Einführung in PGP/GPG
Mailverschlüsselung

Olaf

Olaf.P@gmx.at KeyID: 0xCAB623BD

Finger Abdruck: CAAF 5E4E E0D3 A122 0FC1 568F 995D 1164 **CAB6 23BD**

12.4.2014

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

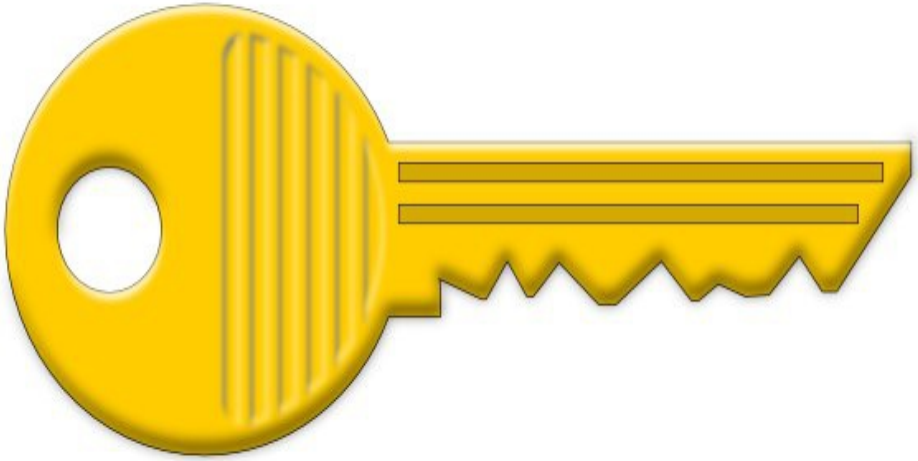
- Nachricht stammt sicher vom Sender
- Nachricht wurde nicht verändert

