

E-Mail-Verschlüsselung



2009-05-25

Stefan Hensel

Seminar: Office

Dozent: Peter Medwed

Staatliche Technikerschule Berlin

Vier Nachrichten



- ⌘ Schaden der deutschen Wirtschaft durch IT-Angriffe: Mehrere Milliarden Euro pro Jahr.
- ⌘ Gmail scannt E-Mails und wertet sie aus.
- ⌘ Über 10.000 Laptops verschwinden pro Woche auf US-Flughäfen.
- ⌘ Beratungsstellen werden nicht mehr angerufen oder angemailt.

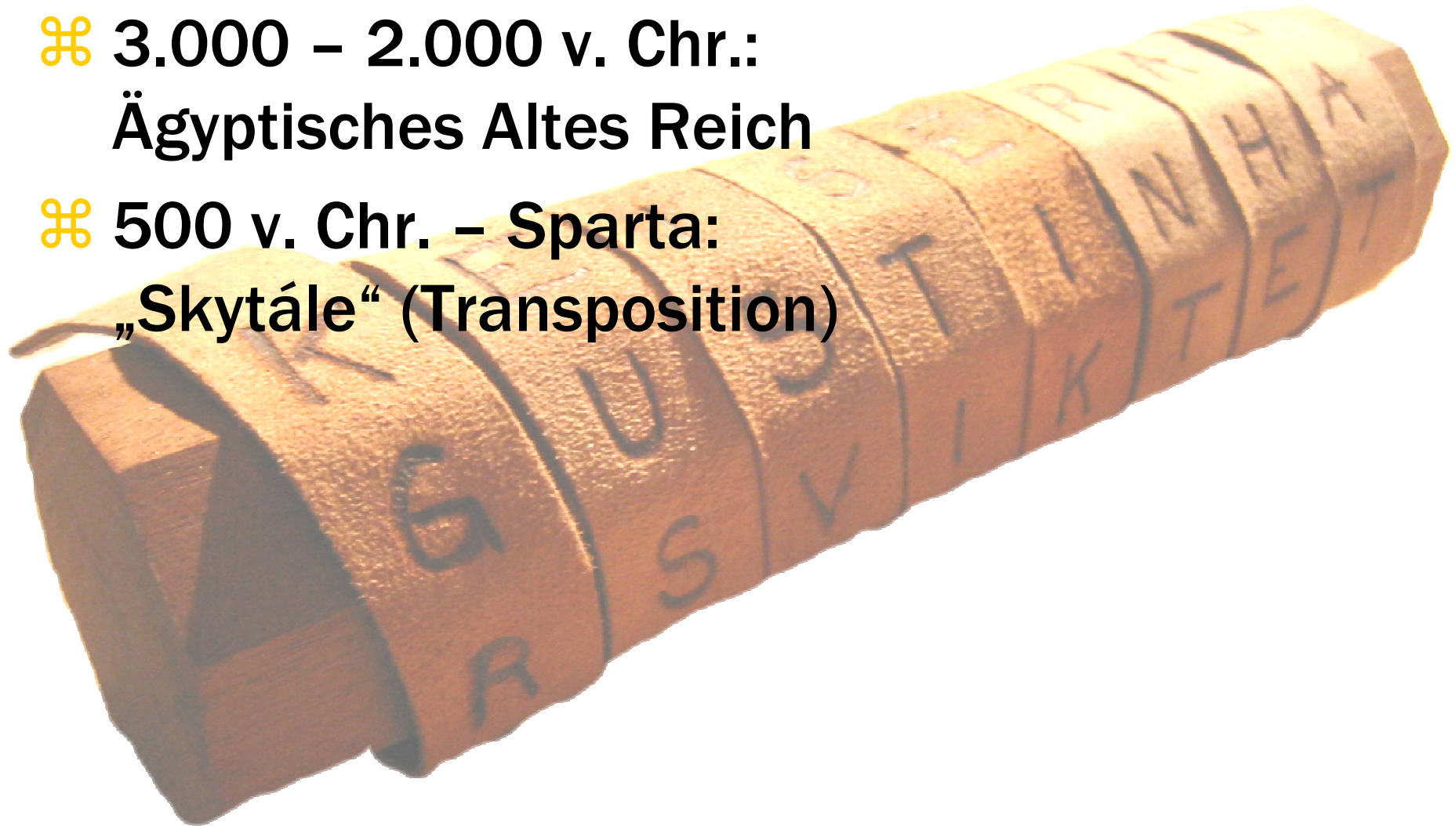
Übersicht

- ⌘ Meilensteine
- ⌘ Einsatzgebiete
- ⌘ Symmetrische und asymmetrische Verschlüsselung
- ⌘ PGP und S/MIME
- ⌘ Praktischer Einsatz
- ⌘ Noch zu lösen ...

Meilensteine: Pyramiden und Stöcke

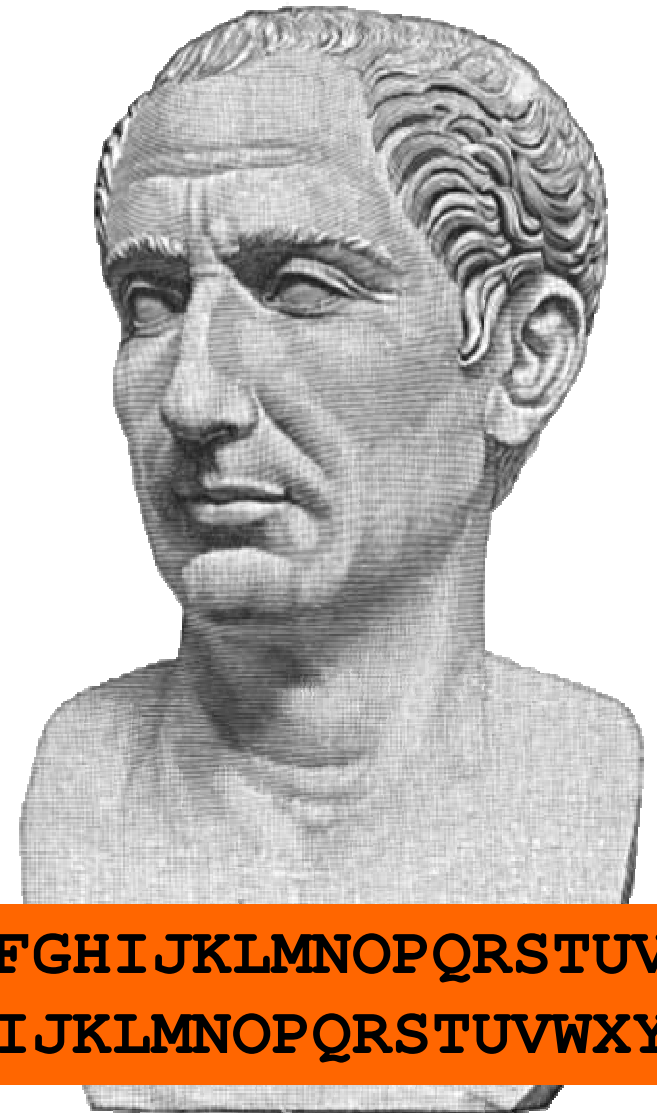
⌘ 3.000 – 2.000 v. Chr.:
Ägyptisches Altes Reich

⌘ 500 v. Chr. – Sparta:
„Skytále“ (Transposition)



Meilensteine: Was haben uns die Römer gebracht?

