MAILS VERSCHLÜSSELN

MIT PGP

„Encryption works.
Properly implemented strong crypto systems are
one of the few things that you can rely on.“

Edward J. Snowden, 17. Juni 2013

PIRATEN PARTEI

ELZPIRATEN EMMENDINGEN

INHALT

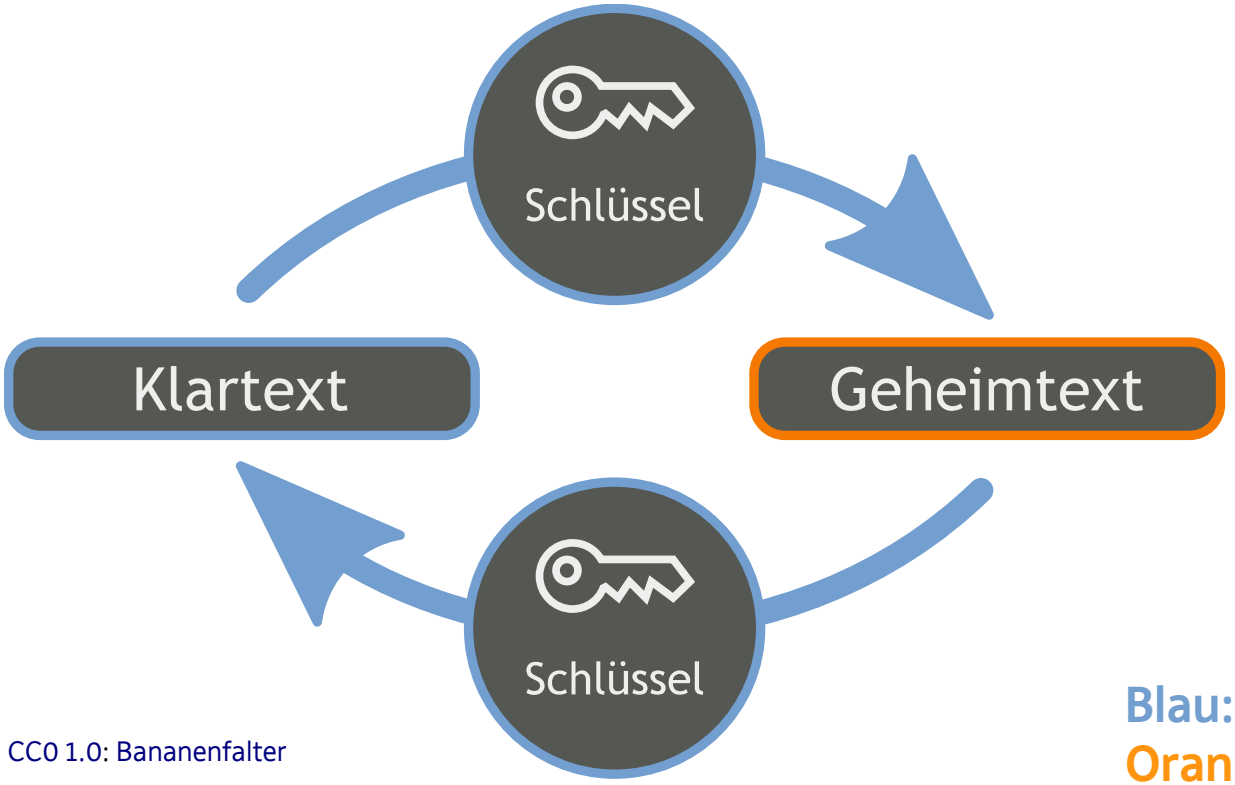
- Ein wenig Theorie zu Verschlüsselungsverfahren
- PGP? OpenPGP? GPG? WTF?
- Keysigning-Partys
- Die benötigten Werkzeuge
- Bedienung in der Praxis
- Was noch zu beachten wäre

EIN WENIG THEORIE ZU VERSCHLÜSSELUNGSVERFAHREN

- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung
- Hybride Verschlüsselung

SYMMETRISCHE VERSCHLÜSSELUNG

- Nutzung desselben Schlüssels für die Ver- und die Entschlüsselung



Blau: geheim
Orange: öffentlich

SYMMETRISCHE VERSCHLÜSSELUNG

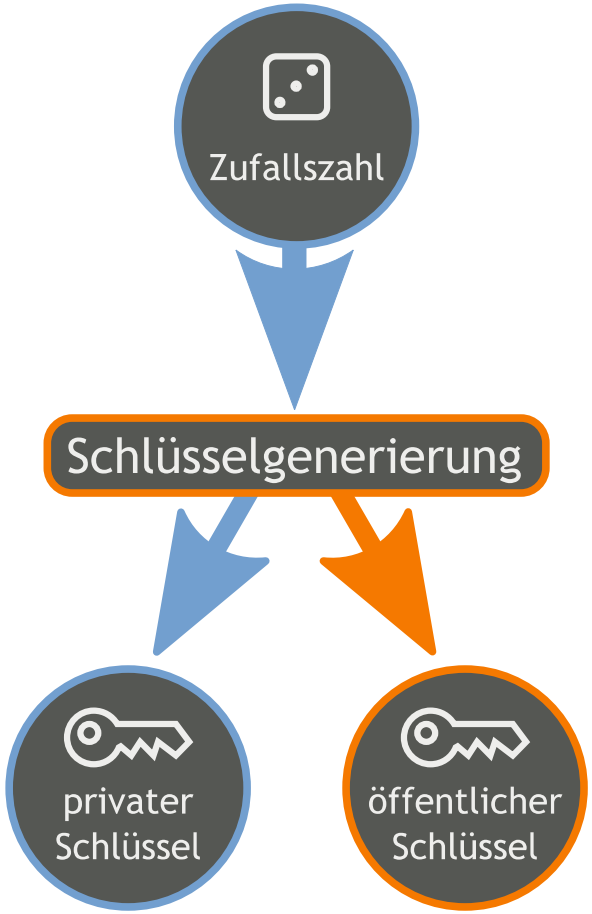
- Vorteile
  - Auch bei großen Datenmengen sehr schnell.
  - In Form eines One-Time-Pads nachweislich unknackbar
- Nachteile
  - Problem der sicheren Übermittlung des Schlüssels

SYMMETRISCHE VERSCHLÜSSELUNG

- Verfahren
  - AES, DES, Triple-DES, Twofish, Serpent
- Anwendungen
  - Wireless LAN (WPA2)
  - IP-Telefonie (SRTP)
  - Dateiverschlüsselung (TrueCrypt)
  - E-Mail (PGP, GPG)