Verschlüsselung

- Briefgeheimnis
- Kuvert für Emails
- Vertrauliche Informationen

Symmetrische Verschlüsselung

SYMMETRISCH



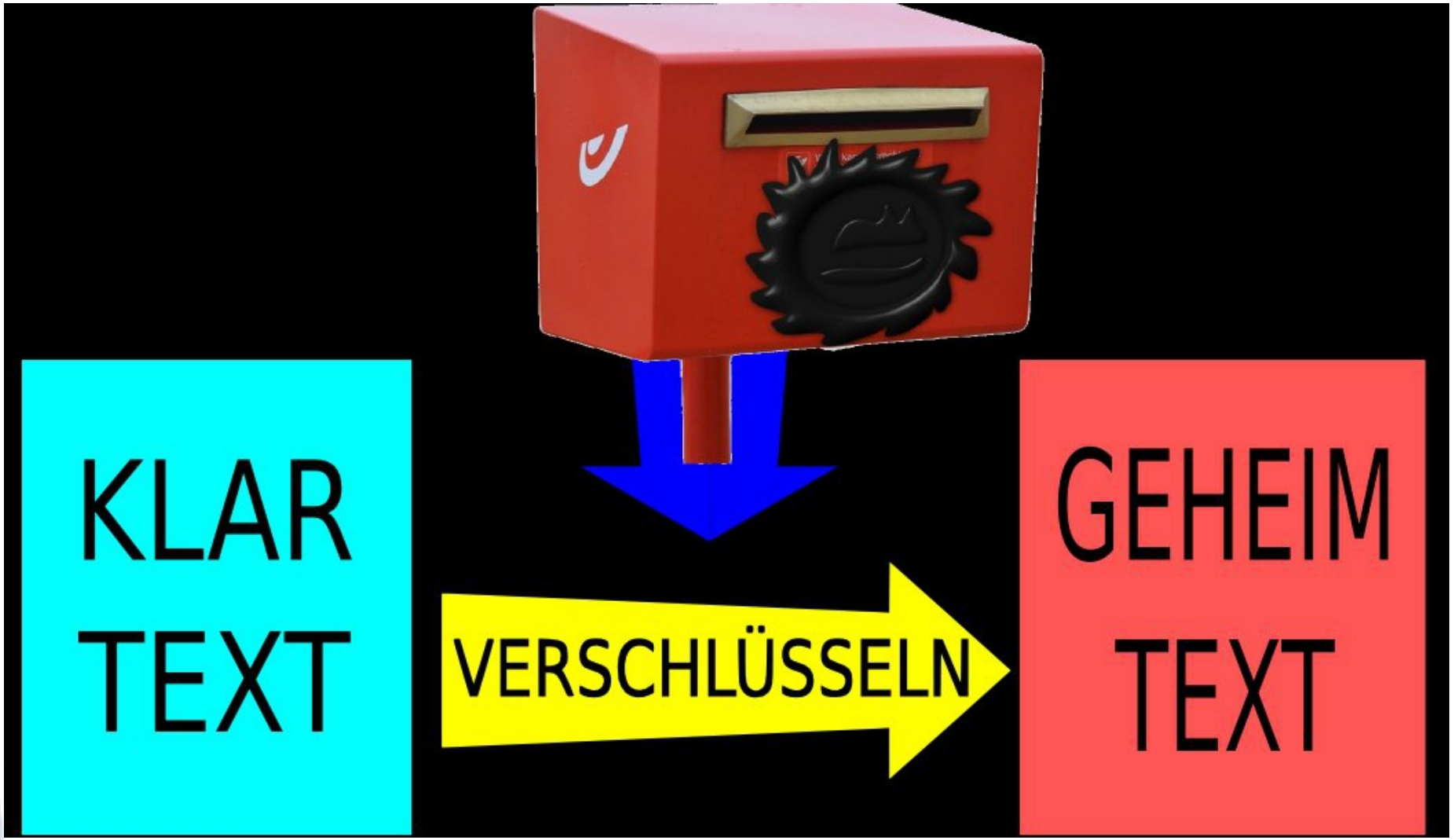
Asymmetrische Verschlüsselung

- öffentlicher und privater Schlüssel
- öffentlicher Schlüssel kann/soll frei verteilt werden
- Privater Schlüssel MUSS geheim gehalten werden!
- Signatur möglich
- RSA, Elgamal, ...

Privater und öffentlicher Teil des Schlüssels

PUBLIC PRIVAT

Verschlüsselung



Geheimtext Beispiel

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

Charset: ISO-8859-1

Version: GnuPG v1.4.8 (Darwin)