- ⌘ 50 v. Chr.: Caesar (Substitution)
- ⌘ 16. Jh.: Vigenère-Verschlüsselung ermöglicht „Passwörter“
- ⌘ 1976: DES verkettete Permutation und Substitution



ZABCDEFGHIJKLMN OPQRSTUVWXYZABCDEFGHIJKLMN OPQRSTUVWXYZ
CDEFGHIJKLMN OPQRSTUVWXYZABCDEFGHIJKLMN OPQRSTUVWXYZ

Meilensteine: Security by Transparency

Kerckhoffs'sches Prinzip
(1883):

- ⌘ „Nur der Schlüssel ist das Geheimnis“
- ⌘ Geheimhaltung des *Schlüssels* statt Geheimhaltung des *Algorithmus*
- ⌘ Open-Source-Prinzip



Meilensteine: Maschinelle Verschlüsselung

Enigma (1918 – 1945):

- ⌘ **Rotor-Schlüsselmaschine**
- ⌘ **Militär des Deutschen Reiches**
- ⌘ **Entzifferung 1938 – 1943 (PL, GB, USA)**
 - **entscheidend für den Sieg der Alliierten**



Meilensteine: Das digitale Zeitalter

- ⌘ 1949: Claude Shannon:
 - Kryptografie auf starker mathematischer Basis
- ⌘ 1976: DES
- ⌘ Public-Key-Kryptographie:
 - 1976: Diffie & Hellman
 - 1977: RSA
- ⌘ 1991: Pretty Good Privacy (PGP) – Phil Zimmermann



Übersicht

- ⌘ Meilensteine
- ⌘ Einsatzgebiete
- ⌘ Symmetrische und asymmetrische Verschlüsselung
- ⌘ PGP und S/MIME
- ⌘ Praktischer Einsatz
- ⌘ Noch zu lösen ...

Wer braucht Verschlüsselung?



⌘ Militär

⌘ Geheimdienste

⌘ Untergrund-
organisationen

⌘ Radikale

⌘ Kriminelle

⌘ Unternehmen

⌘ Banken,
Online-Handel

⌘ Behörden

⌘ Journalisten

⌘ Rechtsanwälte

⌘ Du und ich?

Was wird verschlüsselt?

Verschlüsselung
Verschleierung

lokal

E-Mail

remote

Dateien
Ordner

Partitionen

Übertragung

Kommuni-
kation

FileCrypter
RAR, 7zip

NTFS

SSL, TLS

ReMailer

Stegano-
grafie

(Signatur)

TrueCrypt

WPA

HTTPS

TOR, JAP

Übersicht

- ⌘ Meilensteine
- ⌘ Einsatzgebiete
- ⌘ Symmetrische und asymmetrische Verschlüsselung
- ⌘ PGP und S/MIME
- ⌘ Praktischer Einsatz
- ⌘ Noch zu lösen ...

Eine Schlüsselfrage

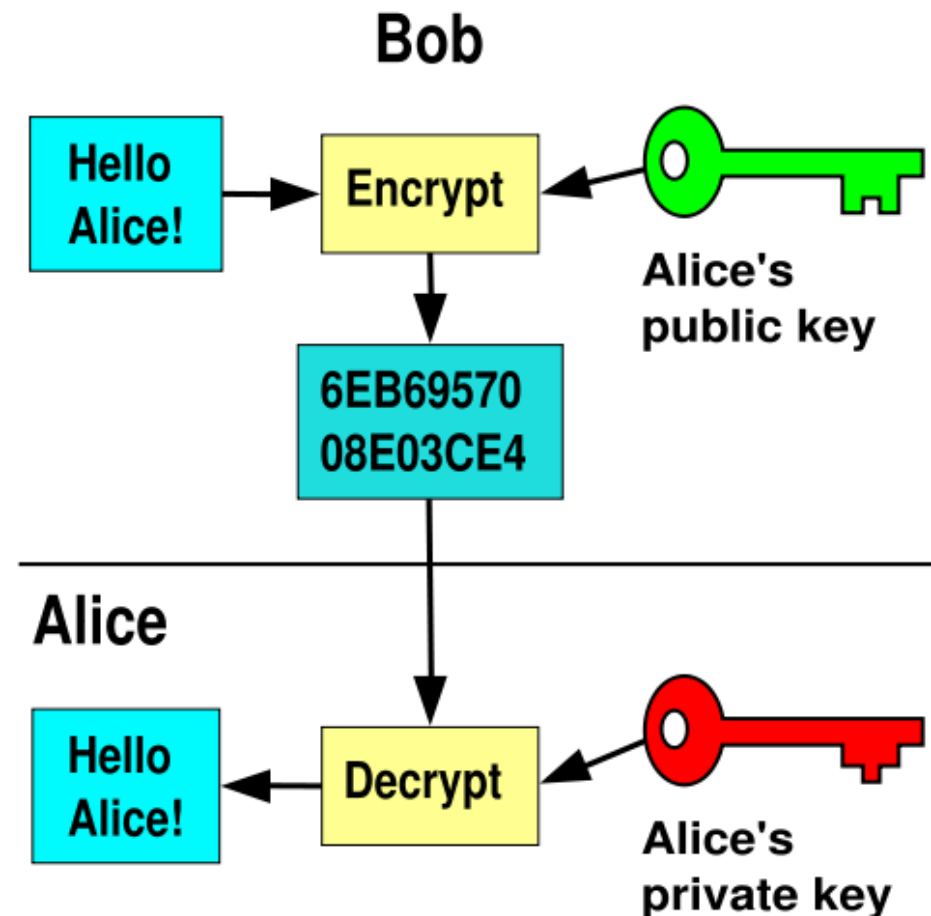
Problem der
Schlüsselübertragung:

- ⌘ Geheimer Schlüssel
- ⌘ Austausch über unsicheren Kanal
- ⌘ → unsichere Verschlüsselung!