ASYMMETRISCHE VERSCHLÜSSELUNG

- Nutzung eines Schlüsselpaares



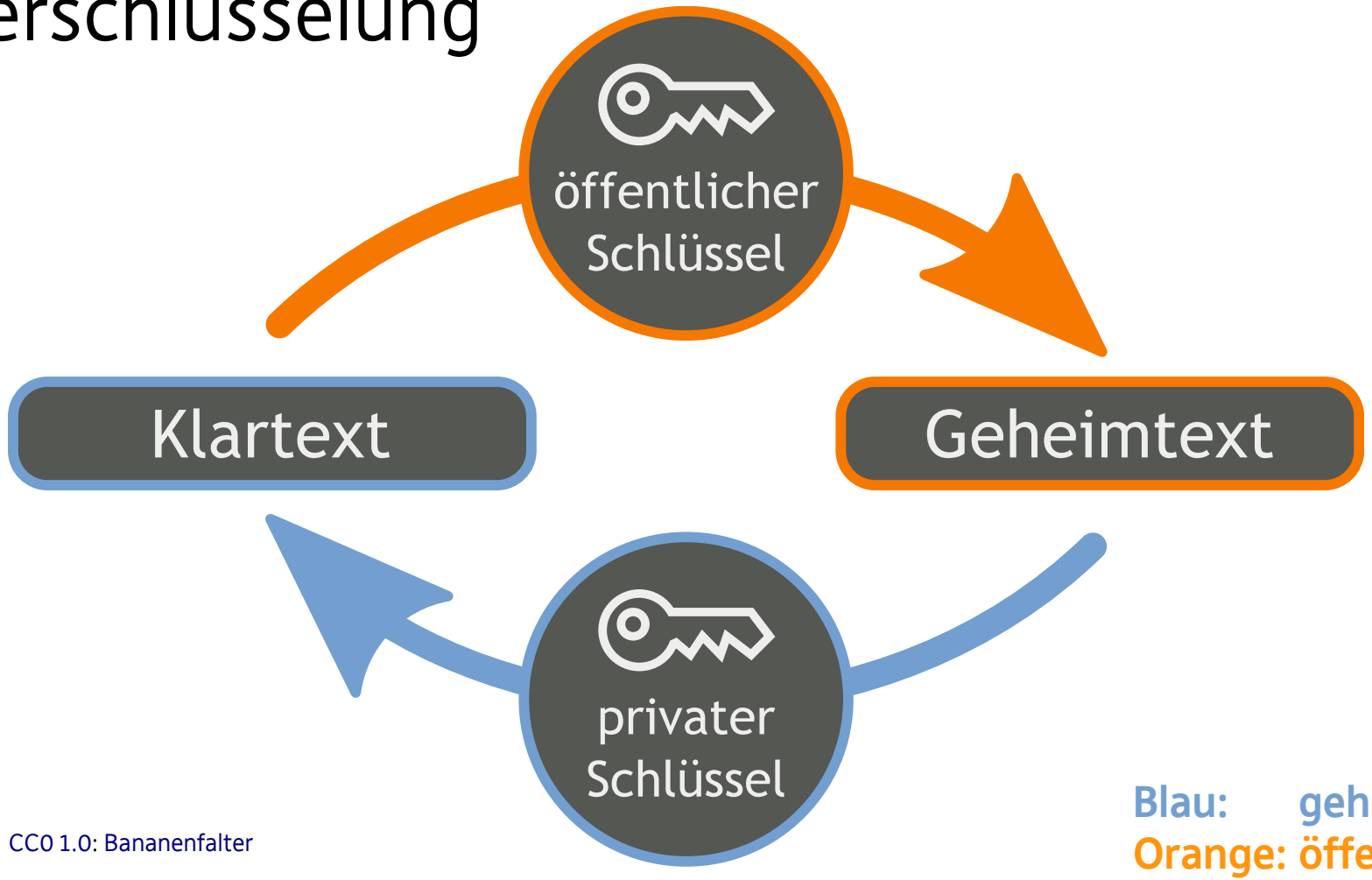
Blau: **geheim**
Orange: **öffentlich**

ASYMMETRISCHE VERSCHLÜSSELUNG

- Öffentlicher Schlüssel (public key)
  - Verschlüsselt Nachrichten
  - Überprüft Signaturen
  - Verfügbar auf Schlüsselservern
- Privater Schlüssel (private key)
  - Entschlüsselt Nachrichten
  - Erzeugt Signaturen
  - Mit Passphrase geschützt und geheim aufbewahrt

ASYMMETRISCHE VERSCHLÜSSELUNG

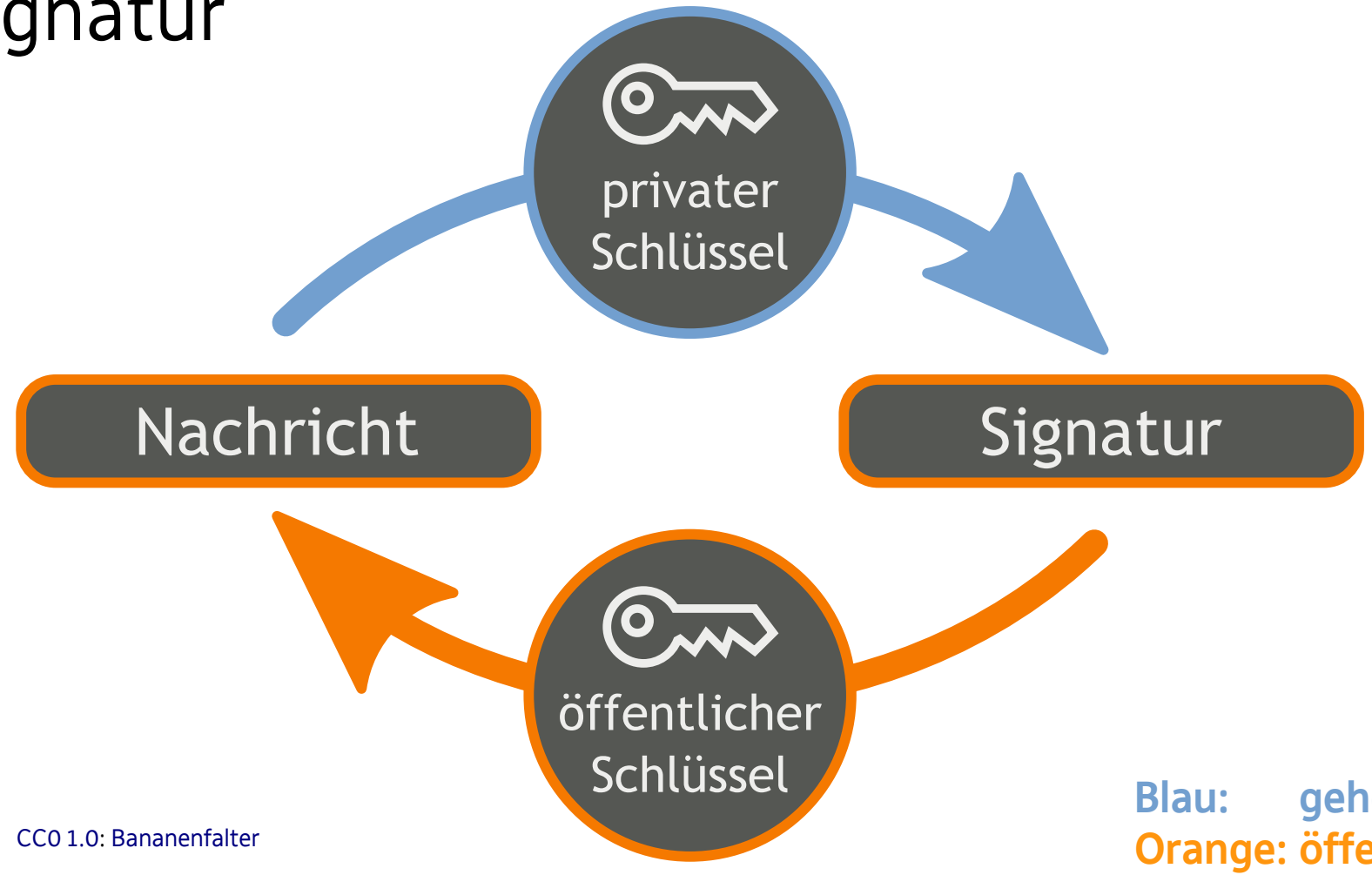
- Verschlüsselung



Blau: geheim
Orange: öffentlich

ASYMMETRISCHE VERSCHLÜSSELUNG

- Signatur



Blau: geheim
Orange: öffentlich

ASYMMETRISCHE VERSCHLÜSSELUNG

- Vorteile
  - Nur privater Schlüssel muss geheim bleiben
  - Öffentlicher Schlüssel kann über unsichere Kanäle übermittelt werden
- Nachteile
  - Ca. um den Faktor 1000 langsamer als symmetrische Verschlüsselungsverfahren
  - Die Nachricht muss für jeden Empfänger separat verschlüsselt werden

ASYMMETRISCHE VERSCHLÜSSELUNG

- Nachteile
  - Sicherheit des Verfahrens beruht auf unbewiesenen Annahmen
  - Man-in-the-Middle-Attacken möglich

ASYMMETRISCHE VERSCHLÜSSELUNG

- Verfahren
  - RSA, Elgamal
- Anwendung
  - World Wide Web (HTTPS mittels SSL/TLS)
  - E-Mail (S/MIME, PGP, GPG)
  - Bitcoin
  - Electronic Banking (HBCI)

