Let's Encrypt

-----BEGIN PGP MESSAGE-----
Version: GnuPG v2

hQIMA1HNQsnD0P+MARAAkbqEdB9aQQEI/Jkw9VAH/aMS7uMriMjBwt+TugDpOeu1
/b8CaxqwB8EHXI3ic8Zb1dbqDAJhn1QTcsWONrwztZm/VIdn8FYAPEuUFZml6VCC
If6pMplRh6gJKAsqvmns1IvZbQaq3ZylcLOm1Ac01co3JyKT229w7UwyR4OwmkM4
kPPKUYrwd4ByWxtQpEbSHqys+CmMwvNtFX4v4kH8J6MyI6KsnVvyA6jHObF/PhyW
SQArlH42CJWhuaMoDfC/IUu4FYaPz4M95wemr1BGgnmtMm2Dw1ZOJNmjrvHUICMa
JheIdPS0IZsLEP6YbM+E+o5/iqWNdbGzQGbOdvxzPKPmwDar7on5rbFAj+n7IF5u
0p2WqgV0ZDqsBXPSBrbTN50ekJ48tbYo57xRjiTNEDa8PqdbJ/Gt7LvOsSGiAoPw
bqaza4fHSTyXI9MG8eXm767ENQEzj5N6fR1bVsaRJUI71HbGntELOuAvcqaCyboK
hEpdiMpd5GoWG6ce8h1ARIoJry3TA8S7gcMAAw7qHwLGA7aty3J6zFCa5sqiHG66
7Aw5sGGVcsyfGhDKIaNnp5UR/cxDJD5G5CSHnFB4b5Sc74qabGkuy8lSf4SgJitJ
Ggj+yiviiHFS4PSySDp0oNRZix0Gwx1+dShF7ObAdA2QjzK/HEbhijb5ZBa4O97S
XwH0wnmEXDAQavi1As+w3MkX4/tm8MvRfNJv12vGZ5JmKRM2Nv4uXgz4QLfJyD3B
xHlSH1iJVEXwBryXfVugBW0T33wFiXR10rTGe0qe/ja7XjUeIKSonTraf8AeysuC
=zrQx
-----END PGP MESSAGE-----