Public-Key-Verfahren

- ⌘ Asymmetrische Verschlüsselung
- ⌘ Zwei zusammengehörende Schlüssel:
 - Öffentlich – Verschlüsselung
 - Privat – Entschlüsselung



Wie schmiedet man ein Schlüsselpaar?

Algorithmen basierend auf ...

⌘ Faktorisierung:

- RSA

$$37.619 \cdot 75.991 = ?$$

- Rabin

$$2.858.705.429 = ? \cdot ?$$

⌘ Diskretem Logarithmus:

- Diffie-Hellman (angreifbar)

- Elgamal

⌘ Elliptischen Kurven

- kleinere Schlüssel bei gleicher Sicherheit

Symmetrisch oder asymmetrisch?

Symmetrisch:

- ⌘ viele Schlüssel
(quadratisch)
- ⌘ > 2 Empfänger:
zunehmend
unsicher
- ⌘ Übertragungs-
Problem
- ⌘ schnell

Asymmetrisch:

- ⌘ wenige Schlüssel
(linear)
- ⌘ > 2 Empfänger:
Mehrfach-
verschlüsselung
- ⌘ Man-In-The-Middle-
Angriff
- ⌘ langsam

Symmetrisch *und* asymmetrisch.

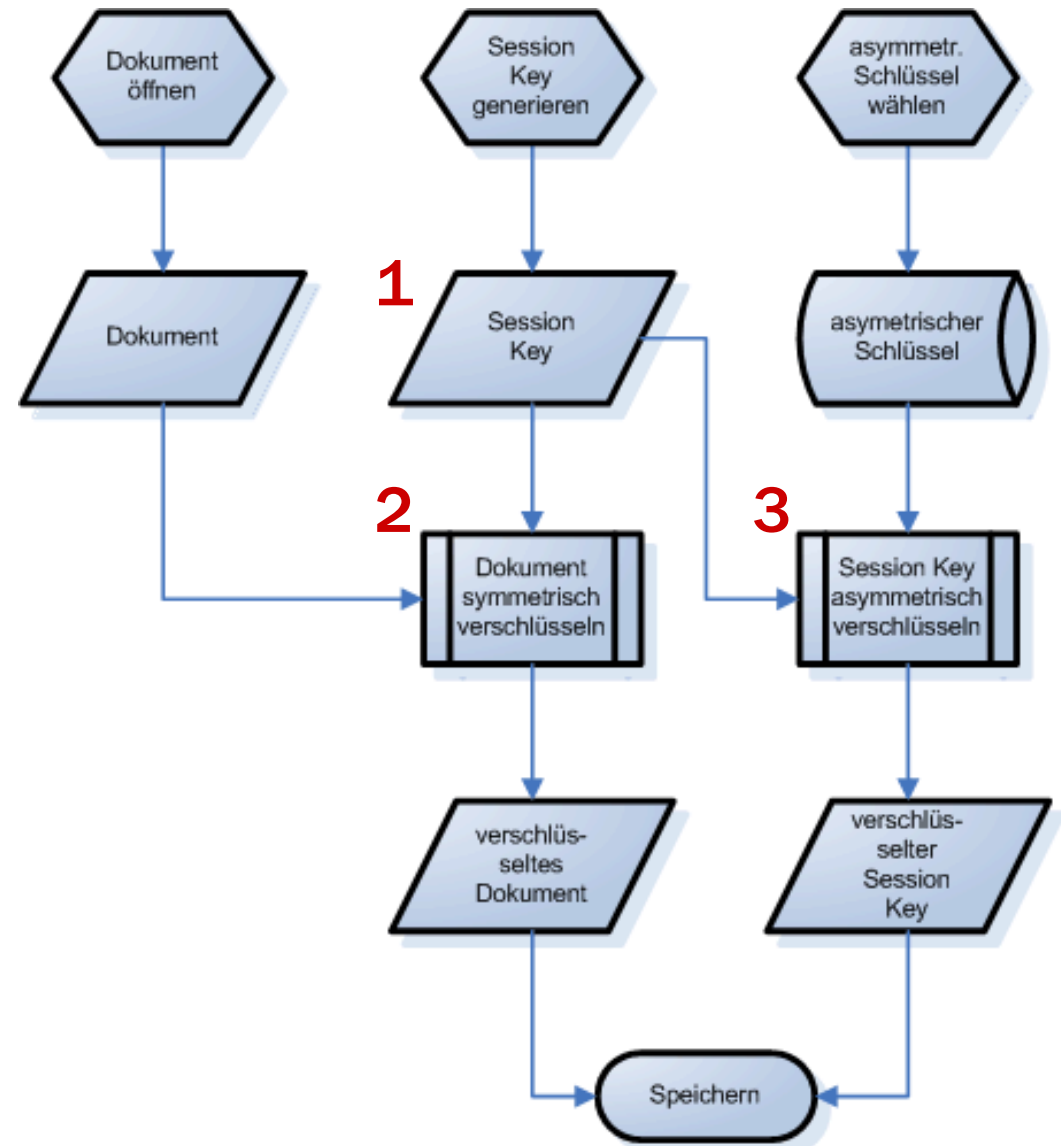
Hybrid-Verschlüsselung:

- ⌘ Inhalt
symmetrisch
verschlüsselt
- ⌘ Schlüssel
asymmetrisch
verschlüsselt



Hybrid-Verschlüsselung: Doppelt genäht hält besser.

- ⌘ Zufälligen Schlüssel (Session Key) erzeugen (1)
- ⌘ Inhalt symmetrisch verschlüsseln (2)
- ⌘ Session Key asymmetrisch verschlüsseln (3)



Übersicht

- ⌘ Meilensteine
- ⌘ Einsatzgebiete
- ⌘ Symmetrische und asymmetrische Verschlüsselung
- ⌘ PGP und S/MIME
- ⌘ Praktischer Einsatz
- ⌘ Noch zu lösen ...

