Einführung in PGP/GPG
Mailverschlüsselung

Vorweg

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

- Diese Präsentation kann in Teilen oder als Ganzen von Jedermann bearbeitet, veröffentlicht und kopiert werden.

Ziele und Motivation

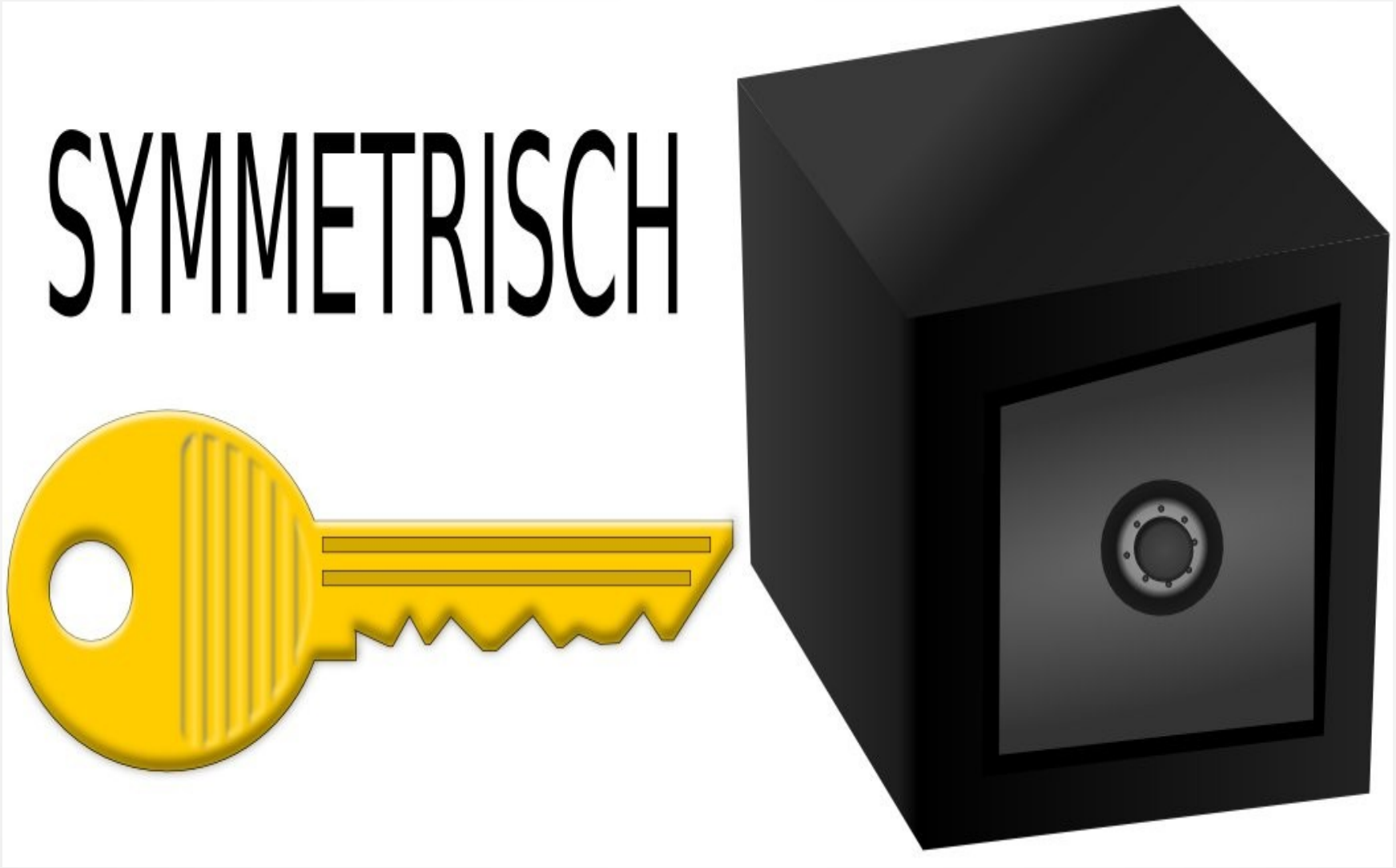
Signatur