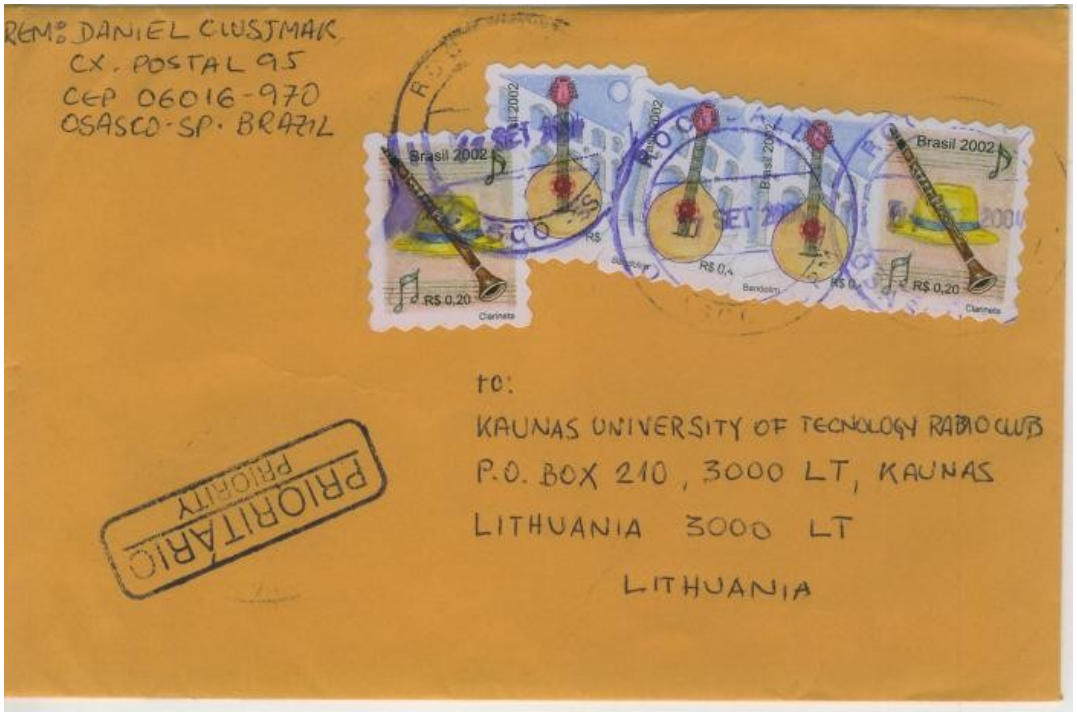
Agenda

- **Basics**
  - Warum Crypto
  - Symmetrische / Asymmetrische Crypto
  - Inhalt oder Verbindung
- **E-Mail Sicherheit**
  - TLS/SSL
  - PGP
- **Internet**
  - HTTPS
  - TOR
- **Abschluss**
- **Q&A**

Gründe

E-Mail

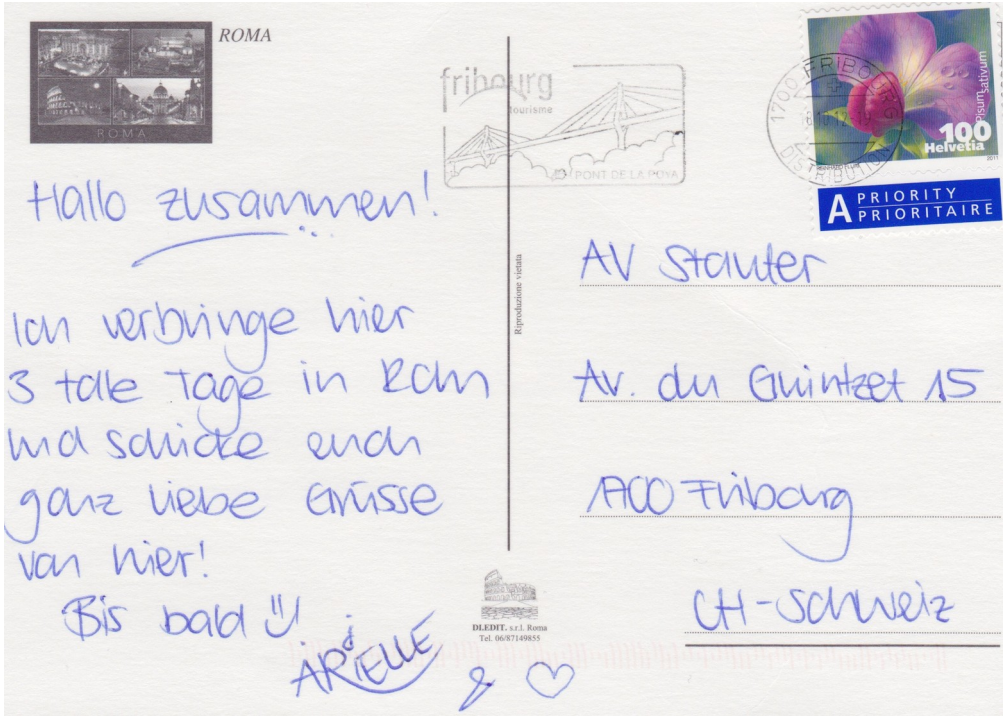
Kennt man als:



Gründe

E-Mail

Realität:

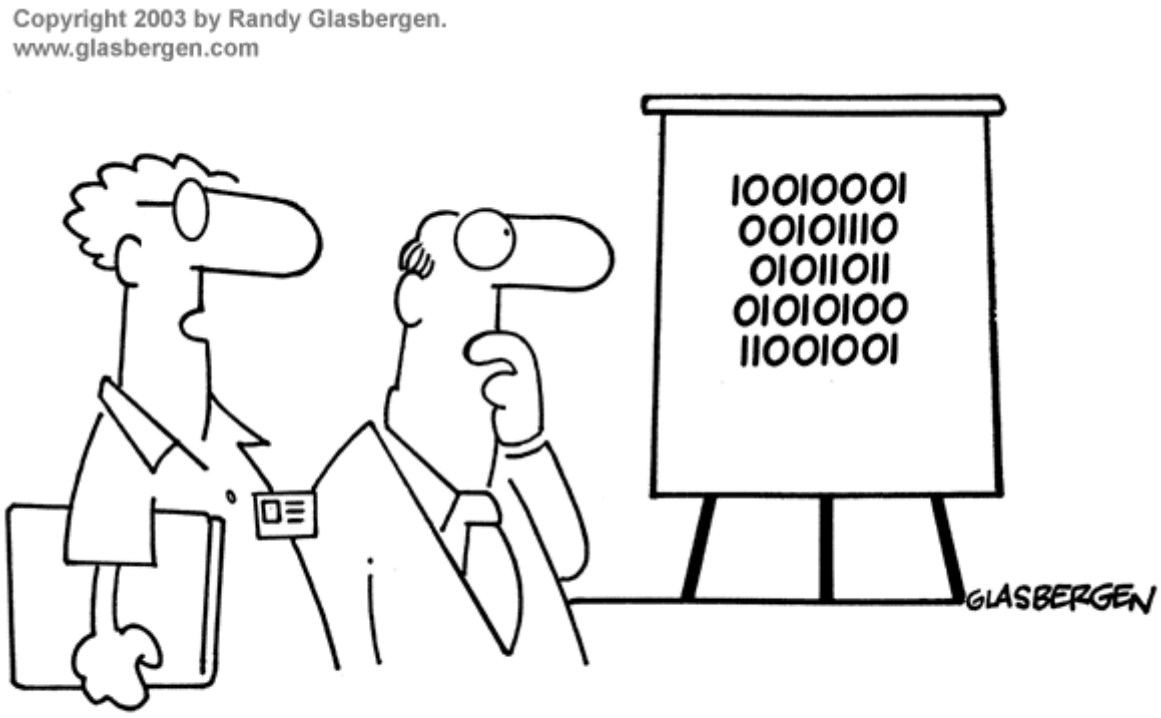


Was sind die Probleme?

- **Jeder kann mitlesen**
  - Reiner Text
  - Mitleser (Potentiel)
    - Clients
    - Server
    - Und alles was dazwischen liegt
    - => also überall
- **Ist der Absender auch wirklich der Absender?**
  - Brief im „Namen“ von anderen Versenden
  - Spam-Bots

Was schafft Abhilfe?

