Einführung in PGP/GPG Mailverschlüsselung

von Olaf Pichler
mit Inhalten von Patrick Strasser

Olaf.P@gmx.at
Schlüssel-ID: 0xCAB623BD
Fingerprint:
CAAF 5E4E E0D3 A122 0FC1 568F 995D
1164 CAB6 23BD

11.2.2014

Wer ist da?

- Vortragende
- Teilnehmer
- HelferInnen

Regeln

- bei Unklarheiten gleich fragen
- Neueinsteiger bestimmen das Tempo
- helft wo Ihr könnt, niemand ist perfekt
- Don't Panic! Wir haben keinen Stress!

Übersicht

- Ziele
- Arten der Verschlüsselung
- Funktion der asymmetrischen Verschlüsselung
- Angriffe auf die Verschlüsselung
- PGP/GPG Emailverschlüsselung
- Praxis: Enigmail und mehr

Ziele

Signatur

- Nachricht stammt sicher vom Sender
- Nachricht wurde nicht verändert

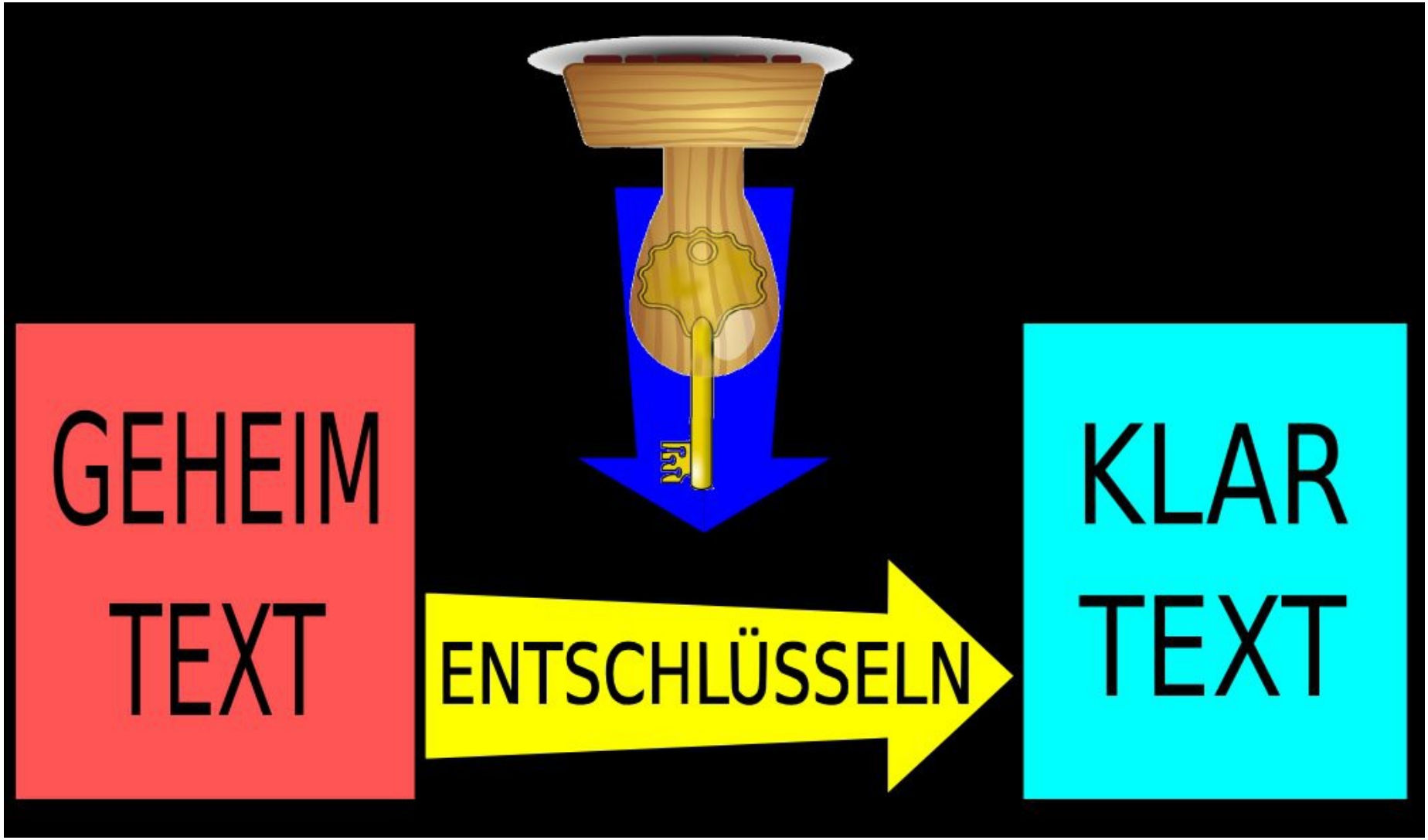
Verschlüsselung

- Briefgeheimnis
- Kuvert für Emails
- Vertrauliche Informationen

Arten der Verschlüsselung

PUBLIC PRIVAT

Funktion der asymmetrischen Verschlüsselung

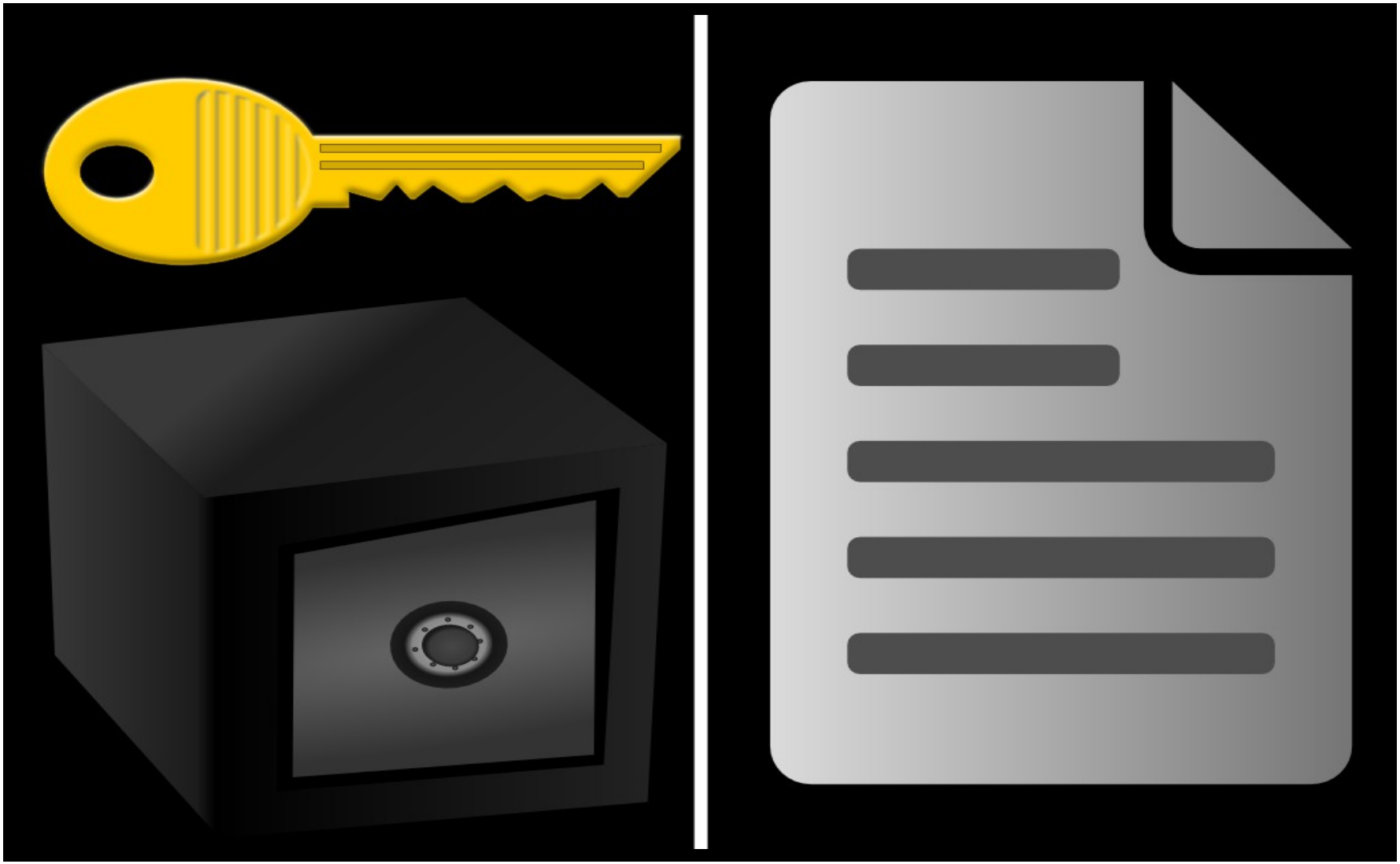


Angriffe auf die Verschlüsselung

- Ihr privater Schlüssel fällt in fremde Hände
- jemand verfälscht öffentliche Schlüssel
- Sie löschen Ihre Dateien nicht gründlich
- Viren und Trojanische Pferde
- unbefugter Zugriff auf Ihren Rechner
- elektromagnetische und akustische Abstrahlungen
- Übergriffe auf Multi-User-Systemen
- Überwachung Ihres Datenverkehrs
- Kryptanalyse

