CjHdbH232kD2CuxSS
ksAYDoalcPHhcE6qM9FBmjqPlXsVr5lYmBqWSAtAKCKzJCiOlqNRw7g7L/r35+6W
O+eZ4aFJa3XbJnQaU/WcUvobtXXjmdLHKZI2kUhNK2f5SetjyQUHseCY/fqhCKyC
7fuOCTdcVf6nEcEuQowwGBzFrqGwU0nT/9yYG4JK2y3J+AeeHZAC/537XxgVSf88
NT6jX02vQp1zFukCJr0qgte90w6GLDVuug4zUP1JYa3mOjtEzYe4ch5DxYB017CD
0LNquCb4I45O8XvwwN8euirDT6HUqAS/7eEx
=riJc
-----END PGP MESSAGE-----
```

weitere Beispiele

Signatur:

```
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.6 (GNU/Linux)

iD8DBQFF0EPqSu67uwXOJGERAqqpAKCsJb00eK+p98fIzSZxAjzO1S1YrwCdHqK6
rGVetWBflGf5vaQ/2AnUmkg=
=/1Ep
-----END PGP SIGNATURE-----
```

Fingerprint:

```
$ gpg --fingerprint 0x05CE2461
pub   1024D/05CE2461 2005-03-16 [expires: 2007-03-16]
      Key fingerprint = 84B3 9B7A 2037 60DD B1BF  4A3F 4AEE BBBB 05CE 2461
uid                  andre meister <ilf@zeromail.org>
uid                  andre meister <ilf@gmx.net>
uid                  andre meister <andre.meister@student.hu-berlin.de>
uid                  andre meister <andrem@riseup.net>
uid                  andre meister <andre@reboot.fm>
sub   4096g/E57AD2AE 2005-03-16 [expires: 2007-03-16]
```

Philip Zimmermann

- 1954
- Programmierer
- Aktivist: Nuclear Weapons Freeze Campaign
- PGP Corporation
- 2006: Z-Fone

Pretty Good Privacy

- 1991: PGP „for protecting human rights overseas and for protecting grassroots political organizations at home“
- Release mit Source, Usenet, cypherpunks
- asymmetrische Kryptographie erstmals Allgemeinheit leicht zugänglich
- am weitesten verbreitete E-Mail Verschlüsselungs-Software

Krypto-Debatte

- 1993: Beginn Polizeiuntersuchung wegen „Export von Waffen ohne Lizenz“
- Export von Verschlüsselung >40 bit illegal
- Netscape: 2 Browser-Versionen mit SSL
- 1995: Buch „PGP Source Code and Internals“
- 1996: Promotion of Commerce On-Line in the Digital Era (Pro-CODE) Act 1996
- Anklage fallen gelassen

Pretty Good Privacy 2

- Patente: IDEA, RSA
- PGP 3: DSA, Diffie-Hellman
- PGP Corporation: 12 GPG-Produkte
- OpenPGP IETF Standard
  - RFC 2440 (1998): OpenPGP Message Format
  - RFC 3156 (2001): MIME Security with OpenPGP
- keine Backdoors

GNU Privacy Guard

- GPL Implementierung
- Werner Koch
- 1999: 1.0, 2006: 2.0
- Förderung von Bundesministerium für Wirtschaft und Arbeit (BMWA) und Bundesministerium des Innern (BMI)
- Plug-ins: Enigmail (Thunderbird), GPGMail (Apple Mail), ...

Fazit

Nutzt GPG!

Quellen 1

- Zimmermann; Philip (1995): PGP Source Code and Internals. MIT Press.
- Zimmermann, Philip: Creator of PGP. Background. In: http://www.philzimmermann.com/EN/background/background.html; Zugriff: 05.02.2007.
- Zimmermann, Philip: The Early Roots of PGP. In: http://www.philzimmermann.com/EN/background/peace.html; Zugriff: 05.02.2007.
- Zimmermann; Philip (1999): Why I Wrote PGP. In: http://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html; Zugriff: 06.02.2007.
- Zimmermann, Philip (1996): Testimony of Philip R. Zimmermann to the Subcommittee on Science, Technology, and Space of the US Senate Committee on Commerce, Science, and Transportation. In: http://www.philzimmermann.com/EN/essays/Testimony.html; Zugriff: 10.02.2007.

Quellen 2

- Bernauer, Alexander: Die Geschichte der Kryptographie und Kryptoanalysis. ein geschichtlicher Abriß. In: http://www.ulm.ccc.de/old/chaos-seminar/krypto2/; Zugriff: 05.02.2007.
- Schneier, Bruce (1996): Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley.
- Network Working Group (1998): Request for Comments: 2440. OpenPGP Message Format. In: http://www.ietf.org/rfc/rfc2440.txt.; Zugriff: 08.02.2007.
- Network Working Group (2001): Request for Comments: 3156. MIME Security with OpenPGP. In: http://www.ietf.org/rfc/rfc3156.txt; Zugriff: 08.02.2007.
- Raven, Kai: Deutsche GnuPG Anleitung. In: http://hp.kairaven.de/pgp/gpg/; Zugriff: 07.02.2007

Quellen 3

- http://de.wikipedia.org/
- http://en.wikipedia.org/
- http://www.pgp.com/
- http://www.openpgp.org/
- http://www.gnupg.org/
- http://blog.fefe.de/?q=gnupg
- https://www.b3rt.de/code/gpgsymcrack/
- http://www.philzimmermann.com/images/photos/PRZ_closeup.jpg; Zugriff: 11.02.2007.
- http://logo-contest.gnupg.org/logo-draft-1.png; Zugriff: 11.02.2007.