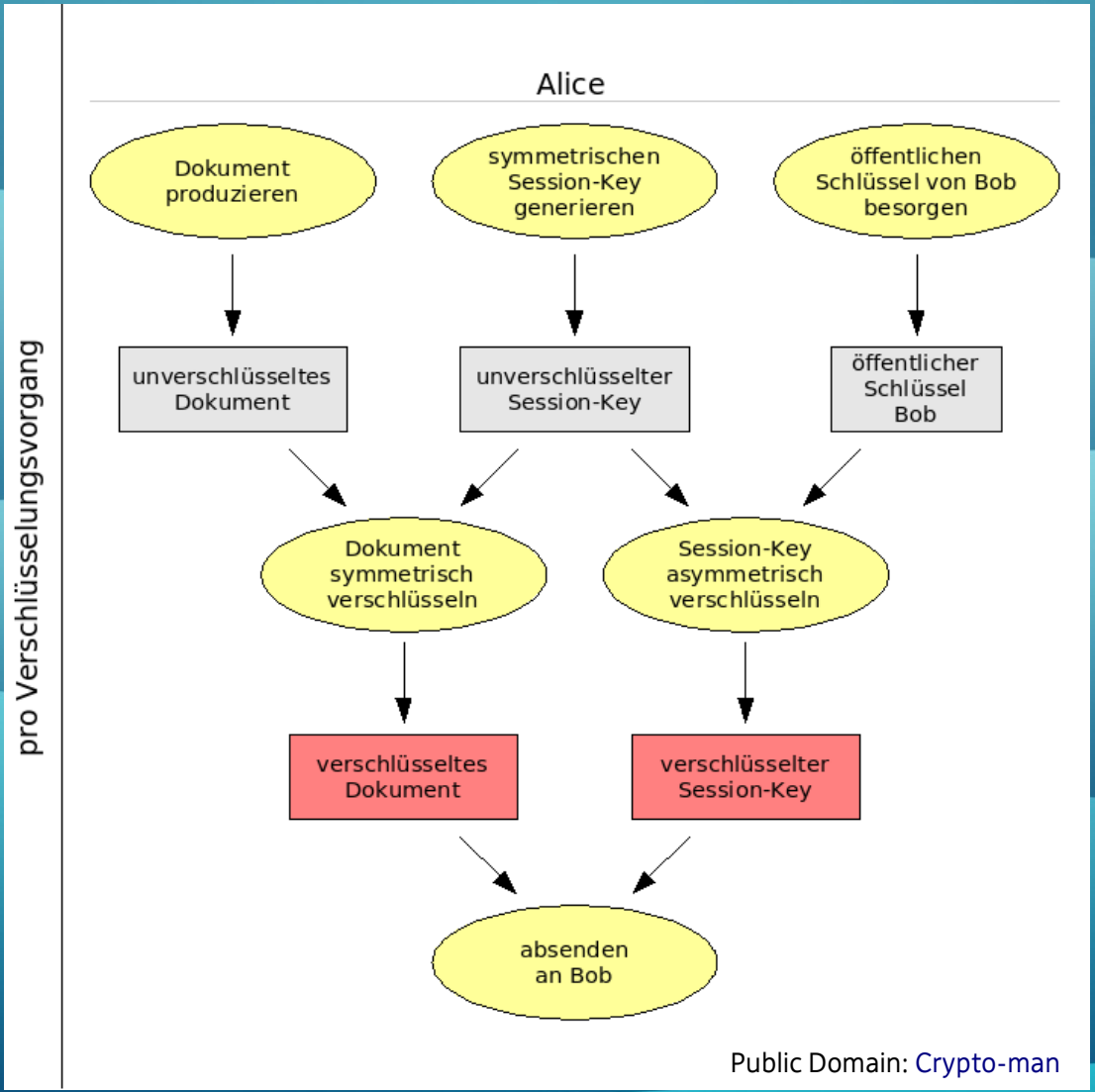
HYBRIDE VERSCHLÜSSELUNG

- Nochmals zur Erinnerung
  - Symmetrische Verschlüsselung ist **schnell**, der Schlüssel muss dem Kommunikationspartner jedoch auf **sicherem** Wege übermittelt werden.
  - Asymmetrische Verschlüsselung erlaubt den Schlüsselaustausch über **unsichere** Wege, ist aber unheimlich **langsam**.

HYBRIDE VERSCHLÜSSELUNG

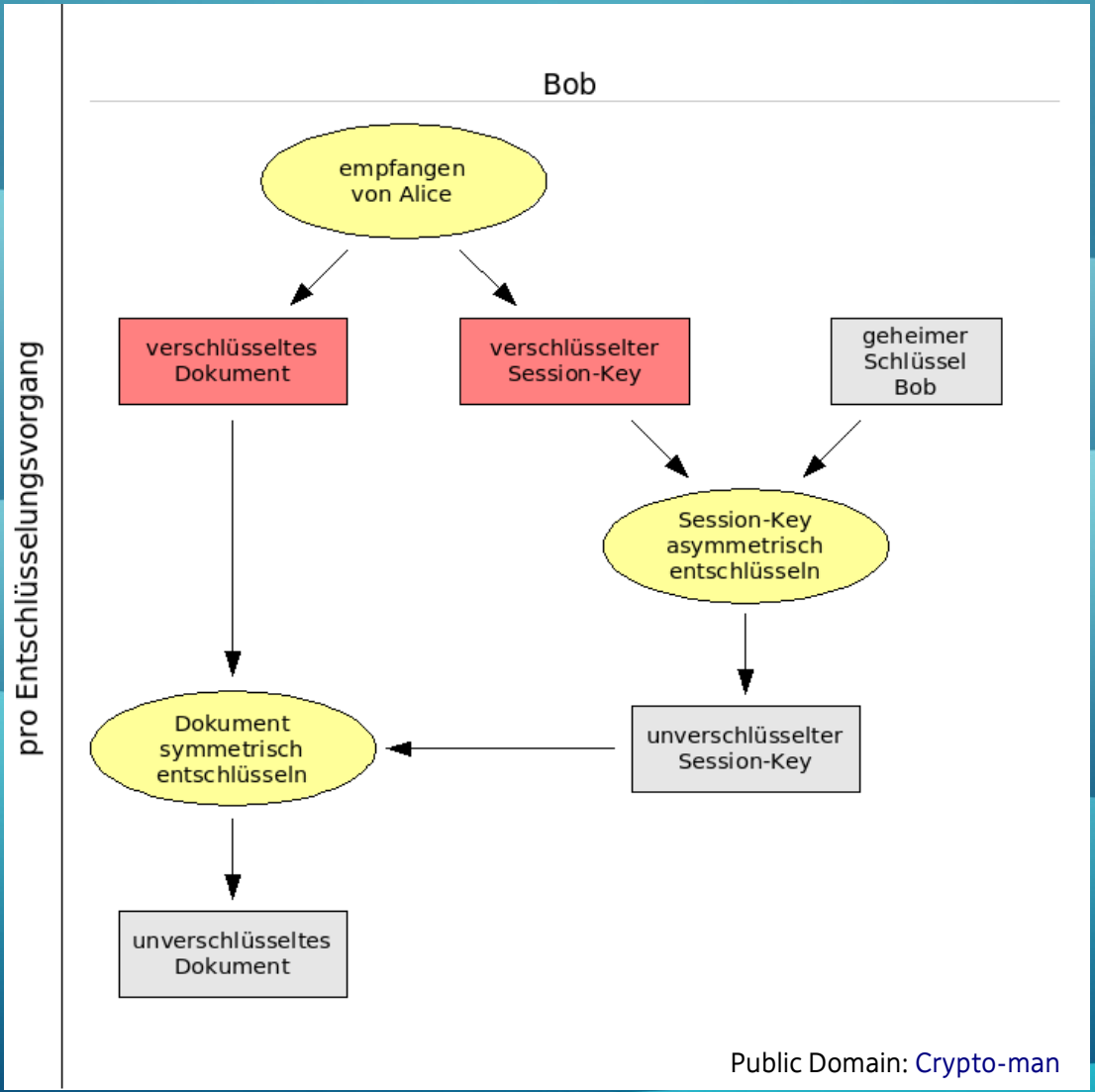
- Lösung
  - Man kombiniert beide Verschlüsselungsverfahren einfach so, dass ihre Vorteile erhalten bleiben
- Vorgehen
  - Man erzeugt einen sym. (Sitzungs-)Schlüssel
  - Dieser wird mittels asym. Verfahren übermittelt (sicher)
  - Die gesamten Nachricht hingegen wird mit dem Sitzungsschlüssel kodiert (schnell)

HYBRIDE VERSCHLÜSSELUNG



Public Domain: Crypto-man

HYBRIDE VERSCHLÜSSELUNG



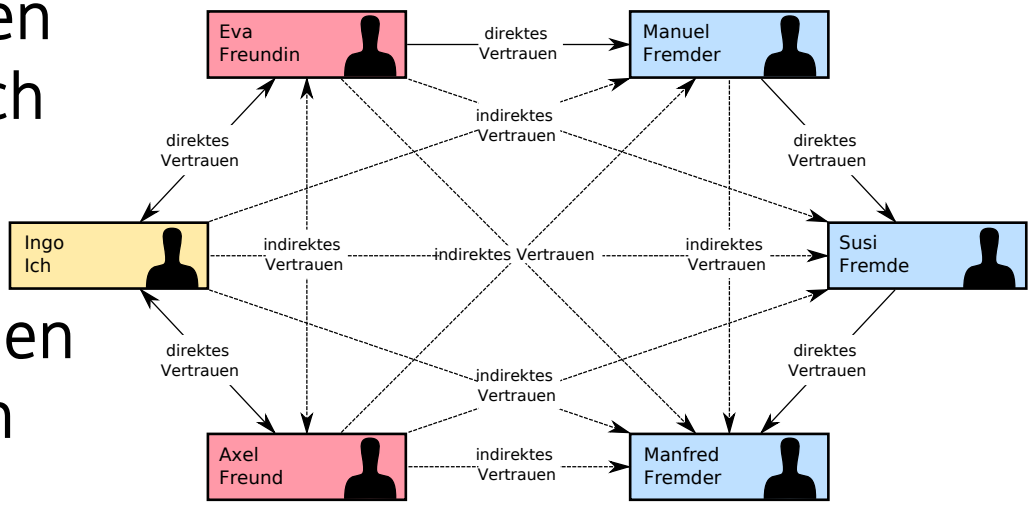
Public Domain: Crypto-man

PGP? OPENPGP? GPG? WTF?