OpenPGP – Ein Industriestandard



- ⌘ **Internet-Standard (RFC 4880)**
- ⌘ **basiert auf PGP 5.x**
- ⌘ **Hybrides Verschlüsselungssystem**
- ⌘ **Public Key Infrastructure:**
 - **Schlüsselservers**
 - **Web of Trust**
 - ◆ **Hierarchische PKI implementierbar**

S/MIME -

Noch ein Industriestandard



- ⌘ **Standard eines Herstellerkonsortiums**
- ⌘ **basiert auf RFC 2311 - 2315**
- ⌘ **Hybrides Verschlüsselungssystem**
- ⌘ **Public Key Infrastructure:**
 - **Zertifizierungsstellen**
 - **hierarchisch**

OpenPGP vs. S/MIME

	OpenPGP	S/MIME
Prinzip	hybrid	hybrid
Signatur	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Algorithmen (asymmetrisch)	RSA, ElGamal, (Elliptic Curve, Diffie-Hellman)	RSA
Algorithmen (symmetrisch)	TripleDES, IDEA, CAST5, Blowfish, SAFER-SK128, Twofish, (DES/SK, AES/Rijndael)	TripleDES, DES, RC2

OpenPGP vs. S/MIME

	OpenPGP	S/MIME
Standardisierung	RFC	IETF
PKI	Öffentliche Schlüssel (flexibel) Netzwerk, (Hierarchie)	Zertifizierungs- stellen hierarchisch (X.509)
Betriebssysteme	fast alle	Windows bevorzugt
geeignet für	E-Mails, Dateien, Partitionen, IP- Traffic	E-Mails

Übersicht

- ⌘ Meilensteine
- ⌘ Einsatzgebiete
- ⌘ Symmetrische und asymmetrische Verschlüsselung
- ⌘ PGP und S/MIME
- ⌘ Praktischer Einsatz
- ⌘ Noch zu lösen ...

Verschlüsselung praktisch: GnuPT

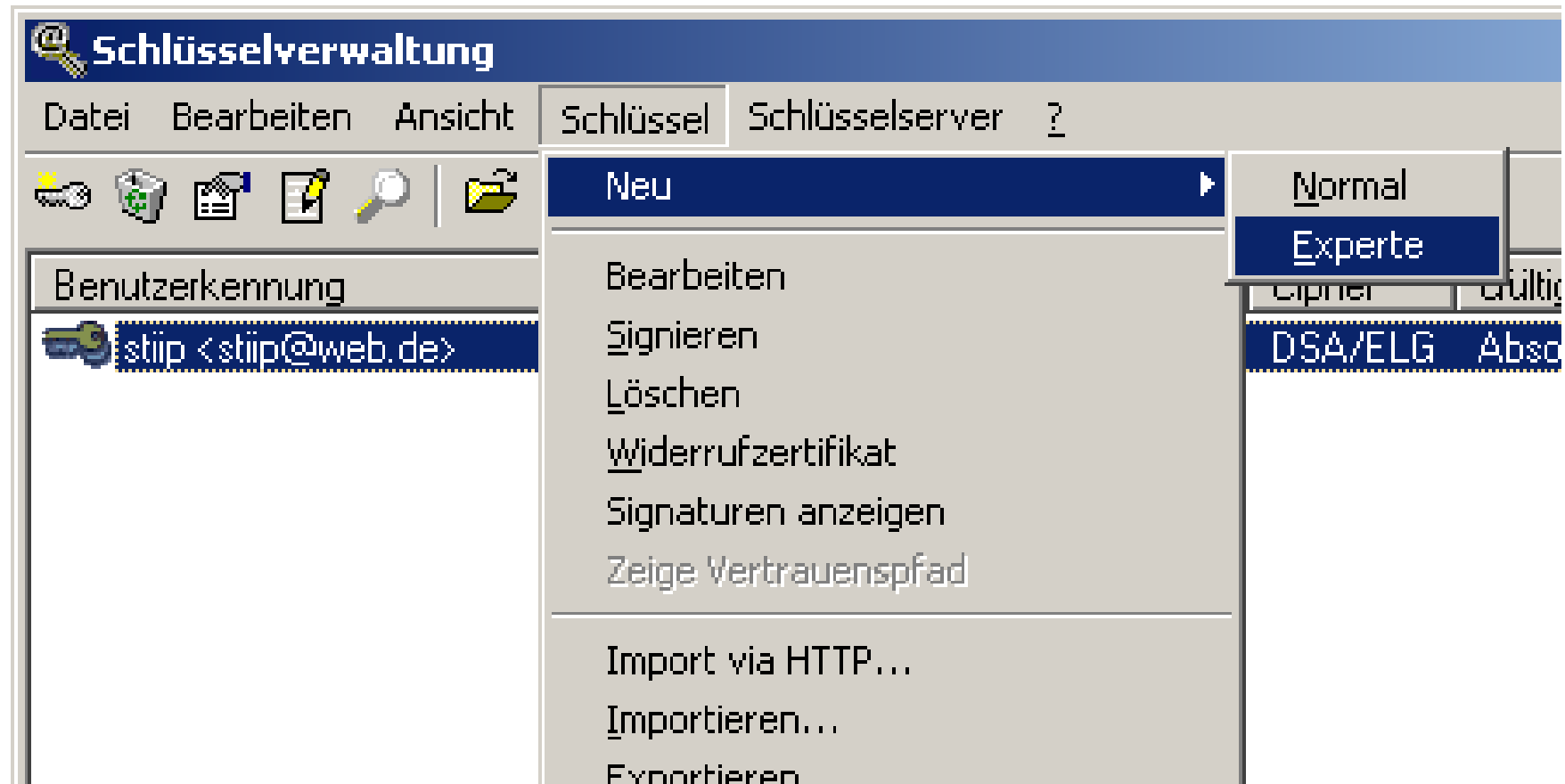


⌘ Komponenten:

- GnuPG (Gnu Privacy Guard)
- Frontend
- WinPT (Windows Privacy Tray)

⌘ <http://www.gnupt.de/wp/>

GnuPG: Schlüssel generieren



GnuPG: Schlüssel generieren

Schlüsselerzeugung [X]

Die Schlüsselerstellung kann eine Weile dauern!
Bitte warten Sie, bis eine Meldung über die
Beendigung der Schlüsselerzeugung erscheint.