Quelle: PGP-Handbuch
www.foebud.org/fruehere-projekte/pgp/pgp-Buch.pdf

PGP/GPG



Praxis: Enigmail und mehr

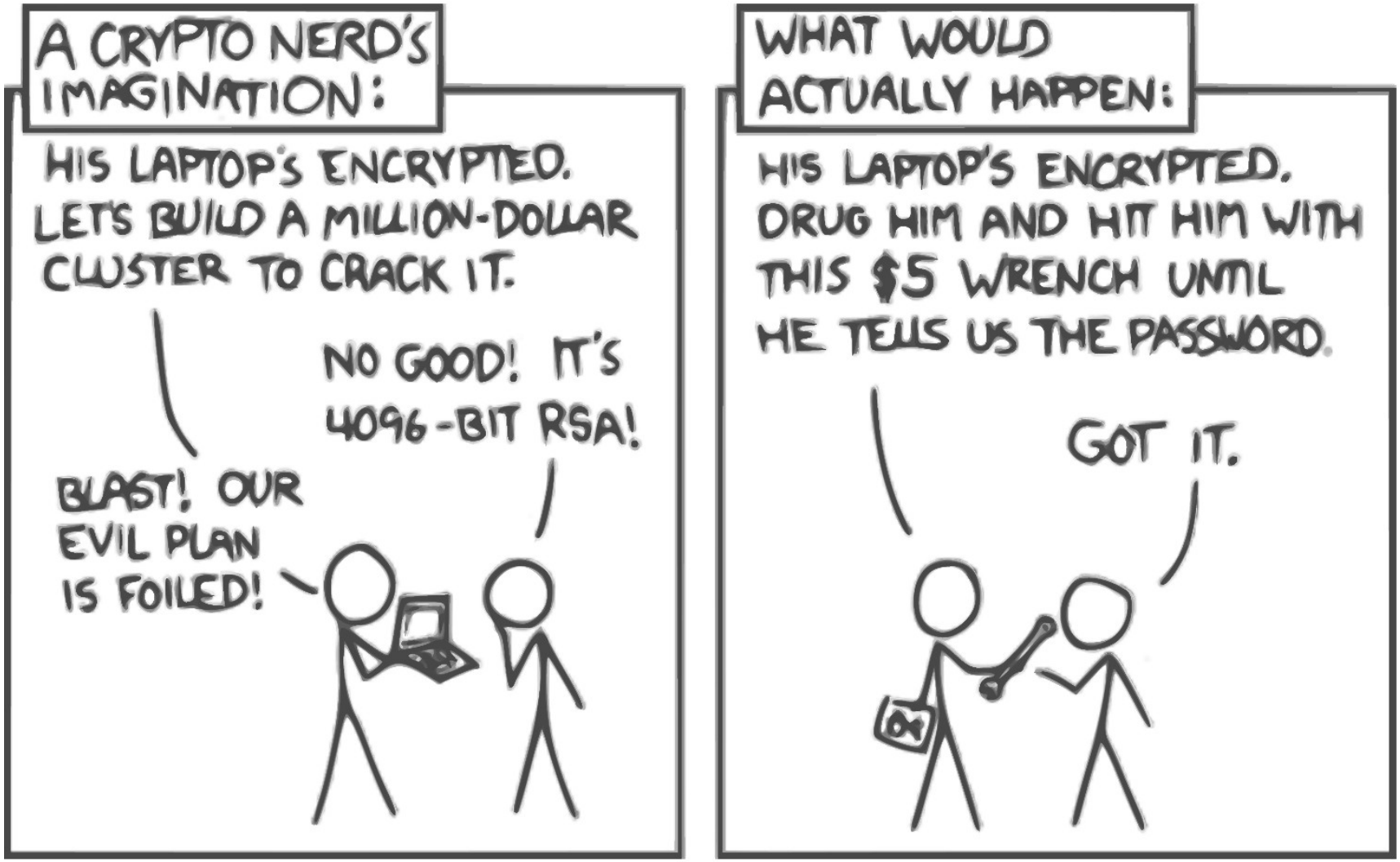
In der Praxis möchte man GPG komfortabel nutzen:

- Thunderbird: Enigmail ist ein GPG Plugin
- Outlook: GPG4win + GPG4o
- Mac: GPGtools

Empfehlung

- Emails mit GPG verschlüsseln
- **Private-Key verschlüsselt speichern**
- starke Schlüssel verwenden (min. 4096bit)
- Schlüssel regelmäßig erneuern (6-12 Monate)
- das Web of Trust nutzen
- Programme verwenden die GPG/MIME unterstützen
- an Crypto-Parties teilnehmen

Danke für Ihre Aufmerksamkeit und Paranoia.



Quelle: https://xkcd.com/538/