Comments

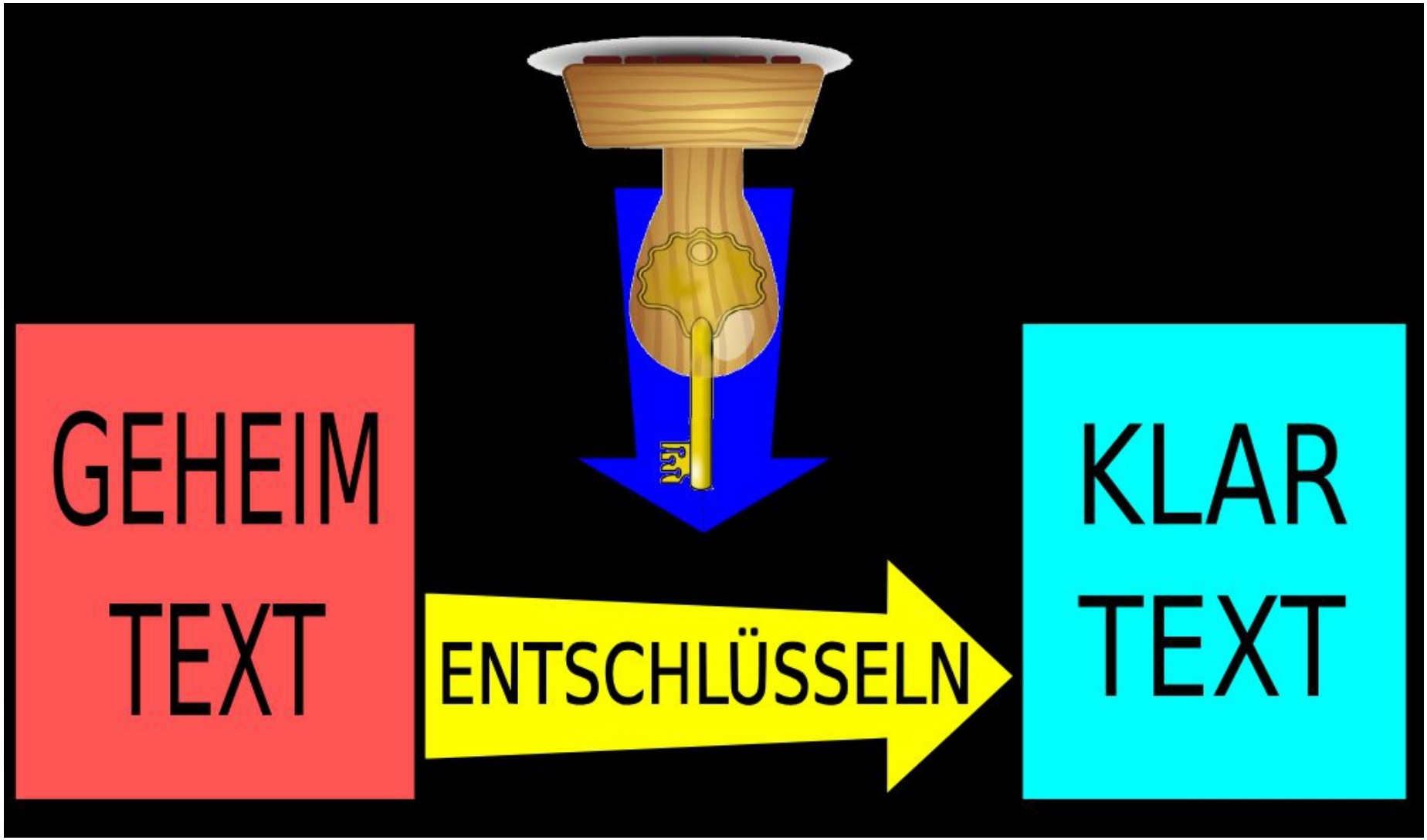
e+HWncM+lZ7lfwUzXi3KEfqNqYyrh4u9xtc2je
BDz2mFNbmZo1sZNAq6ZzU/8dlF

uiUri5M8zNBSpCVbTDq2QF3xiMddnYyZ

=3DDX2S.....

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

Entschlüsselung



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

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

Praxis: GPG installieren

- Linux: meist vorinstalliert
- Windows: Download gpg4win von

  https://www.gpg4win.org
- Mac OS X: Download gpgtools von

  https://gpgtools.org
- **Wichtig:**

  Überprüfen der Checksumme der Downloads

Praxis: Schlüssel erzeugen

Komandozeile:

- gpg --gen-key

Thunderbird:

- Extras > Add-ons
- Enigmail installieren
- OpenPGP > Schlüssel verwalten
- Erzeugen > neues Schlüsselpaar

Praxis: Empfohlene Einstellungen

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

Praxis: Wiederrufzertifikat erstellen

Bei Generierung: Speicherort wählen

Dannach:

- Komandozeile:

  gpg --gen-revoke KeyID

- Thunderbird:

  OpenPGP > Schlüssel verwalten

  Rechtsklick auf den Schlüssel >

  Wiederrufzertifikat erstellen

Praxis: Export der Schlüssel (optional)

Zusätzliche Sicherheit:

- Im Klartext
- Sicher, offline Aufbewahren (ausdrucken,...)