Schlüssel Typ DSA und ELG (Standard) ▼

Schlüsselgröße in 2048 1024-4096

Ihr Name Stefan Hensel

Kommentar

E-Mail-Adresse stefan.hensel@email.de

Ablaufdatum Niemals 25.05.09 ▼

GnuPG: Schlüssel generieren

Schlüsselerzeugung - Fortschrittsdialog

```
+++++ . . +++++ .  
+++++ . . +++++ .  
+++ . . +++ . . +++++ . . . . .  
 . . . . . >++++ . <++++ . . . . .  
 . >++++ . . . . +++++
```

Verschlüsselung praktisch: Enigmail und Thunderbird

Enigmail:

⌘ Add-on für Thunderbird

⌘ integriert

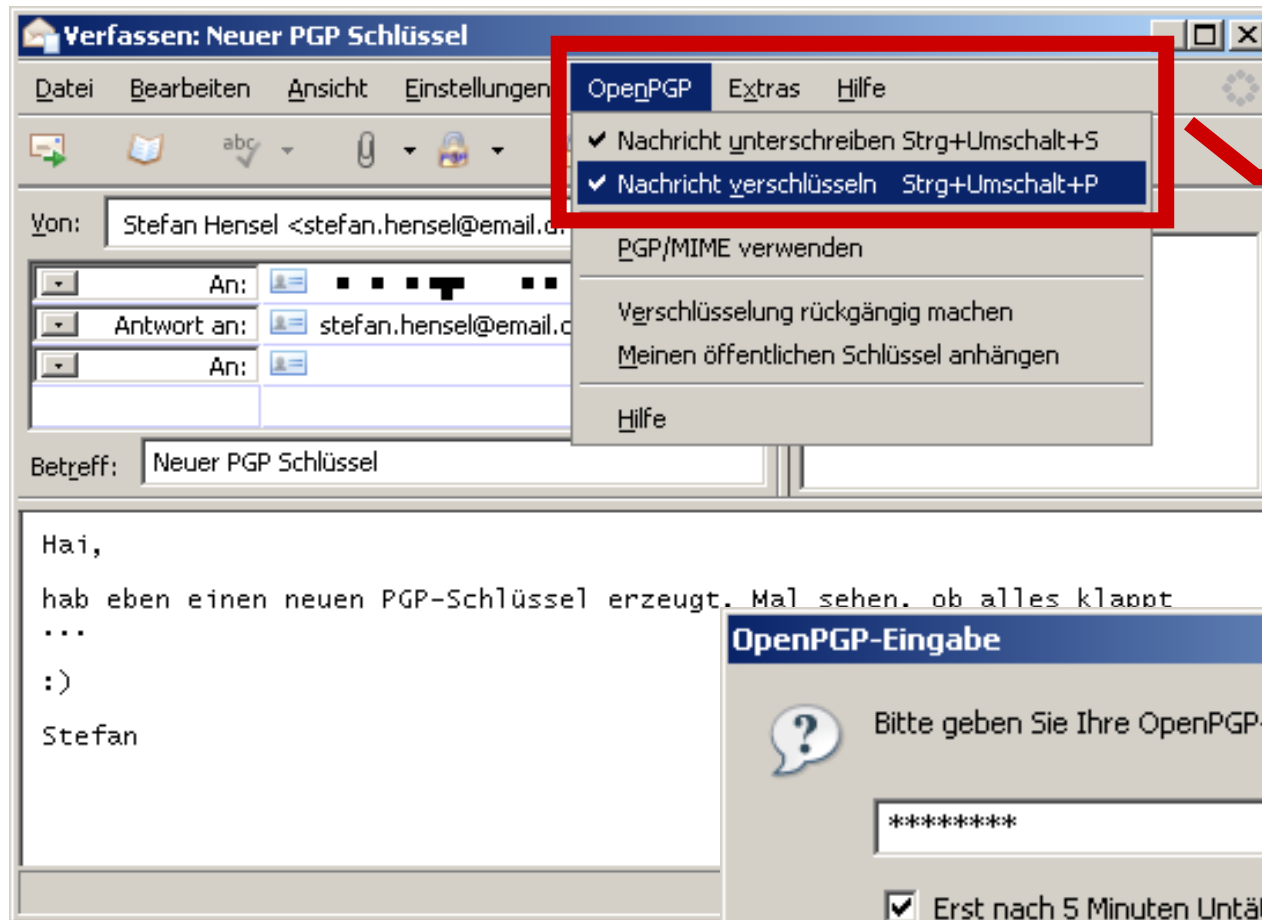
- OpenPGP-Verschlüsselung

- Authentifizierung

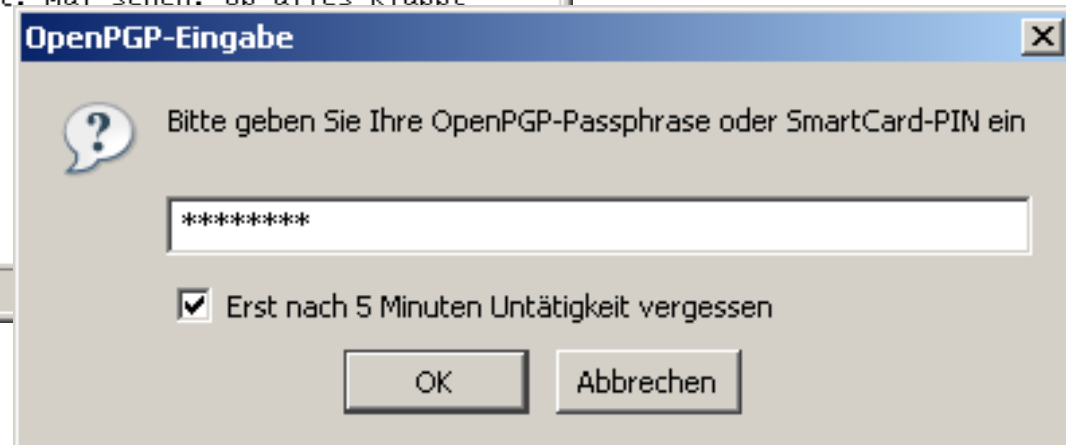
⌘ OpenPGP/GnuPG muss installiert sein

⌘ <https://addons.mozilla.org/de/thunderbird/addon/71>

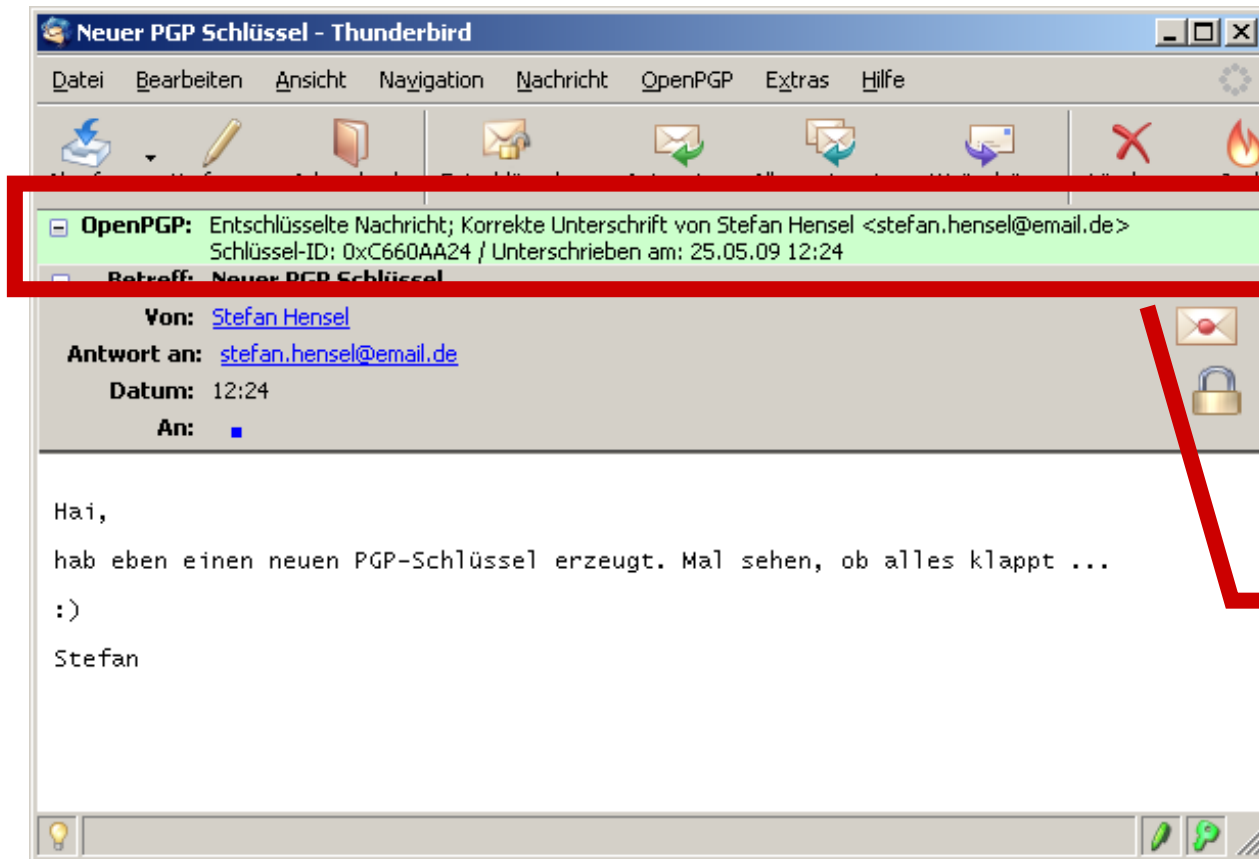
Verschlüsselung praktisch: Enigmail und Thunderbird



Öffentlicher
Schlüssel des
Empfängers



Verschlüsselung praktisch: Enigmail und Thunderbird



Privater
Schlüssel des
Empfängers

Verschlüsselung praktisch: Enigmail und Thunderbird

```
-----BEGIN PGP MESSAGE-----  
Charset: ISO-8859-15  
Comment: GnuPT v3.6.4  
Comment: Download: http://www.gnupt.de  
Comment: Using GnuPG with Mozilla - http://enigmail.mozdev.org
```

```
hQIOA4fYg1w2h077EAf9HNxAU5nnK6oL9BSQA2YJCKRZDBCd/f7MWFTCorZwpuqe  
Wr4wMiAdwRRmhVY8ke3Xeh3i+s0uuIoxzA1+W40DptT3n00IT662vd045uNy2cNk  
sgol3VlPN+c+01qUFop9Wpos3Cw+u0XqmnivDIQa76AawR0tpz2xGI1E+48dXV6  
C5xd0og45VlW0CI7pduNYURneG6IwP i3lqDUV68hXhhtEuZUw0D+zj iK4w2wmcVC  
YbfcQsn4E5GK0Q2f2IwmRaGUm7apj+wdgC0 izYMLspnsxf8ur2fbmUkbVispWokM  