- Nachricht stammt sicher vom Sender
- Nachricht wurde nicht verändert

Verschlüsselung

- Briefgeheimnis
- Kuvert für E-Mails
- Vertrauliche Informationen

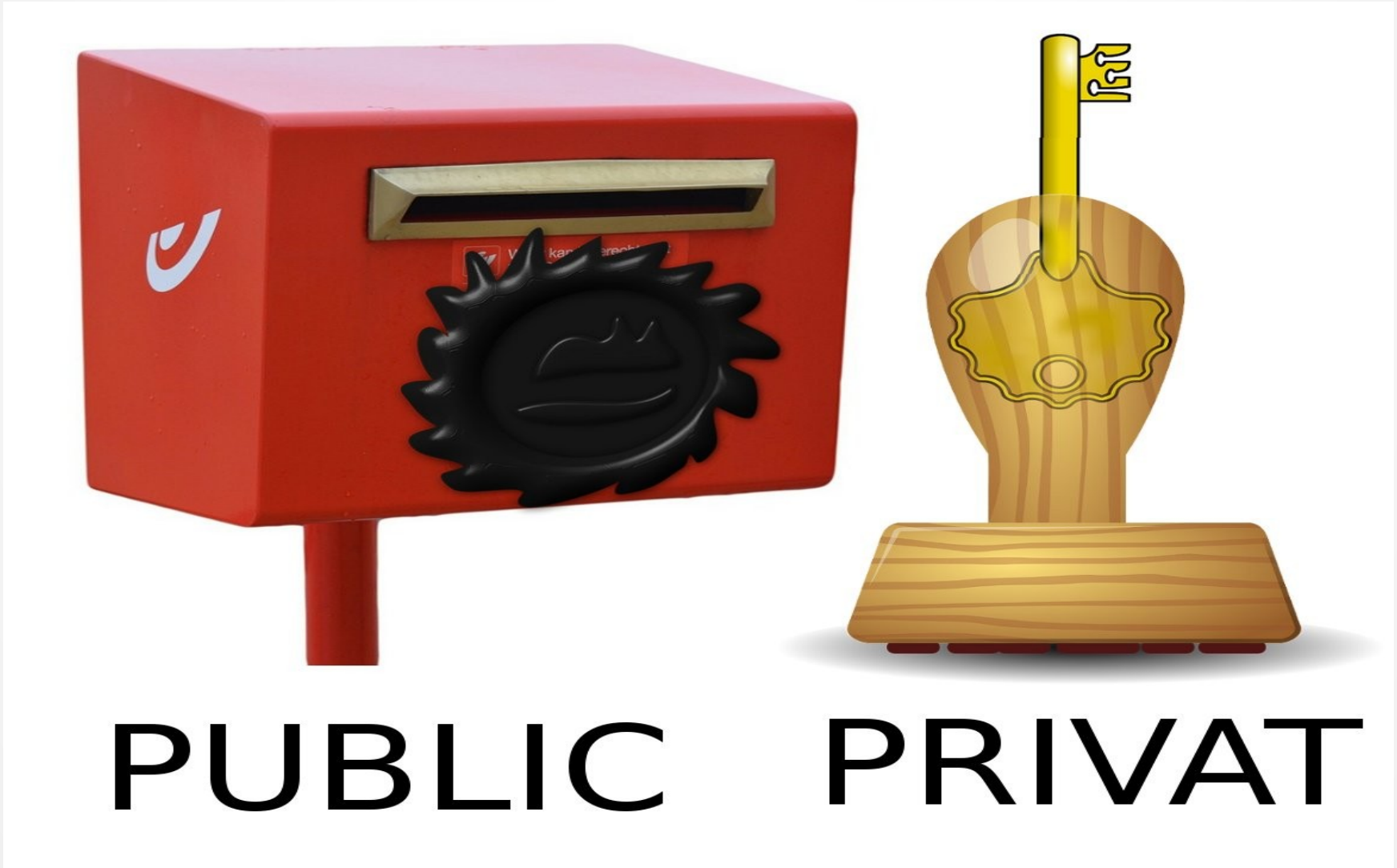
Symmetrische Verschlüsselung



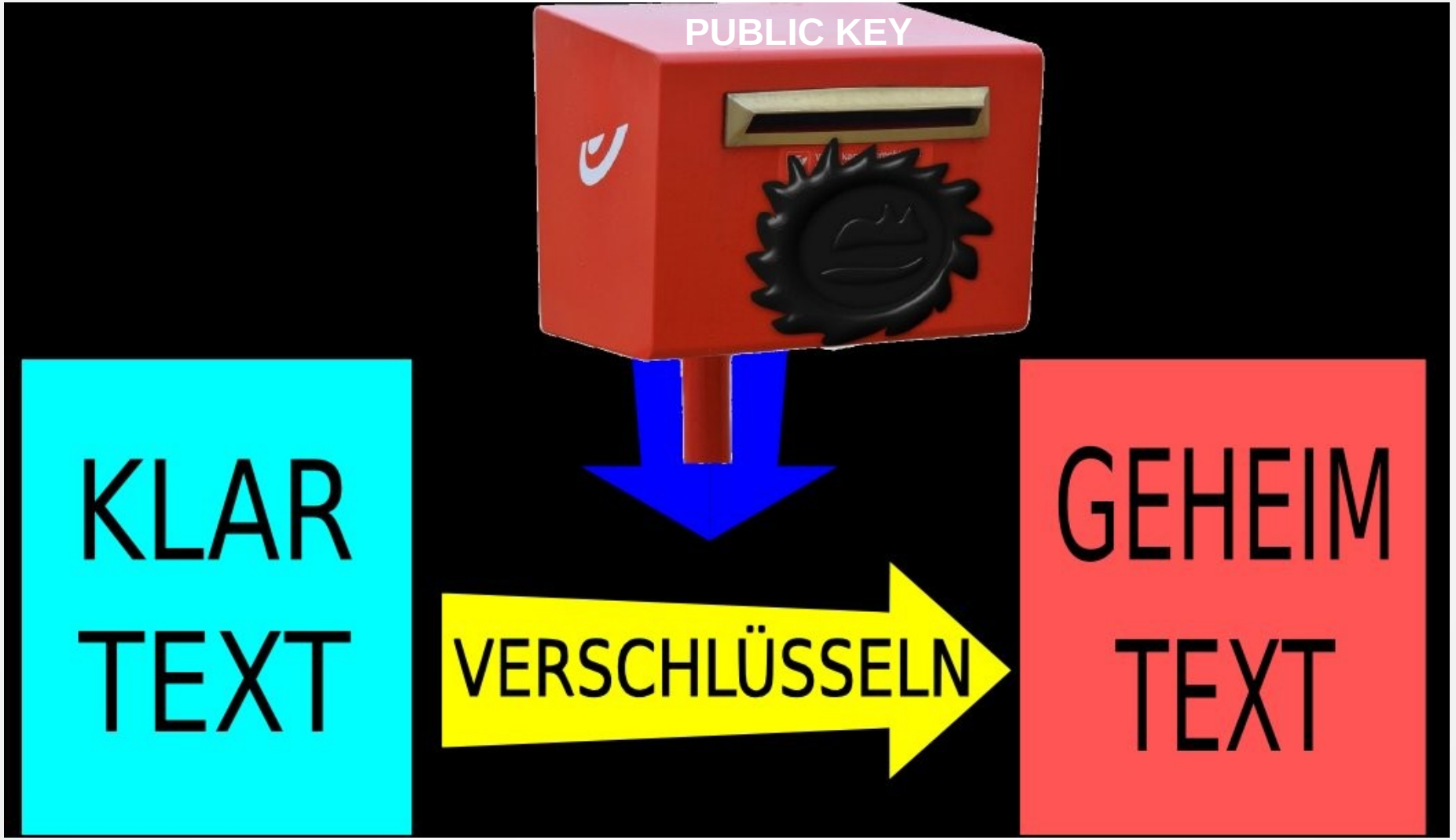
Asymmetrische Verschlüsselung

- Paar aus öffentlichem und privatem Schlüssel
- öffentlicher Schlüssel kann/soll frei verteilt werden
- Privater Schlüssel MUSS geheim gehalten werden!
- Zum verschlüsseln verwendet man den öffentlichen Schlüssel des Empfängers
- Empfänger verwendet seinen privaten Schlüssel zum entschlüsseln
- Signatur möglich