Crypto



**"We've devised a new security encryption code.
Each digit is printed upside down."**

Wie geht denn das?
Symmetrische Crypto

Wie geht denn das?
Symmetrische Crypto - Realbeispiel

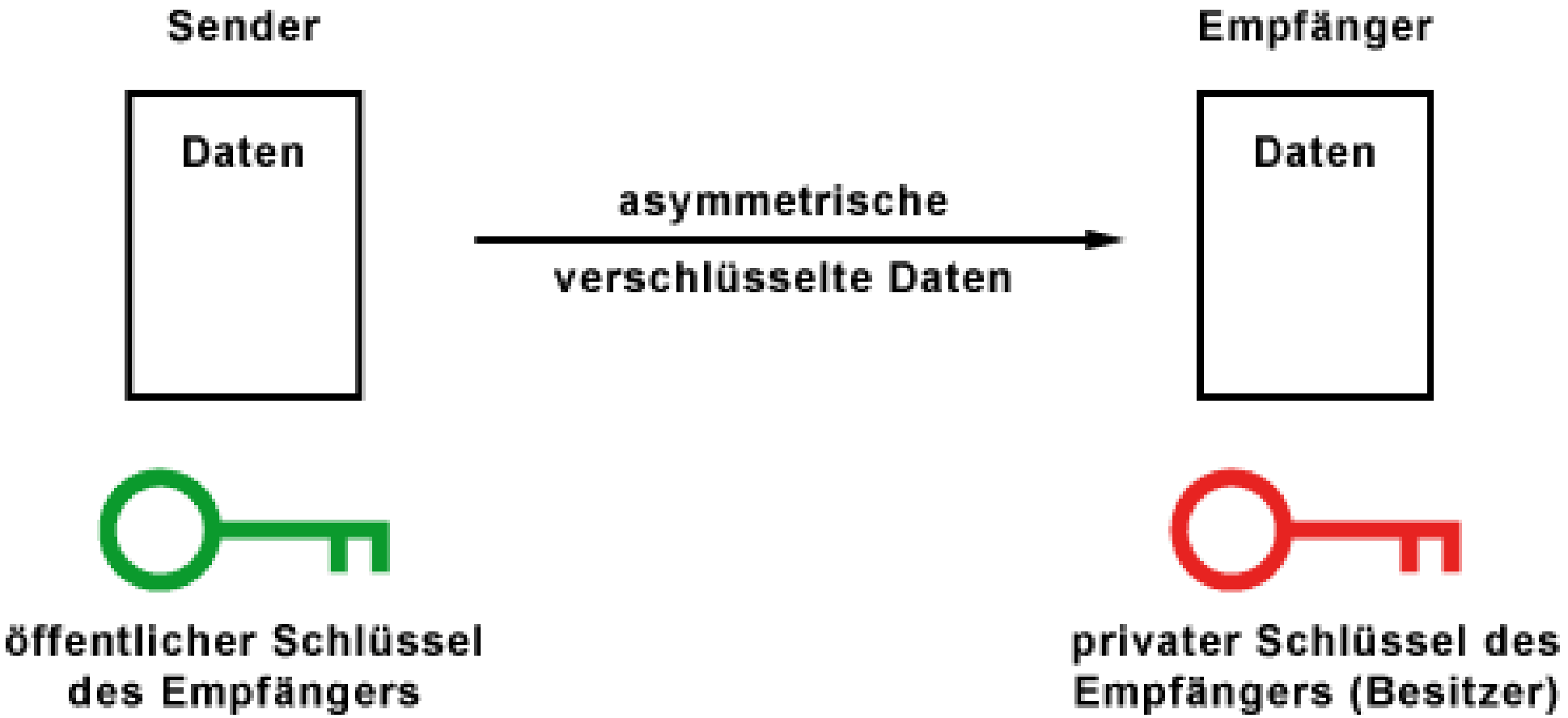
Wie geht denn das?
Symmetrische Crypto

- **Pro**
  - Einfach
  - Braucht nicht viel Aufwand
  - Kann jeder lesen, der den Schlüssel hat
- **Contra**
  - Einfach(er)
  - Braucht nicht viel Aufwand
  - Kann jeder lesen, der den Schlüssel hat

Wie geht denn das?
Symmetrische Crypto – Nutzung

- **Verschlüsselung für ein Gruppe**
  - z.B.: Freigegebene Dateien
    - Firmennetz
    - Cloud
- **Verschlüsselung für Daten die sich nicht bewegen**
  - Backupverschlüsselung
  - Einfache Dateiverschlüsselung
  - Festplattenverschlüsselung

Wie geht das denn?
Asymmetrische Crypto



Wie geht denn das?
Asymmetrische Crypto - Realbeispiel

Wie geht denn das?
Asymmetrische Crypto

- **Pro**
  - Bestimmte Empfänger
  - Kleiner Schlüsselaustausch
  - Kann nur der mit dem Privaten Schlüssel lesen
  - Lässt Absender Verifikation zu
- **Contra**
  - Komplex
  - Hat nicht jeder
  - Schwachstelle Privater Schlüssel

Was kann ich Verschlüsseln?

- **Verbindung**
  - Verschlüsselt von Client zu Server
  - Häufig SSL/TLS
- **Inhalte**
  - Verschlüsselt Inhalt
  - Haufig
    - AES 256bit
    - PGP

Wie schalte ich Verschlüsselung ein? E-Mail (Nachrichten-Dienste)

- **Sichere Verbindung zum Mailserver**
  - SSL/TLS
- **Verifikation des Mailservers**
  - SSL/TLS
- **Sicheren Inhalt**
  - PGP
- **Verifikation des Absenders/Empfängers**
  - PGP

Wie schalte ich Verschlüsselung ein?
E-Mail - Verschlüsselte Verbindungen

- **IMAP (Empfang)**
  - STARTTLS
    - Port: 143
  - IMAPS (IMAP over SSL)
    - Port: 993
- **POP3 (Empfang)**
  - STARTTLS
    - Port: 110
  - POP3 over SSL
    - Port: 995

Wie schalte ich Verschlüsselung ein? E-Mail - Verschlüsselte Verbindungen

- **SMTP (Senden)**
  - STARTTLS
    - 465
  - SSL
    - 587 (aber auch: 465)
  - Benutzt Authentifizierung (eurem Mailanbieter zuliebe)

Wie schalte ich Verschlüsselung ein?
E-Mail - Verschlüsselte Verbindungen

„Mein Mailanbieter hat aber sowas wie SSL/TLS nicht“

SUCH DIR EINEN ANDEREN MAILANBIETER!!!