GgISt/4RFsr2gV0f/PbMKrsUWtoPb32BrDRiPi2Kogf7B8QZ1AphXuqvLNP+ROB1  
NsV7a6Tcvk+fhXfk1rtlI5cIp674lufglXzITuSHPssc10fWmpPXdP63lWUwlzH5  
wLP1sNKqVh7YQDt6T5d3ZOM9orvi/qmfa5K24swRsPdA6MxpG/FPLx2hkeUKER99  
Rr/6IT08wDFhfGB1dUvSmhmbBn3T8N7l6g0fHMGsoltwLYHfprx0cE25q0xEkyh9  
U+1ZXzATAep0QimX+Edfon0qsNk2wYpZnaFUDwf0/At9S9siHhK7TKY28tiPgUDJ  
i7RCTaiYudRUNtU2Q339e1VKA0u0IVxzwS51y0jsJgV3whHrIZmxcUobLxYHDXZH  
6oUCDgMGafUyFlowlBAH/0hGP1zm2dYz i+WY2YqJGcy6f+ C21E2/Kvf7FdYOPRXT  
rTuYHogmA0cTKsHTEbf10z0iaqj7H5N+5fG0lMszQJaTiY7Jw0P1z0+1m2gpNr0N  
7gWmHv0rFqkXLZ/758hg3q1RSiG/f1v7PD7iz3PZSuItkS0Ch+j+cXdFk81ayLkU  
OnLHQjFMkto5/3Vfcu9vTyXLuzfXIk4Ss2PkmHvwZd0a0zH3topazndHDEm0EVs2  
T1xhljt9A5Nlk5SSzMMpCIIowf4q7F440kRhYQ5FcG9r60YxtYav9X+sCBKhyLz  
g5LMLZForumMjWd8iRaSwnrRJ3vxyBF7pZYricWM2/kH/jdLBAJHDb5ABPp5iuAv  
x1Q0tTB6LohBYL8VPzwU1pD2vKSgXHVxIwz1US06Bup3NXujn/EeGt00cQFG0Hzh  
ezAhosHu7gcMaxPbYbz3E5c+47di28qwxDGyCFPOUqZ+yBQ9d6omMIsGqTbmQ8vc  
nH24nGhm3jLcM4701m+azX+dDbWvc4zY+v0Ae1IezVvvTzzff8v9/V4zEfa90jkr  
+h2eRITKEAD1JEZMmqY5DCfk/RqpEjJt37P6FqbGHwGblGZXu//oNl2v0KbTbC9Z  
Vz9VcgtVVPV66e6U/nXsh3Hosye9pdopKWHXY31kFPYzXvnxW61RZb20lGp+bPis  
0GrSwCsbtjFULLNRgmLMeuv70jsci5+ilnmEGC7yt/pcspKw04Yn00n5hY1b08r  
g2qAB0V30aIDN97tvu1BwlBq2Nsgu0q2+X0sGSmYkbbVmM/0G1EyeCsE+HIUGmim  
8B3uZT9AR66fxTdpwJFmXo2umjgXzI8+MubTS9l8wgF7Zq2dZ5wTcto76rflqmN3  
pIct6Ra4yulDwyilDT6k7Ss3GjpdftAzXbntIhbo63Qs31gRpnI6kzt0FncVQUv  
pCRl04h+LaLnwJJpac3gAsh27/Wzsc4BxcTicA92MuH0yvrC8DF1aUExoJieInYV  
=am6p  
-----END PGP MESSAGE-----
```