- PGP
  - Pretty Good Privacy
  - 1991 von Phil Zimmermann veröffentlicht
  - Programm zur Verschlüsselung und zum Unterschreiben von Daten
  - PGP verwendet hybride Verschlüsselung
  - Verschlüsselte Kommunikation sollte auch für Bürger*innen und v.a. Bürgerbewegungen zugänglich sein

PGP? OPENPGP? GPG? WTF?

- PGP
  - Web of Trust (Netz des Vertrauens)
    - Keine zentralen Zertifizierungsstellen
    - Echtheit von digitalen Schlüsseln wird durch ein Netz von gegen-seitigen Bestäti-gungen und Vertrauen in die Bestätigungen anderer gesichert
    - Schlüssel werden signiert



PGP? OPENPGP? GPG? WTF?

- PGP
  - Web of Trust (Netz des Vertrauens)
    - Schlüssel sind auf öffentlich zugänglichen Schlüsselservern abgelegt, die sich untereinander regelmäßig synchronisieren
    - Einmal exportierte Schlüssel können nicht mehr gelöscht werden und unterliegen keiner Verbreitungskontrolle
    - Möglichkeit des Schlüsselwiderrufs (key revocation), wodurch der Schlüssel ungültig gemacht werden kann

PGP? OPENPGP? GPG? WTF?

- PGP
  - Web of Trust (Netz des Vertrauens)
    - Durch Keyserver entstehen auch Problematiken:
      - Server können als Quelle für Spam-Versender dienen
      - Preisgabe personenbezogener Daten:
        - Wer hat meinen Schlüssel signiert?
        - Wer gehört zu meinem sozialen Netzwerk?
        - Welche E-Mail-Adressen nutze ich und wie lange schon?
      - Mögliche Verstöße gegen die Informationelle Selbstbestimmung durch missbräuchlich erstellte Schlüssel
      - Keine Kontrolle, welche Signaturen einem Schlüssel hinzugefügt werden

PGP? OPENPGP? GPG? WTF?

- PGP
  - Web of Trust (Netz des Vertrauens)
    - Beispiel eines Web of Trust abseits der Kryptographie: CouchSurfing

  - Aussehen einer verschlüsselten Nachricht
    - Klartext: `http://de.wikipedia.org/wiki/Pretty_Good_Privacy`
    - Chiffrat:

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v2.0.16 (GNU/Linux)

