DIGITALE SELBSTVERTEIDIGUNG: MAIL-VERSCHLÜSSELUNG

1 WO SIND DIE PROBLEME?

- E-Mails sind offen wie Postkarten.
- Jeder auf dem Weg kann sie lesen:
  IT-Abteilung des Arbeitgebers, Google, …
- Tempora: Britischer Geheimdienst schneidet gesamten Transatlantik-Datenverkehr mit.

2 WAS KÖNNEN WIR TUN?

- PGP („Pretty Good Privacy“) bzw. GPG („GNU Privacy Guard“)
- Asymmetrische Verschlüsselung
  - keine Verabredung eines geheimen Schlüssels nötig
  - Verschlüsselung mit öffentlich bekannt gegebenem Schlüssel
  - Entschlüsselung nur mit privatem Schlüssel möglich
  - auch für digitale Unterschriften geeignet:
    Unterschreiben nur mit privatem Schlüssel möglich und
    Überprüfen mit öffentlich bekannt gegebenem Schlüssel
- Plugins für alle gängigen Mail-Programme verfügbar
  - *Enigmail* für Mozilla Thunderbird
  - *GPGTools* für Apple Mail.app
  - *Gpg4win* für Microsoft Outlook

3 WAS BLEIBT AN PROBLEMEN?

- Beide Seiten müssen Verschlüsselung eingerichtet haben.
  ⇒ immer noch recht niedrige Verbreitung
- Privater Schlüssel muss vor Dritten geschützt werden.
- Meta-Daten („Wer schreibt wann an wen?“) und Betreff bleiben unverschlüsselt.
- Eventuell erwecken *gerade* verschlüsselte Mails Interesse.
  ⇒ kein Schutz gegen gewaltsamen (oder rechtlichen) Zwang

PIRATEN INFORMIEREN