Privater und öffentlicher Teil des Schlüssels



Verschlüsselung



Geheimtext Beispiel

-----BEGIN PGP MESSAGE-----

Charset: ISO-8859-1

Version: GnuPG v1.4.8 (Darwin)

Comments

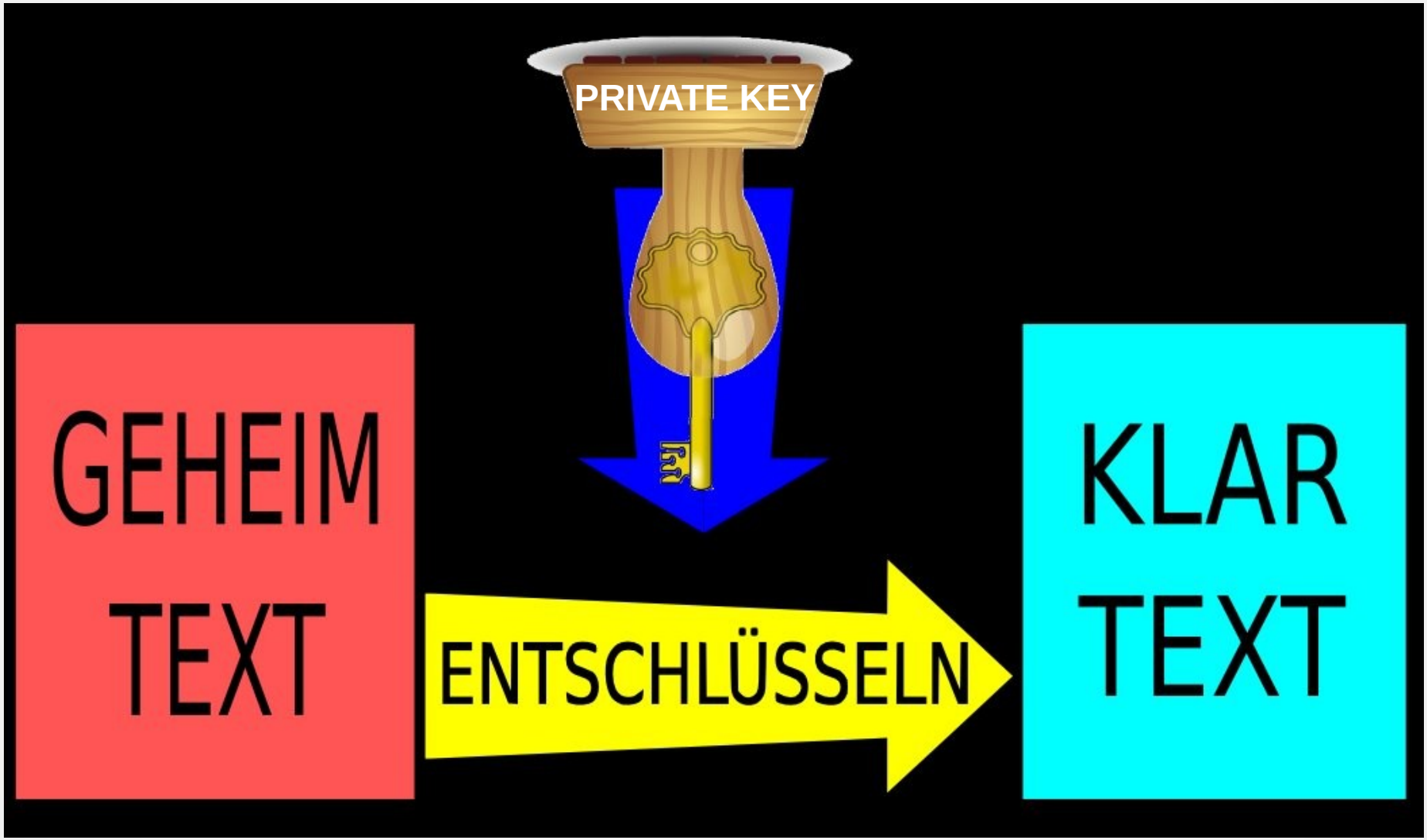
e+HWncM+lZ7lfwUzXi3KEfqNqYyrh4u9xtc2je
BDz2mFNbmZo1sZNAq6ZzU/8dlF