hQEMA1PUVhZb8UnsAQf+KS9PNvkWYFONnoStveMc4KwvGT7WlRFv/ZACvdyFsKDO
icurhL57uh56KCof1m5drfftwjDQWgNyMy0cixqV/2WzeQgjZILE0Z1FDg7cgAbs
UZvy2hmaJf0dhHEUziALotfUMhoSeHeObxmomzb7vovJv5tWDtQ9W+p2tbQ4tiin
LAsJtwQhEVPNltootBteC0dTgOdISe6kfqUSoN3A22SiSUihmjxMPiiO6iZB8gBS
hhfiSPa4khNwODncRe2BjqW+YQHf7L6CfLjx2S1BCSr+KWLmUnVdWSUonhHPF9mI
E/q7t2uoBWg0iQgCjQubgYeqSUYN/xWpqAUX9O71zdKUAbVjjLVT0qTjNLLvms2H
s4BDzHEqKeuGuMAWFzyfuW+VNofTxtcHhzrdjPuYi7sRL3YNUvqUpcGeKGyTApW2
k/fd7U32av7Pq63NoKK2g3RFcyBUiSdNlNhW8TYS1NdMSMXNw1R9dWVgFmsLj2vs
Rv89ufRiPbNLDXcx7CkRrTf13q0miy1850d6k5nt8qUFrnh4xQ==
=z6Xk
-----END PGP MESSAGE-----
```

PGP? OPENPGP? GPG? WTF?

- OpenPGP
  - Standardisiertes Datenform für verschlüsselte und digital signierte Daten
  - Basiert auf PGP 5
  - Entstand 1998 u.a. aus folgenden Gründen:
    - PGP beinhaltete patentierte Algorithmen
    - PGP war kommerziell und proprietär und es bestand der Verdacht, daß eine Hintertür eingebaut sei
    - In den USA gab es ein Exportverbot für Software mit starker Verschlüsselung (ab 40 Bit Schlüssellänge)

PGP? OPENPGP? GPG? WTF?

- OpenPGP
  - Hauptanwendungen sind Signierung und Verschlüsselung von E-Mails
  - Dafür gibt es zwei Formate
    - PGP/INLINE:
      Kompatibilitätsformat für E-Mail-Programme, die OpenPGP von sich aus nicht beherrschen (nur Text)
    - PGP/MIME:
      Technisch saubere Lösung, die auch mit HTML-Mails und Dateianhängen umgehen kann

PGP? OPENPGP? GPG? WTF?

- OpenPGP
  - Nachteile
    - E-Mail-Programme, die OpenPGP nicht unterstützen, zeigen im Zweifelsfall leere Mails mit Dateianhängen an
    - Es wird **nur** der **Inhalt** der E-Mail **verschlüsselt**!
    - Metadaten können weiterhin eingesehen werden
      - Absenderadresse
      - Empfängeradresse
      - Betreff
      - Datum und Uhrzeit
      - ...

PGP? OPENPGP? GPG? WTF?

- GnuPGP (GPG)
  - GNU Privacy Guard
  - Freies Kryptographiesystem zum Ver- und Entschlüsseln von Daten sowie zum Erzeugen und Prüfen elektronischer Signaturen
  - Implementiert den OpenPGP-Standard
  - Wurde als Ersatz für PGP entwickelt und enthält patentfreie Algorithmen

PGP? OPENPGP? GPG? WTF?