Verfahren
im
Klartext!

Was
tatsächlich
übermittelt
wurde

Übersicht

- ⌘ Meilensteine
- ⌘ Einsatzgebiete
- ⌘ Symmetrische und asymmetrische Verschlüsselung
- ⌘ PGP und S/MIME
- ⌘ Praktischer Einsatz
- ⌘ Noch zu lösen ...

Noch zu lösen ...



- ⌘ Zwei konkurrierende Standards
 - PGP und S/MIME inkompatibel trotz gleicher Verfahren
- ⌘ Wenige Teilnehmer
- ⌘ Mobiler Einsatz
- ⌘ Überwachung der Verkehrsdaten
- ⌘ Vertrauen

... aber:

**Privatsphäre
ist ein
Menschen-
recht!**



Quellen



- Arbeitskreis Vorratsdatenspeicherung (2008): Forsa-Umfrage: Vorratsdatenspeicherung verhindert sensible Gespräche. Pressemitteilung des Arbeitskreis Vorratsdatenspeicherung vom 03./04.06.2008. Arbeitskreis Vorratsdatenspeicherung. Online verfügbar unter http://www.daten-speicherung.de/data/forsa_2008-06-03.pdf, zuletzt aktualisiert am 2008-06-03 Di, zuletzt geprüft am 2009-05-24 So.
- Bundesnetzagentur (2009): Bundesnetzagentur | Häufig gestellte Fragen zur Vorratsdatenspeicherung. Bundesnetzagentur. Online verfügbar unter http://www.bundesnetzagentur.de/enid/Informationen_zum_Thema__Vorratsdatenspeicherung_/Haeufig_gestellte_Fragen_zur_Vorratsdatenspeicherungu_4rq.html, zuletzt aktualisiert am 2009-05-24, zuletzt geprüft am 2009-05-24 So.
- Financial Times Deutschland online (2009): FTD.de - Forschungsprojekt: Alarmanlage gegen Hacker-Angriffe - Forschung. Financial Times Deutschland online. Online verfügbar unter http://www.ftd.de/forschung_bildung/forschung/:Forschungsprojekt-Alarmanlage-gegen-Hacker-Angriffe/497283.html, zuletzt aktualisiert am 2009-04-06, zuletzt geprüft am 2009-05-25 Mo.
- Hauer, Philipp (2006-12-13): Asymmetrische Verschlüsselung. Theoretische Abhandlung. Eine Präsentation von Philipp Hauer 2006. Veranstaltung vom 2006-12-13. Ribnitz-Damgarten. Online verfügbar unter <http://www.philippbauer.de/info/info/asymmetrische-verschluesselung/asymmetrische-Verschluesselung.ppt>, zuletzt geprüft am 2009-05-24 So.
- Hauer, Philipp (2006): Asymmetrische Verschlüsselung/Public-Key-Verfahren. Das Verfahren. Die Vorteile/Pro und Nachteile/Kontra. Eine Präsentation von Philipp Hauer vom 13.12.2006. Erstmals gehalten am Richard-Wossidlo-Gymnasium. Online verfügbar unter <http://www.philippbauer.de/info/info/asymmetrische-verschluesselung/>, zuletzt aktualisiert am 24.05.09, zuletzt geprüft am 2009-05-24 So.
- Kersken, Sascha (2008): IT-Handbuch für Fachinformatiker. 19.2 Netzwerk- und Serversicherheit. Galileo Press. (Galileo Computing). Online verfügbar unter http://openbook.galileocomputing.de/it_handbuch/fachinformatiker_19_it_sicherheit_002.htm, zuletzt aktualisiert am 2007-10-31, zuletzt geprüft am 2009-05-23 Sa.
- Kirsch, Christian (2001): S/MIME vs. OpenPGP: Eine Entscheidungshilfe. Management und Wissen. E-Mail-Verschlüsselung. Online verfügbar unter <http://www.kes.info/archiv/online/01-01-60-SMIMEvsOpenPGP.htm>, zuletzt aktualisiert am 2001-05-17, zuletzt geprüft am 2009-05-25 Mo.
- Kreutzmann, Ralf: GnuPT 3.6.4 | Gnu Privacy Tools. Online verfügbar unter <http://www.gnupt.de/wp/?p=3>, zuletzt geprüft am 2009-05-25 Mo.
- mozilla.org (2008): Enigmail :: Thunderbird Add-ons. mozilla.org. Online verfügbar unter <https://addons.mozilla.org/de/thunderbird/addon/71>, zuletzt geprüft am 2009-05-25 Mo.
- Müller-Quade, Jörn (o. J.): Hieroglyphen, Enigma, RSA. Eine Geschichte der Kryptographie. Fakultät für Informatik, Universität Karlsruhe (TH). Online verfügbar unter <http://iaks-www.ira.uka.de/eiss/fileadmin/User/enigma.pdf>, zuletzt aktualisiert am 2006-10-26 Do, zuletzt geprüft am 2009-05-24 So.
- Otto, Alexander (2003): Internet-Sicherheit für Einsteiger. Für Homeanwender & kleine Firmennetze. Sicherheitslücken & Abwehrmaßnahmen, Schritt-für-Schritt-Anleitungen, CD-ROM mit vielen Sicherheits-Tools. 1. Aufl. Bonn: Galileo Press.
- Patholog [Pseudonym] (2008): Gmail and expose... Security for Dummies. Online verfügbar unter <http://security4dummies.wordpress.com/2008/07/12/gmail-and-expose/>, zuletzt aktualisiert am 23.05.09, zuletzt geprüft am 2009-05-23 Sa.
- Shah, Agam (2008): Laptops Lost Like Hot Cakes at US Airports - Business Center - PC World. Monday, June 30, 2008 12:30 PM PDT. PC World Business Center. Online verfügbar unter http://www.pcworld.com/businesscenter/article/147739/laptops_lost_like_hot_cakes_at_us_airports.html, zuletzt aktualisiert am 2009-05-23, zuletzt geprüft am 2009-05-23 Sa.