Wie schalte ich die Verschlüsselung ein? E-Mail - Inhaltsverschlüsselung

- **PGP**
  - Thunderbird → Enigmail
  - Outlook → Gpg4Win
  - Apple Mail → GPGTools
  - K9 Mail (Android) → OpenKeyChain
  - IOS → iPgMail

Wie schalte ich die Verschlüsselung ein?
E-Mail - Inhaltsverschlüsselung - Schritte

1. **Schlüsselpaar erzeugen**
   1. Auf eine Mailadresse
   2. Mit einem Passwort gesichert
2. **Öffentlichen Schlüssel austauschen**
   1. Key Server
   2. Von Hand
3. **Privaten Schlüssel sichern (WICHTIG)**
4. **Lossenden**

Wie prüfe ich den Sender/Empfänger? E-Mail - Das Web of Trust

- **Unterschreiben öffentlicher Schlüssel**
  - Keysigning
  - Nach Überprüfung der Person
  - Unterschreiben mit eigenem privaten Schlüssel
- **Web of Trust**
  - A vertraut B vertraut C vertraut D
- **Wirkung**
  - Ist der öffentliche Schlüssel von mir unterschrieben?

Wie ist denn das mit dem Internet? Crypto im Internet

- **HTTPS**
  - Asymmetrische Verschlüsselung
  - Schloss in der Adressleiste
  - Verifizierung über CA
  - Forcieren durch https anywhere
  - Beispiele
    - https://www.google.ch (Gutes Beispiel)
    - https://www.lugo.ch(Schlechtes Beispiel)

Wie ist denn das mit dem Internet? Crypto im Internet

- **TOR**
  - https://www.torproject.org
  - Anonymes Surfen
  - Gesicherten Verbindungen
  - Empfehlung: Tor-Browser (Windows / Linux / Mac)

Abschluss

-----BEGIN PGP MESSAGE-----
Version: GnuPG v2

hQIMA1HNQsnD0P+MARAAkbqEdB9aQQEI/Jkw9VAH/aMS7uMriMjBwt+TugDpOeu1
/b8CaxqwB8EHXI3ic8Zb1dbqDAJhn1QTcsWONrwztZm/VIdn8FYAPEuUFZml6VCC
If6pMplRh6gJKAsqvmns1IvZbQaq3ZylcLOm1Ac01co3JyKT229w7UwyR4OwmkM4
kPPKUYrwd4ByWxtQpEbSHqys+CmMwvNtFX4v4kH8J6MyI6KsnVvyA6jHObF/PhyW
SQArlH42CJWhuaMoDfC/IUu4FYaPz4M95wemr1BGgnmtMm2Dw1ZOJNmjrvHUICMa
JheIdPS0lZsLEP6YbM+E+o5/iqWNdbGzQGbOdvxzPKPmwDar7on5rbFAj+n7IF5u
0p2WqgV0ZDqsBXPSBrbTN50ekJ48tbYo57xRjiTNEDa8PqdbJ/Gt7LvOsSGiAoPw
bqaza4fHSTyXI9MG8eXm767ENQEzj5N6fR1bVsaRJUI71HbGntELOuAvcqaCyboK
hEpdiMpd5GoWG6ce8h1ARIoJry3TA8S7gcMAAw7qHwLGA7aty3J6zFCa5sqiHG66
7Aw5sGGVcsyfGhDKIaNnp5UR/cxDJD5G5CSHnFB4b5Sc74qabGkuy8lSf4SgJitJ
Ggj+yiviiHFS4PSySDp0oNRZix0Gwx1+dShF7ObAdA2QjzK/HEbhijb5ZBa4O97S
XwH0wnmEXDAQavi1As+w3MkX4/tm8MvRfNJv12vGZ5JmKRM2Nv4uXgz4QLfJyD3B
xHlSH1iJVEXwBryXfVugBW0T33wFiXR10rTGe0qe/ja7XjUeIKSonTraf8AeysuC
=zrQx
-----END PGP MESSAGE-----

Äääähh
Ich hab da glaub ich was nicht verstanden

Fragen tut nicht schaden

ausser bei Politikern vielleicht ;)

Happy Encrypting/Decrypting