- GnuPGP (GPG)
  - Hauptanwendungen
    - Signierung und Verschlüsselung von E-Mails
    - Sicherung der Integrität der verteilten Softwarepakete bei den meisten GNU/Linux-Distributionen
  - Auf vielen Plattformen verfügbar
    - GNU/Linux
    - Mac OS X (und andere unixoide Systeme
    - Windows
    - Teilweise auch auf mobilen Systemen (z.B. Android)

KEYSIGNING-PARTYS

- Veranstaltung, durch die das Web of Trust aufgebaut wird
- Benutzer von PGP und ähnlichen Diensten treffen sich, um gegenseitig öffentliche Schlüssel zu signieren
- Identifikation einer Person geschieht hierbei in der Regel durch amtliche Dokumente (Personalausweis, Reisepass oder Führerschein)

KEYSIGNING-PARTYS

- Aus Sicherheitsgründen werden die Schlüssel meist nicht vor Ort signiert
  - kein „sauberer“ Rechner vor Ort
  - Mitlesen von Passphrasen durch „Über-die-Schulter-Schauen“
- Weit verbreitet sind Keysigning-Partys bei Universitäten, IT-Messen- und Veranstaltungen, dem CCC und den Piraten ;)

DIE BENÖTIGTEN WERKZEUGE

- Mozilla Thunderbird
  - Freies Open-Source-E-Mail-Programm
- GnuPG
  - Freie Implementierung des OpenPGP-Standards
  - GNU/Linux: In der Regel bereits installiert
  - Mac OS X: GPGTools
  - Windows: Gpg4win

DIE BENÖTIGTEN WERKZEUGE

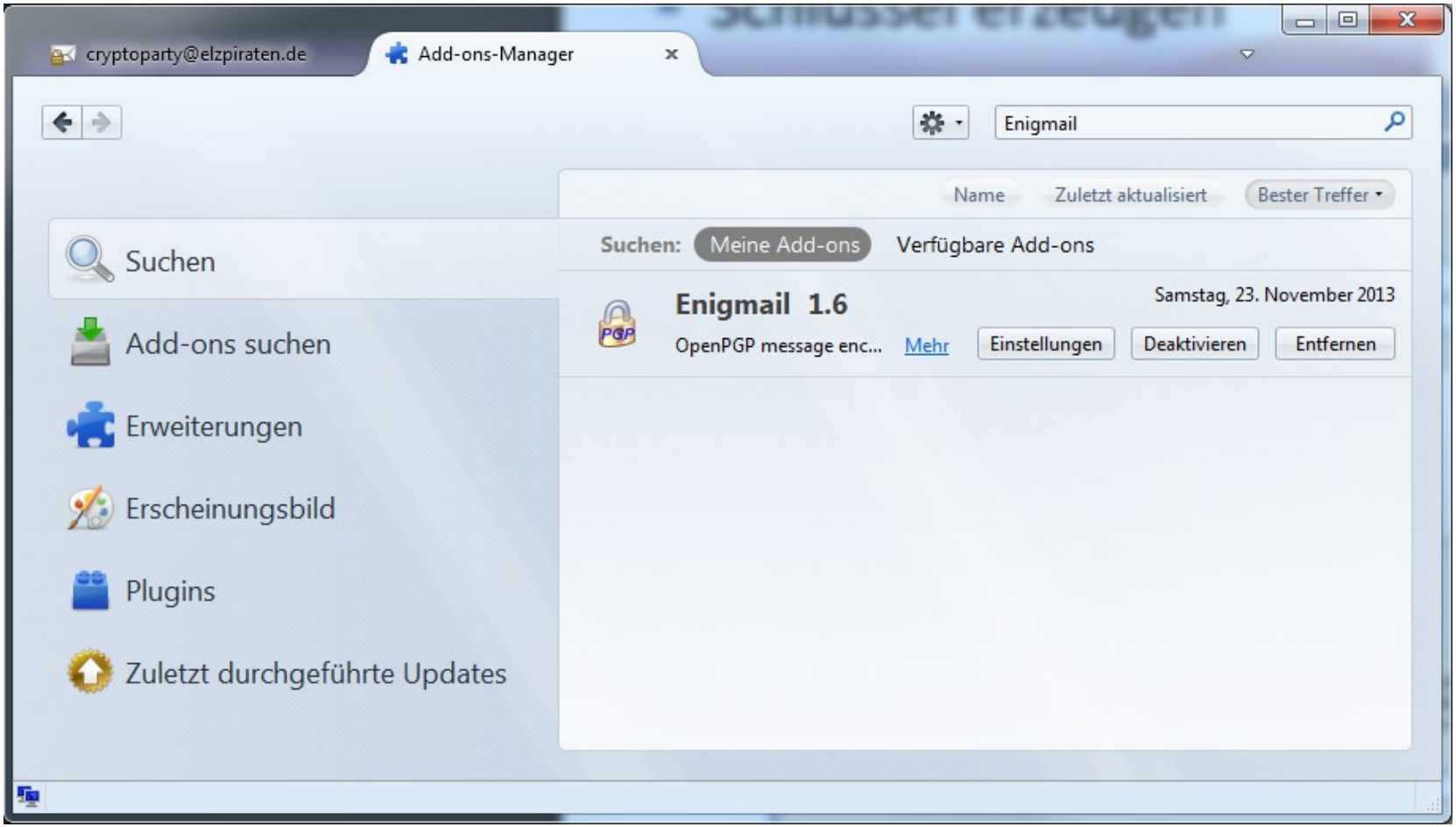
- Thunderbird-Add-on Enigmail
  - Erweitert Thunderbird um Nachrichtenverschlüsselung und -authentifizierung
  - Als Voraussetzung dient GnuPG
  - GNU/Linux-Benutzer sollten das Add-on aus ihrer Paketverwaltung installieren

BEDIENUNG IN DER PRAXIS

- Installation
  - Thunderbird läßt sich analog zu herkömmlicher Software ziemlich einfach und schnell installieren
  - Anschließend ein E-Mail-Konto anlegen
  - Enigmail über Thunderbirds Add-ons-Manager (Windows) oder über das Paketmanagement (GNU/Linux) installieren

BEDIENUNG IN DER PRAXIS

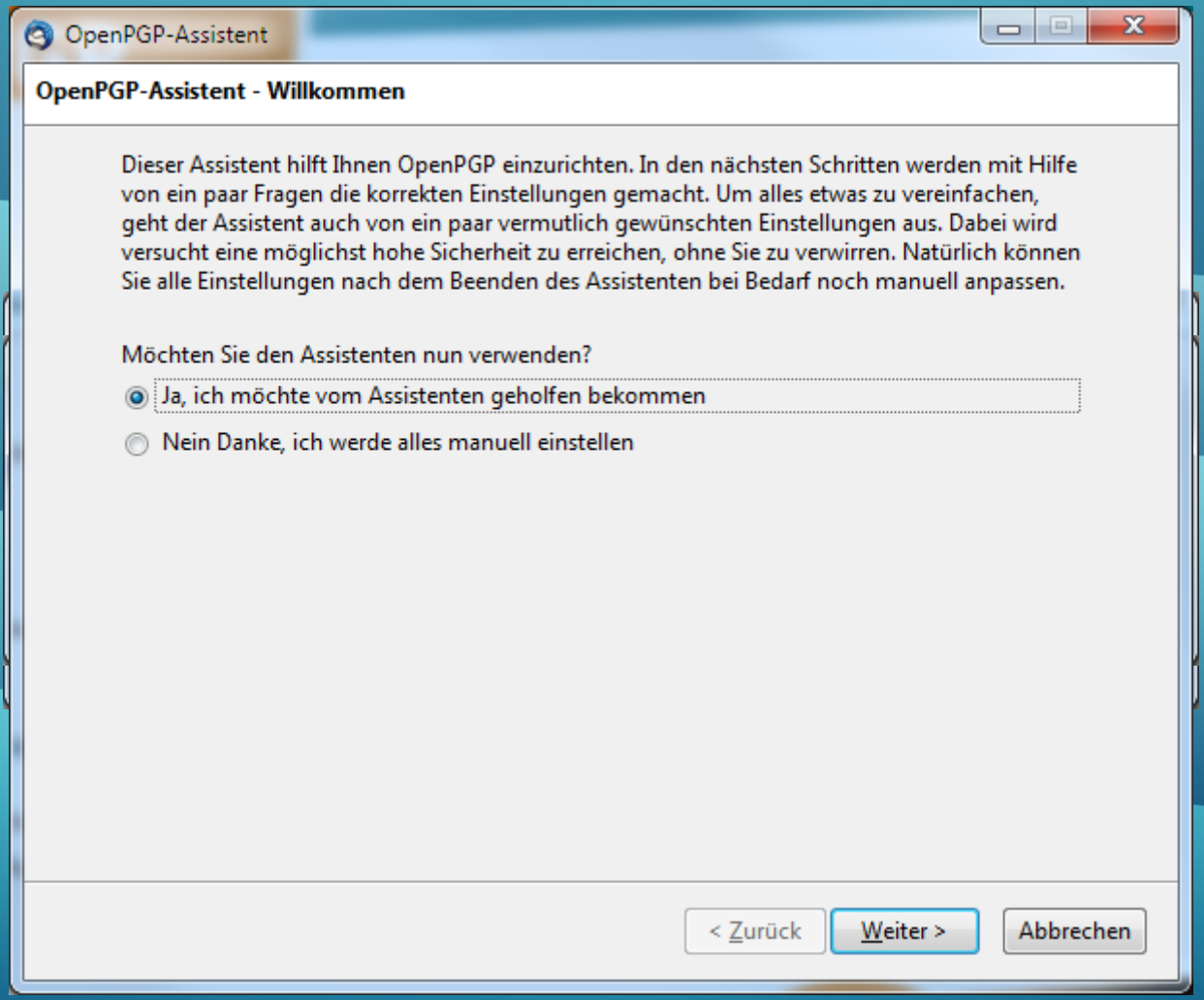
- Installation



BEDIENUNG IN DER PRAXIS

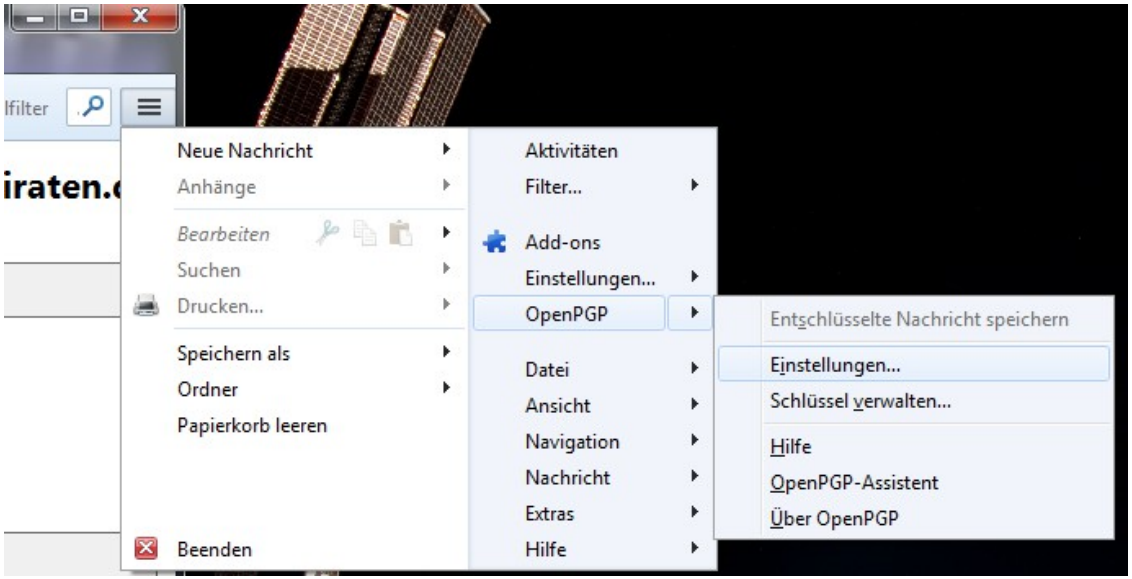
- Enigmail führt nach der Installation mit einem OpenPGP-Assistenten durch die Konfiguration
- Findet er kein GnuPG, kann es heruntergeladen und installiert werden (Windows)