Quellen



- Wikipedia (de) (2009): S/MIME - Wikipedia, the free encyclopedia. Wikipedia (de). Online verfügbar unter <http://en.wikipedia.org/wiki/S/MIME>, zuletzt aktualisiert am 2009-05-18, zuletzt geprüft am 2009-05-25 Mo.
- Wikipedia (de) (2009): Telekommunikations-Überwachungsverordnung – Wikipedia. Wikipedia (de). Online verfügbar unter <http://de.wikipedia.org/wiki/TK%C3%9CV>, zuletzt aktualisiert am 2009-05-19, zuletzt geprüft am 2009-05-24 So.
- Wikipedia (de) (2009): Symmetrisches Kryptosystem – Wikipedia. Wikipedia (de). Online verfügbar unter http://de.wikipedia.org/wiki/Symmetrisches_Kryptosystem, zuletzt aktualisiert am 2009-05-12, zuletzt geprüft am 2009-05-24 So.
- Wikipedia (de) (2009): Enigma (Maschine) – Wikipedia. Wikipedia (de). Online verfügbar unter [http://de.wikipedia.org/wiki/Enigma_\(Maschine\)](http://de.wikipedia.org/wiki/Enigma_(Maschine)), zuletzt aktualisiert am 2009-05-16, zuletzt geprüft am 2009-05-24 So.
- Wikipedia (de) (2009): Diffie-Hellman-Schlüsselaustausch – Wikipedia. Wikipedia (de). Online verfügbar unter <http://de.wikipedia.org/wiki/Diffie-Hellman-Algorithmus>, zuletzt aktualisiert am 2009-05-20, zuletzt geprüft am 2009-05-24 So.
- Wikipedia (de) (2009): Kryptographie – Wikipedia. Wikipedia (de). Online verfügbar unter <http://de.wikipedia.org/wiki/Kryptographie>, zuletzt aktualisiert am 2009-05-22, zuletzt geprüft am 2009-05-24 So.
- Wikipedia (de) (2009): Vorratsdatenspeicherung – Wikipedia. Wikipedia (de). Online verfügbar unter <http://de.wikipedia.org/wiki/Vorratsdatenspeicherung>, zuletzt aktualisiert am 2009-05-23, zuletzt geprüft am 2009-05-24 So.
- Wikipedia (de) (2009): RSA-Kryptosystem – Wikipedia. Wikipedia (de). Online verfügbar unter <http://de.wikipedia.org/wiki/RSA-Kryptosystem>, zuletzt aktualisiert am 2009-05-20, zuletzt geprüft am 2009-05-24 So.
- Wikipedia (de) (2009): Geschichte der Kryptographie – Wikipedia. Wikipedia (de). Online verfügbar unter http://de.wikipedia.org/wiki/Geschichte_der_Kryptographie, zuletzt aktualisiert am 2009-05-22, zuletzt geprüft am 2009-05-24 So.

Quellen



- Wikipedia (de) (2009): Asymmetrisches Kryptosystem – Wikipedia. Wikipedia (de). Online verfügbar unter http://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem, zuletzt aktualisiert am 2009-05-11, zuletzt geprüft am 2009-05-24 So.
- Wikipedia (de) (2009): OpenPGP – Wikipedia. Wikipedia (de). Online verfügbar unter <http://de.wikipedia.org/wiki/OpenPGP>, zuletzt aktualisiert am 2009-03-30, zuletzt geprüft am 2009-05-25 Mo.
- Wikipedia (de) (2009): Skytale – Wikipedia. Wikipedia (de). Online verfügbar unter <http://de.wikipedia.org/wiki/Skytale>, zuletzt aktualisiert am 2009-04-05, zuletzt geprüft am 2009-05-25 Mo.
- Wikipedia (de) (2009): Kerckhoffs' Prinzip – Wikipedia. Wikipedia (de). Online verfügbar unter http://de.wikipedia.org/wiki/Kerckhoffs%E2%80%99_Prinzip, zuletzt aktualisiert am 2009-03-07, zuletzt geprüft am 2009-05-24 So.
- Wikipedia (de) (2009): Rabin-Kryptosystem – Wikipedia. Wikipedia (de). Online verfügbar unter <http://de.wikipedia.org/wiki/Rabin-Kryptosystem>, zuletzt aktualisiert am 2009-03-25, zuletzt geprüft am 2009-05-24 So.
- Wikipedia (de) (2009): Elgamal-Kryptosystem – Wikipedia. Wikipedia (de). Online verfügbar unter <http://de.wikipedia.org/wiki/Elgamal-Kryptosystem>, zuletzt aktualisiert am 2009-04-12, zuletzt geprüft am 2009-05-24 So.
- Wikipedia (de) (2009): Verschiebechiffre – Wikipedia. Wikipedia (de). Online verfügbar unter <http://de.wikipedia.org/wiki/C%C3%A4sar-Chiffre>, zuletzt aktualisiert am 2009-04-30, zuletzt geprüft am 2009-05-24 So.
- Wikipedia (de) (2009): Claude Elwood Shannon – Wikipedia. Wikipedia (de). Online verfügbar unter http://de.wikipedia.org/wiki/Claude_Shannon, zuletzt aktualisiert am 2009-05-03, zuletzt geprüft am 2009-05-24 So.
- Wikipedia (de) (2009): Elliptic Curve Cryptography – Wikipedia. Wikipedia (de). Online verfügbar unter <http://de.wikipedia.org/wiki/Elliptische-Kurven-Kryptosystem>, zuletzt aktualisiert am 2009-04-13, zuletzt geprüft am 2009-05-24 So.
- Wikipedia (de) (2009): Hybride Verschlüsselung – Wikipedia. Wikipedia (de). Online verfügbar unter http://de.wikipedia.org/wiki/Hybride_Verschl%C3%BCsselung, zuletzt aktualisiert am 2009-04-23, zuletzt geprüft am 2009-05-24 So.

Danke fürs Zuhören