uiUri5M8zNBSpCVbTDq2QF3xiMddnYyZ

=3DDX2S.....

-----END PGP MESSAGE-----

Entschlüsselung



Grenzen von PGP/GPG

- Ihr privater Schlüssel fällt in fremde Hände
- jemand veröffentlicht öffentliche Schlüssel unter falschem Namen bzw. E-Mail
- Sie löschen Ihre Dateien nicht gründlich
- Viren und Trojanische Pferde
- unbefugter Zugriff auf Ihren Rechner

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

Was tun?

- Privaten Schlüssel mit Passwort sichern
- Fingerprints überprüfen
- „Web of Trust“ benutzen (optional)
- Software und Virenscanner aktuell halten

Praxis: GPG installieren

- Linux: meist vorinstalliert (Packetmanger)
- Windows: Download gpg4win von
  https://www.gpg4win.org
- Mac OS X: Download gpgtools von
  https://gpgtools.org

Praxis: Schlüssel erzeugen

Tunderbird:

Enigmail > Schlüssel verwalten

Erzeugen > Neues Schlüsselpaar

Komandozeile:

gpg --gen-key

Praxis: Empfohlene Einstellungen

- Algorithmus: RSA
- Schlüssellänge: 4096
- Gültigkeitsdauer: 1-3 Jahre
- Name und E-Mail eingeben
- Kein Kommentar
- Passphrase eingeben

Praxis: Wiederrufzertifikat erstellen

Thunderbird:

Enigmail > Schlüssel verwalten

Rechtsklick auf den Schlüssel >

Wiederrufzertifikat erstellen

Kommandozeile:

gpg --gen-revoke KeyID

Praxis: Export des Schlüssels

Thunderbird:

Enigmail > Schlüssel verwalten

Rechtsklick auf den Schlüssel >

In Datei exportieren ...

Kommandozeile:

gpg -a --export-secret-subkeys KeyID

Praxis: Schlüsselserver benutzen

Veröffentlichen des **öffentlichen** Schlüssels:

Thunderbird:

OpenPGP > Schlüssel verwalten

Rechtsklick auf den Schlüssel >

Auf Schlüsselserver hochladen …

Kommandozeile:

gpg --send-keys KeyID

Praxis: Öffentliche Schlüssel besorgen

Thunderbird:

OpenPGP > Schlüssel verwalten

Schlüssel-Server > Schlüssel suchen

KeyID oder e-Mail eingeben

Kommandozeile:

gpg --recv-keys KeyID

Web:

https://sks-keyservers.net/

Praxis: Schlüssel überprüfen

Um sicherzustellen dass ein öffentlicher Schlüssel wirklich der erwarteten Person gehört muss man über einen zweiten Kommunikationskanal den Fingerprint austauschen!

Thunderbird:

OpenPGP > Schlüssel verwalten

Rechtsklick auf den Schlüssel > Schlüsseleigenschaften

Kommandozeile:

gpg --fingerprint KeyID

Erste verschlüsselte e-Mail

Thunderbird:

OpenPGP > Nachricht verschlüsseln

OpenPGP > Nachricht signieren

Kommandozeile:

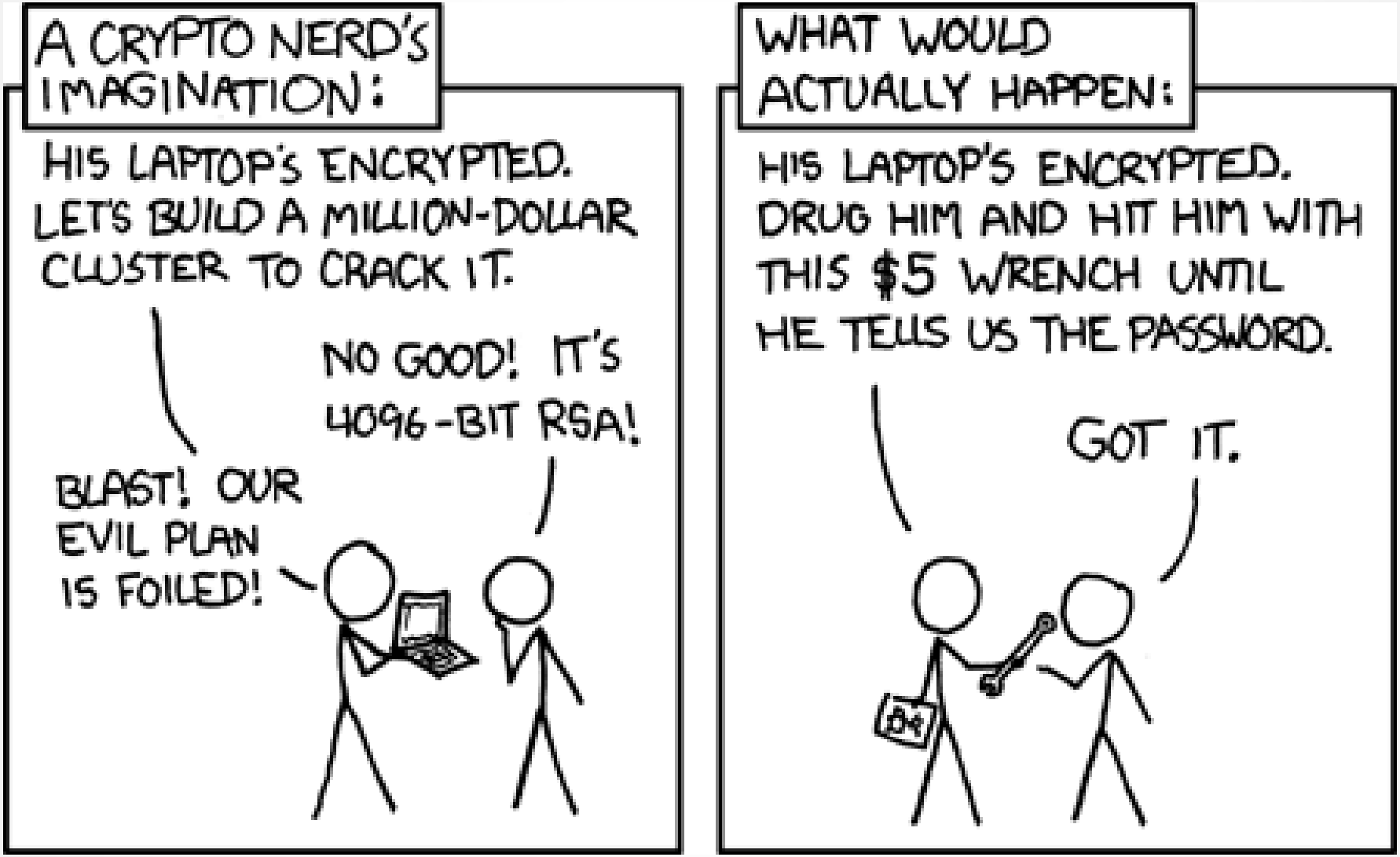
E-Mail in Datei speichern (e-mail.txt)

gpg -a -e -s -u "SenderID" -r "ReceiverID" e-mail.txt

Verschlüsselte, signierte Datei in e-mail.txt.asc

Entschlüsseln: gpg -d --verify message.txt.asc

Danke für Ihre Aufmerksamkeit und Paranoia.



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

Weiter geht’s mit...

Keysigning-Party:

heute und morgen um 18:00!

Nur mit Ausweis!

Fleißig nutzen und weitersagen!

Digitale Selbstverteidigung/CryptoParty:

- cryptoparty@mur.at
- cryptoparty-orga@mur.at
- https://cryptoparty.at/graz