- Danach wird ein Schlüsselpaar erzeugt oder importiert
- Zuletzt kann (und sollte) man sich ein Widerrufszertifikat generieren lassen

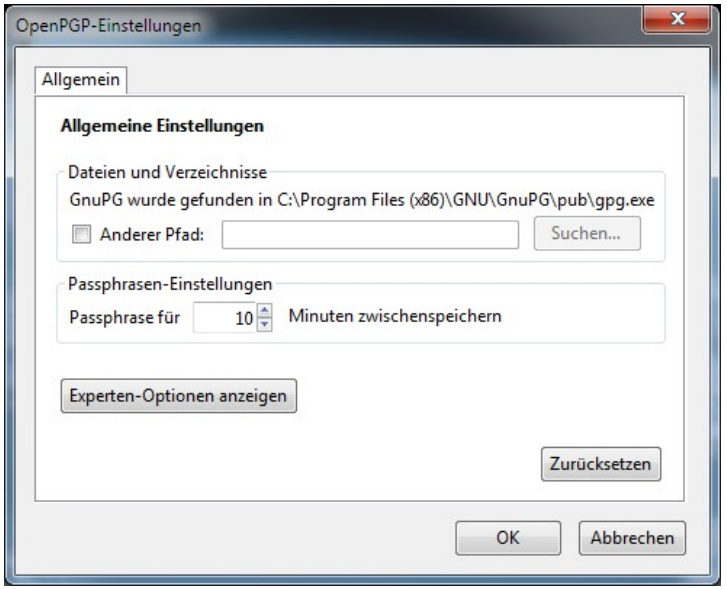
BEDIENUNG IN DER PRAXIS



BEDIENUNG IN DER PRAXIS

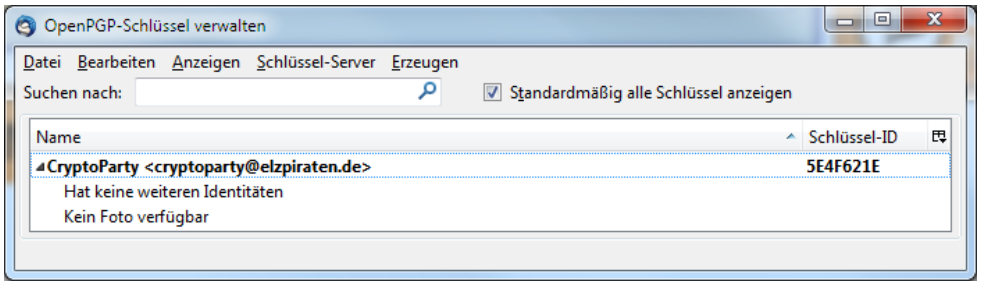
- Spätere Änderungen an der Konfiguration können über den Menüpunkt „OpenPGP“ → „Einstellungen…“ durchgeführt werden





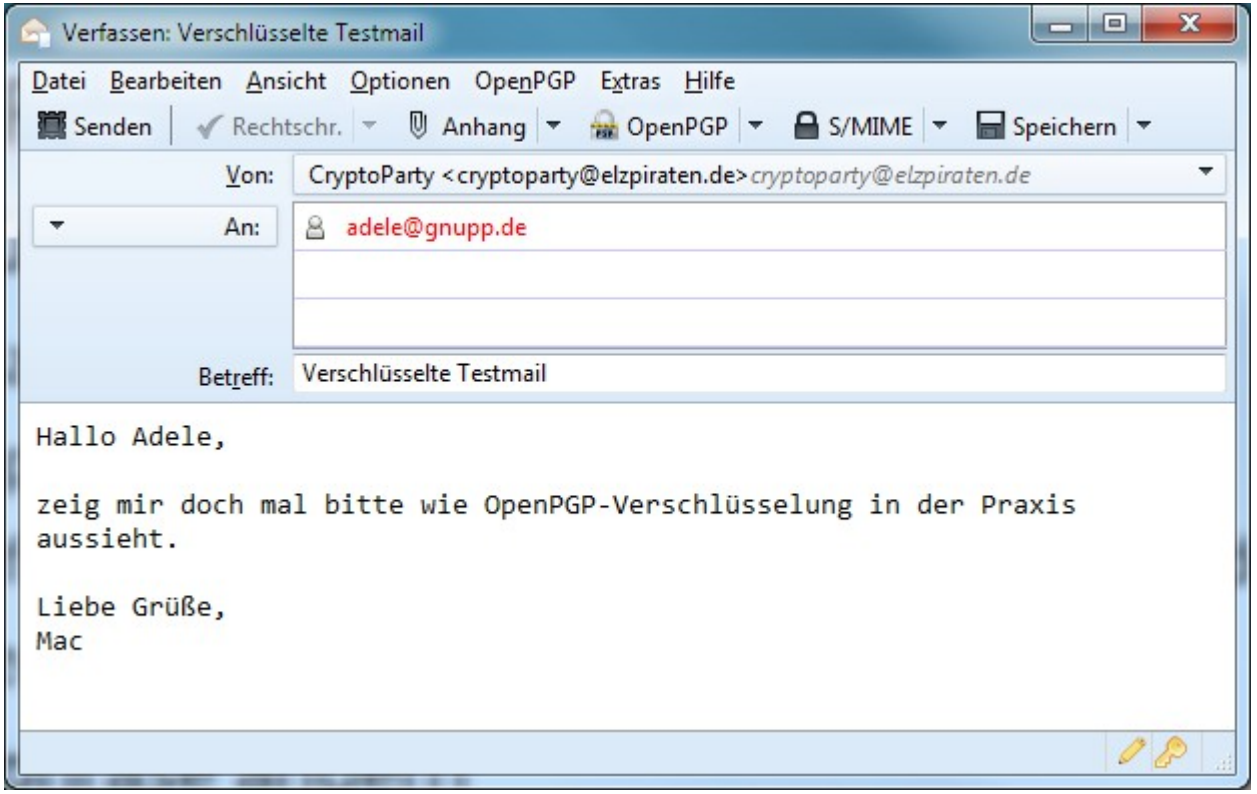
BEDIENUNG IN DER PRAXIS

- „OpenPGP“ → „Schlüssel verwalten…“
  - Schlüssel
    - anzeigen lassen
    - importieren/exportieren/per Mail versenden
    - auf Schlüsselservern suchen oder dort hochladen
    - erzeugen
  - Passphrase ändern
  - Ablaufdatum ändern
  - …



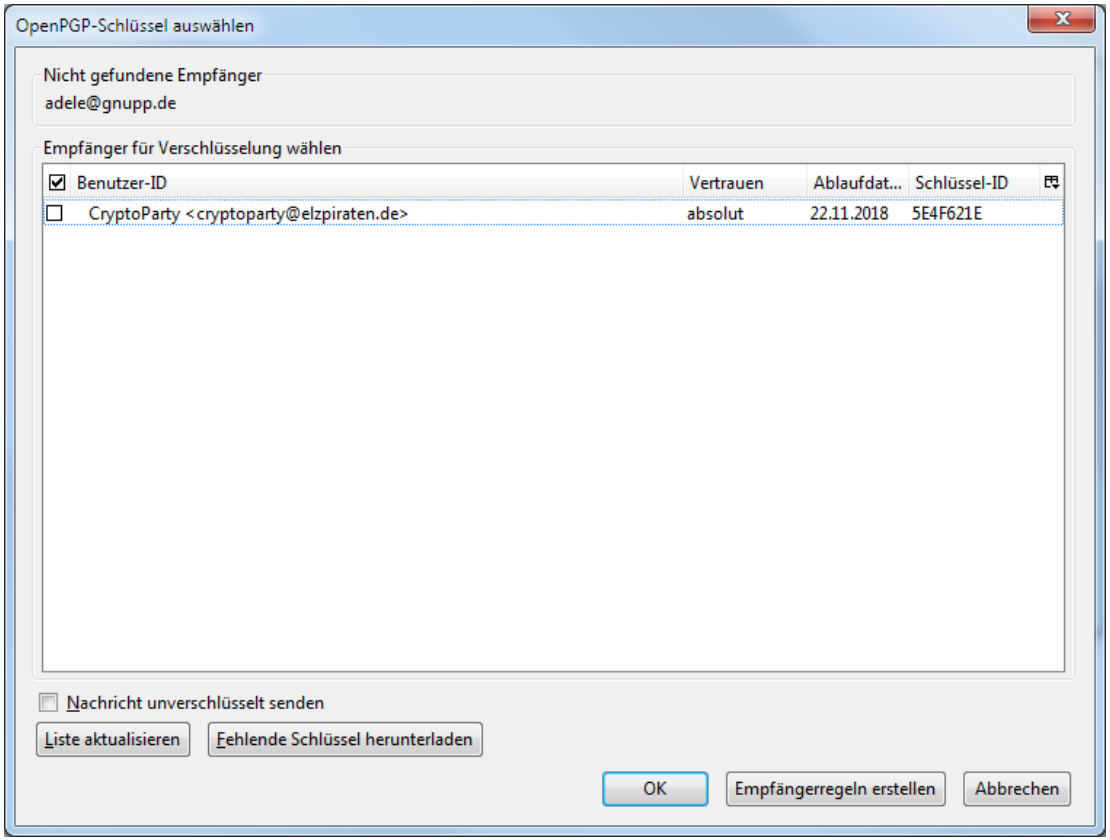
BEDIENUNG IN DER PRAXIS

- Beispiel: E-Mail an neuen Kontakt



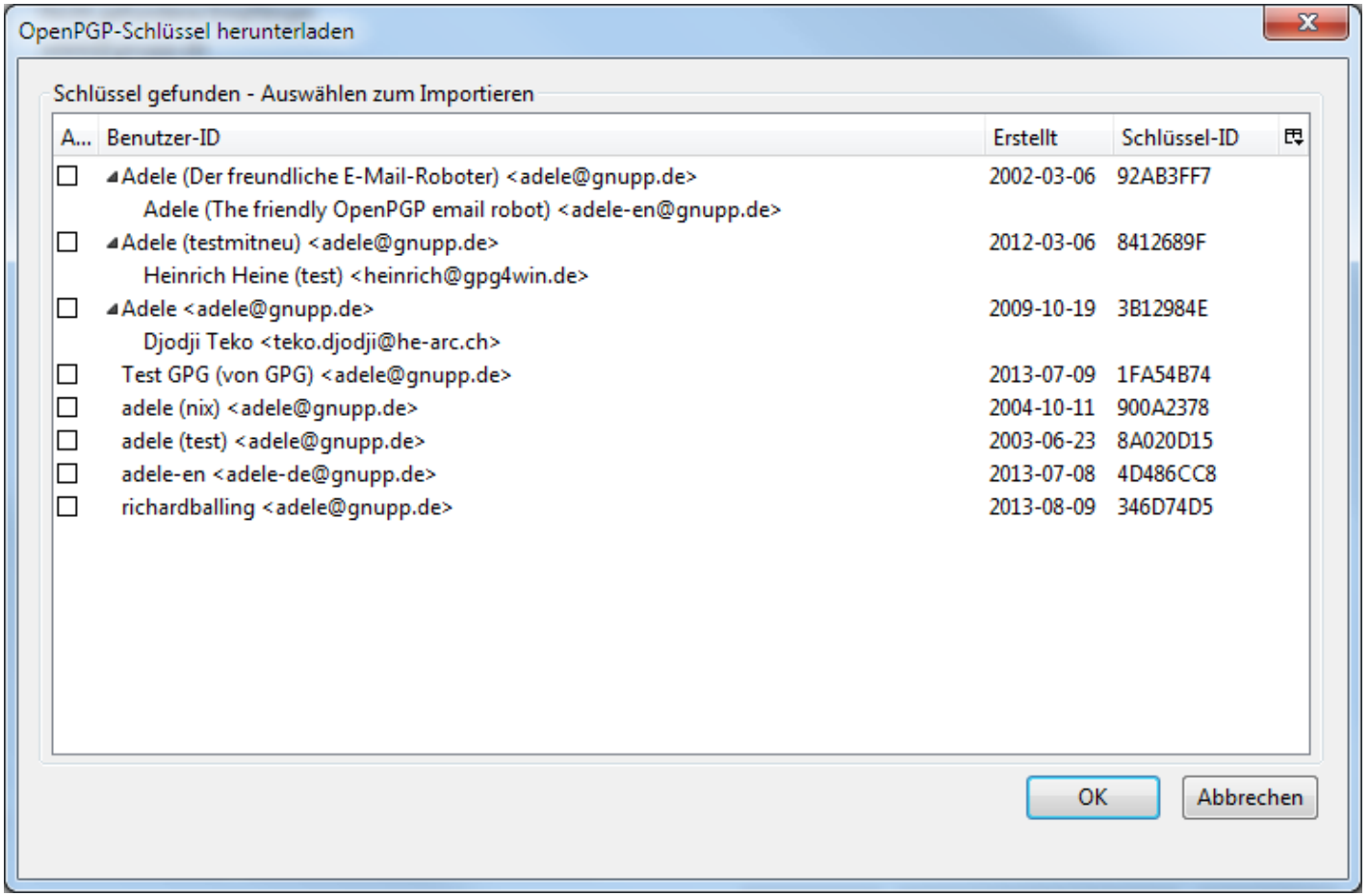
BEDIENUNG IN DER PRAXIS

- Noch fehlt der öffentliche Schlüssel des Empfängers in der Schlüsselverwaltung



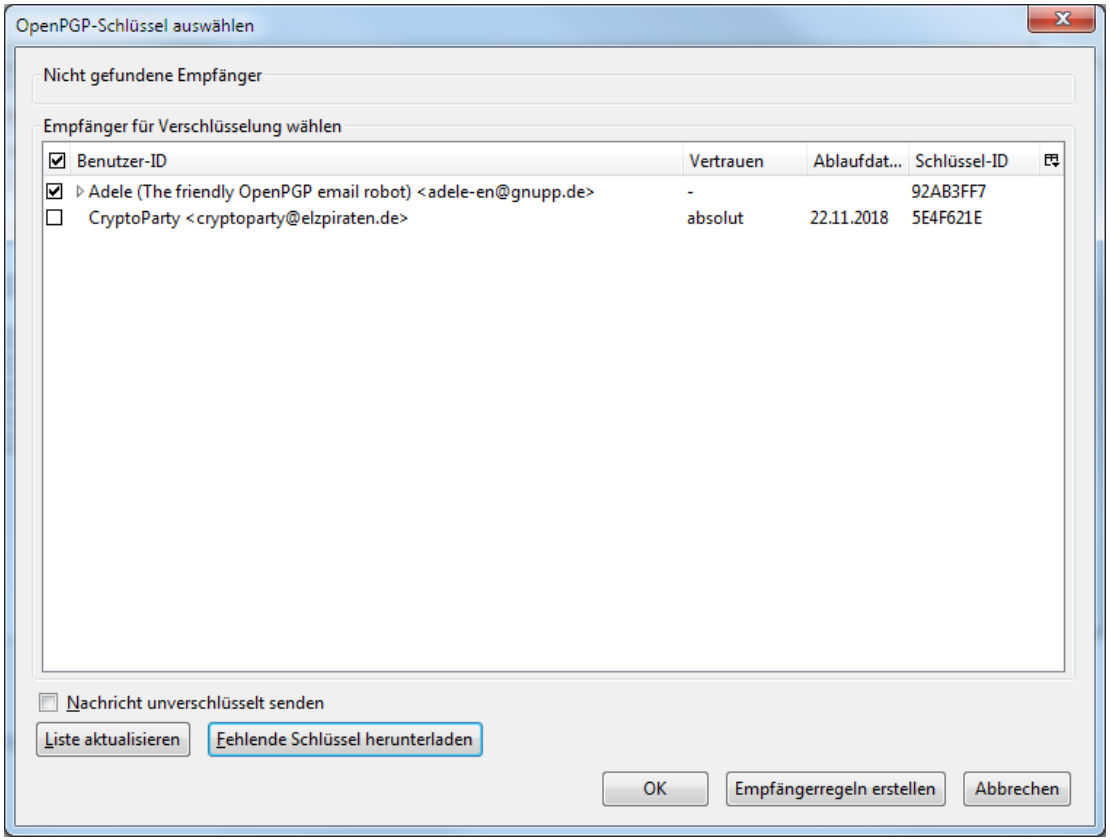
BEDIENUNG IN DER PRAXIS

- Auf einem Schlüsselserver wird man fündig



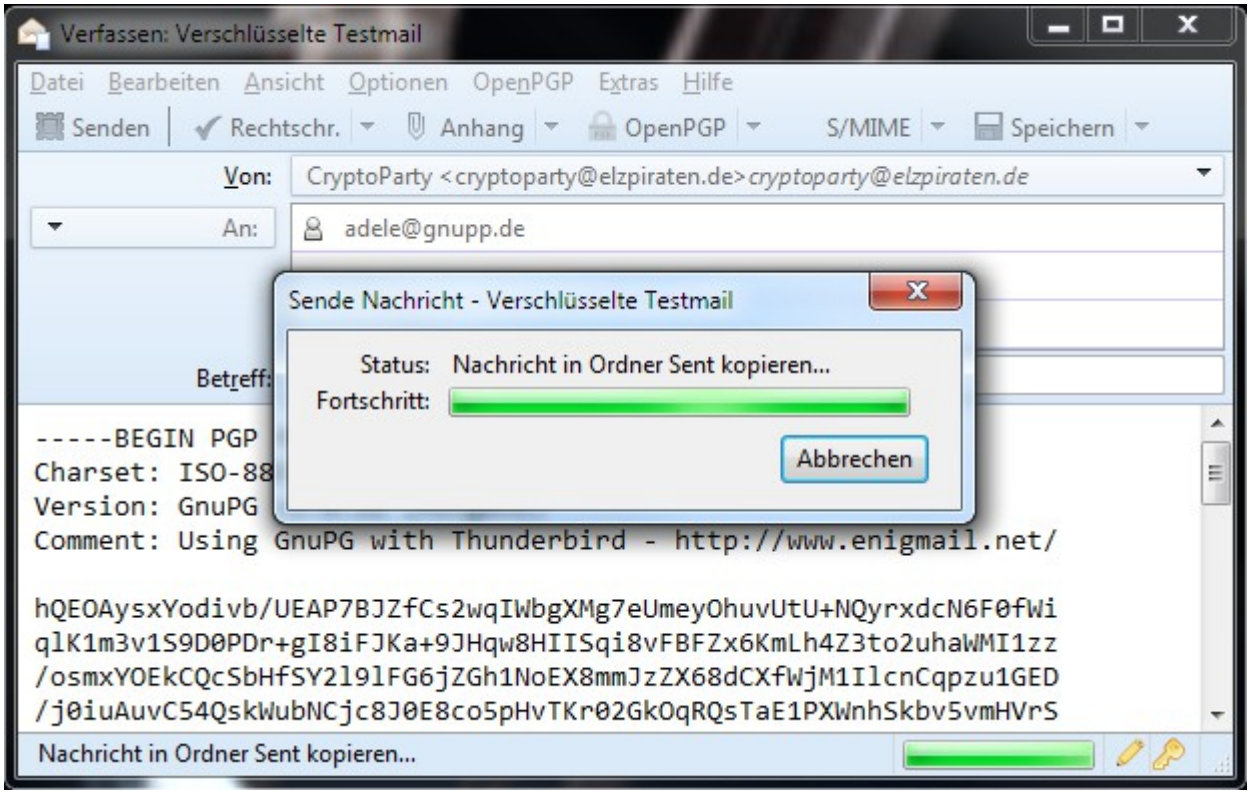
BEDIENUNG IN DER PRAXIS

- Nach dem Import liegt der Schlüssel auf dem eigenen System und kann ausgewählt werden



BEDIENUNG IN DER PRAXIS

- Nun kann eine verschlüsselte Nachricht an den Empfänger verschickt werden



WAS NOCH ZU BEACHTEN WÄRE

- Sicherheit der Kommunikation kann unterminiert werden.
  - Kompromittierung der eingesetzten Systeme durch bspw. Trojaner oder Hintertüren in (proprietären) Betriebssystemen
  - Fortschritte in der Kryptoanalyse
- Betreff und weitere Metadaten werden unverschlüsselt übertragen.

WAS NOCH ZU BEACHTEN WÄRE

- Auswertung und Speicherung der Metadaten möglich. (Wer? Wann? Mit wem? Wie häufig?)
- Schlüsselserver werden ausgewertet.
- Verschlüsselte Kommunikation ist als solche erkennbar und kann verdächtig sein.
- Am 18.10.07 hat der Bundesgerichtshof jedoch in seinem Urteil Az.: StB 34/07 eindeutig festgestellt, dass Verschlüsselung als Tatverdacht nicht ausreichend ist.

WAS NOCH ZU BEACHTEN WÄRE