Zum Portieren:

- Verschlüsseln
- Auf anderem Rechner importieren

Paxis: Schlüsselserver benutzen

Hochladen des **öffentlichen (public)** 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

Erste verschlüsselte e-Mail

- Thunderbird:

  OpenPGP > Nachricht verschlüsseln

  OpenPGP > Nachricht signieren

- Kommandozeile:

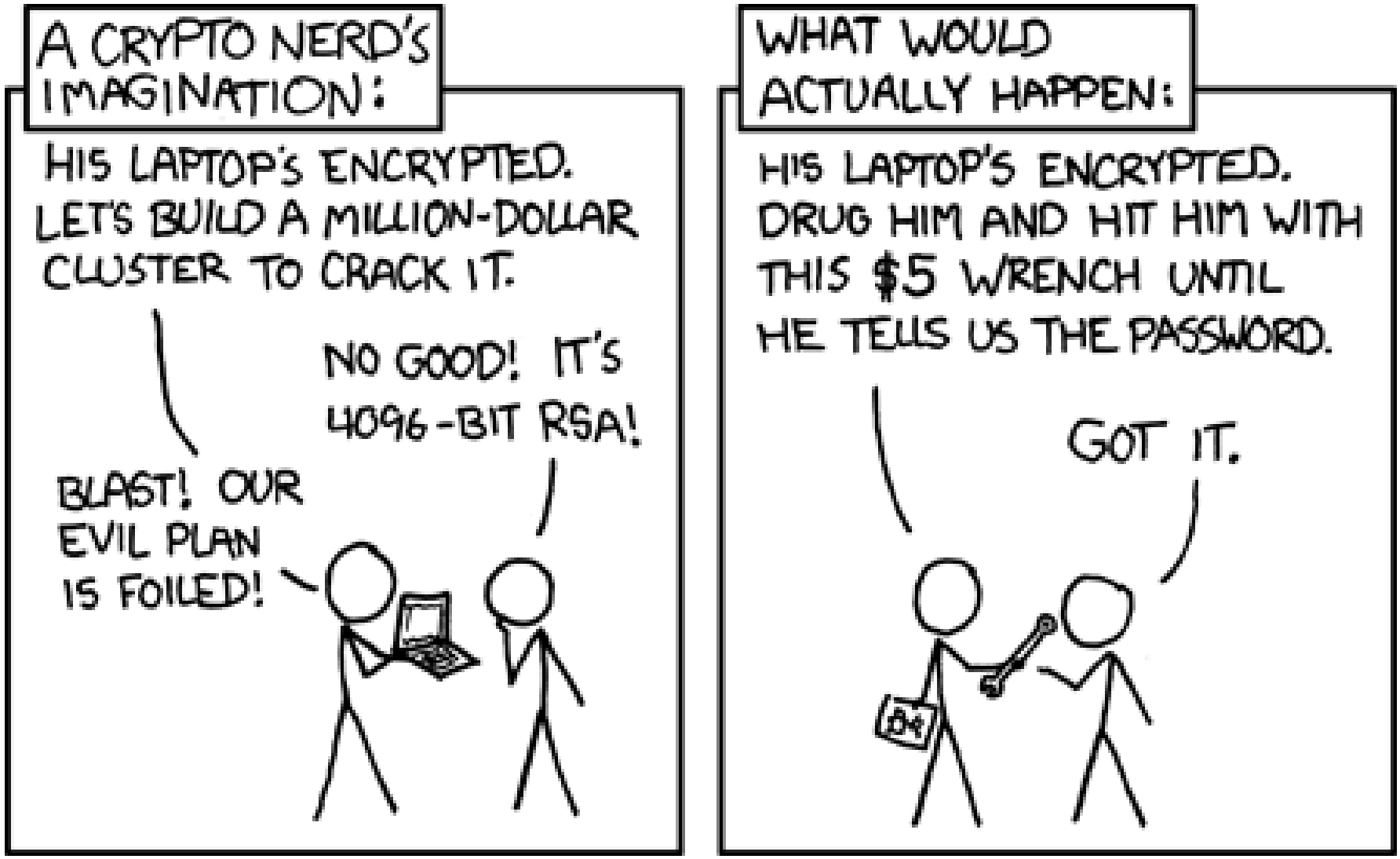
  E-Mail in Datei speichern (e-mail.txt)

  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...

Fleißig nutzen und weitersagen!

Digitale Selbstverteidigung/CryptoParty:

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