- In manchen Ländern ist der Einsatz von Verschlüsselung illegal oder man kann zur Herausgabe der Schlüssel gezwungen werden (z.B. Großbritannien).
- Eine vollständig anonyme Kommunikation ist praktisch nicht machbar.
- Fällt der private Schlüssel in fremde Hände, kann die gesamte vergangene Kommunikation entschlüsselt werden.

WAS NOCH ZU BEACHTEN WÄRE

- E-Mail-Programme können im Hintergrund Entwürfe einer aktuell bearbeiteten Mail speichern. Wurde vergessen zuvor die Verschlüsselung zu aktivieren, kann der Klartext der Mail im Falle von IMAP auf einen Server des Mail-Anbieters gelangen! Darum am besten automatisches Speichern abstellen.
- Ein Blick auf OpenPGP Best Practices schadet nicht.

FAZIT

- Die Ende-zu-Ende-Verschlüsselung bzw. die damit verbundenen Verfahren, die hinter OpenPGP stecken, sind derzeit noch sicher.
- Wie gesehen lauern im Bezug auf OpenPGP allerdings auch einige Fallstricke.
- Im Schatten der Snowden-Veröffentlichungen brüten derzeit viele Hacker und Kryptoexperten über neue Möglichkeiten der sicheren und anonymen Kommunikation.

DISCLAIMER

- Dieser Vortrag enthält Vereinfachungen.
- Er ist nach bestem Wissen und Gewissen erstellt, kann aber Fehler enthalten und erhebt deshalb keinen allgemeinen Wahrheitsanspruch.
- Fragt und forscht im Zweifelsfall selbst nach. Die Verantwortung liegt bei Euch.

FRAGEN?

QUELLEN

- Asymmetrisches Kryptosystem
- Einwegfunktion
- Enigmail (OpenPGP-Add-on für Thunderbird, benötigt GnuPG, z.B. in Gpg4win enthalten)
- GNU Privacy Guard (GPG)
- GnuGP (GNU Privacy Guard – freie Implementierung des OpenPGP-Standards)
- Gpg4win (GNU Privacy Guard für Windows)
- GPGTools (GNU Privacy Guard für Mac OS X)
- Hybride Verschlüsselung
- Keysigning-Party
- Kryptoparty.de (CryptoParty-Plattform der Piratenpartei)
- Mozilla Thunderbird (weit verbreitetes Open-Source-E-Mail-Programm)
- One-Time-Pad

QUELLEN

- OpenPGP
- OpenPGP Best Practices
- Pretty Good Privacy (PGP)
- Schlüsselserver
- Symmetrisches Kryptosystem
- Thunderbird Mail DE - Enigmail OpenPGP (gute Enigmail-Dokumentation)
- Vortrag „PRISM BREAK“ von André Martens (Piraten Freiburg) anläßlich einer CryptoParty
- Web of Trust