KRYPTOGRAFIE FÜR (JAVA-)ENTWICKLER

Grundlagen der Verschlüsselung

ITCONSULTINGHEMPEL

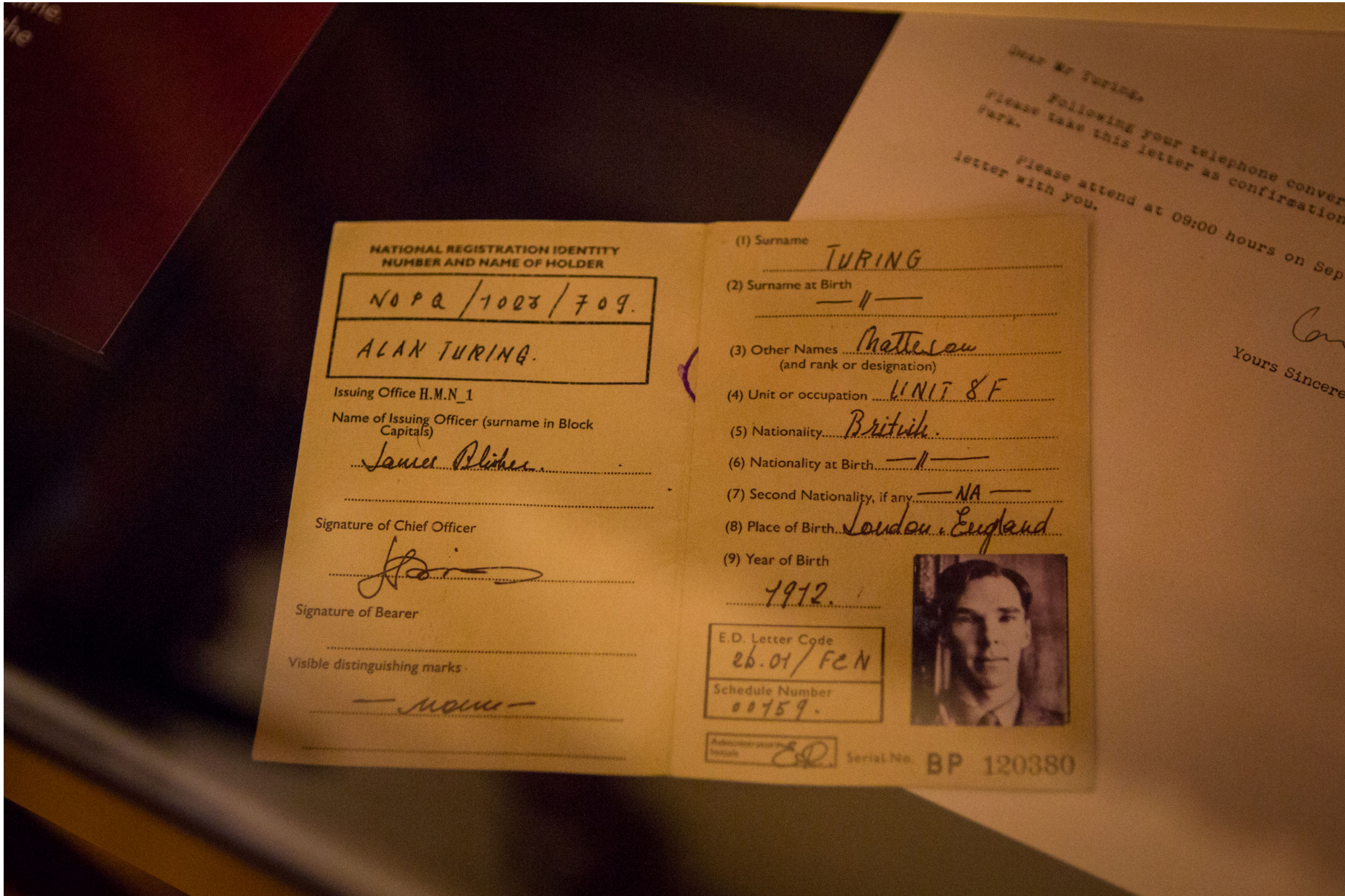
Sebastian Hempel

Sebastian Hempel

IT-Consulting Hempel
@ithempel
shempel@it-hempel.de

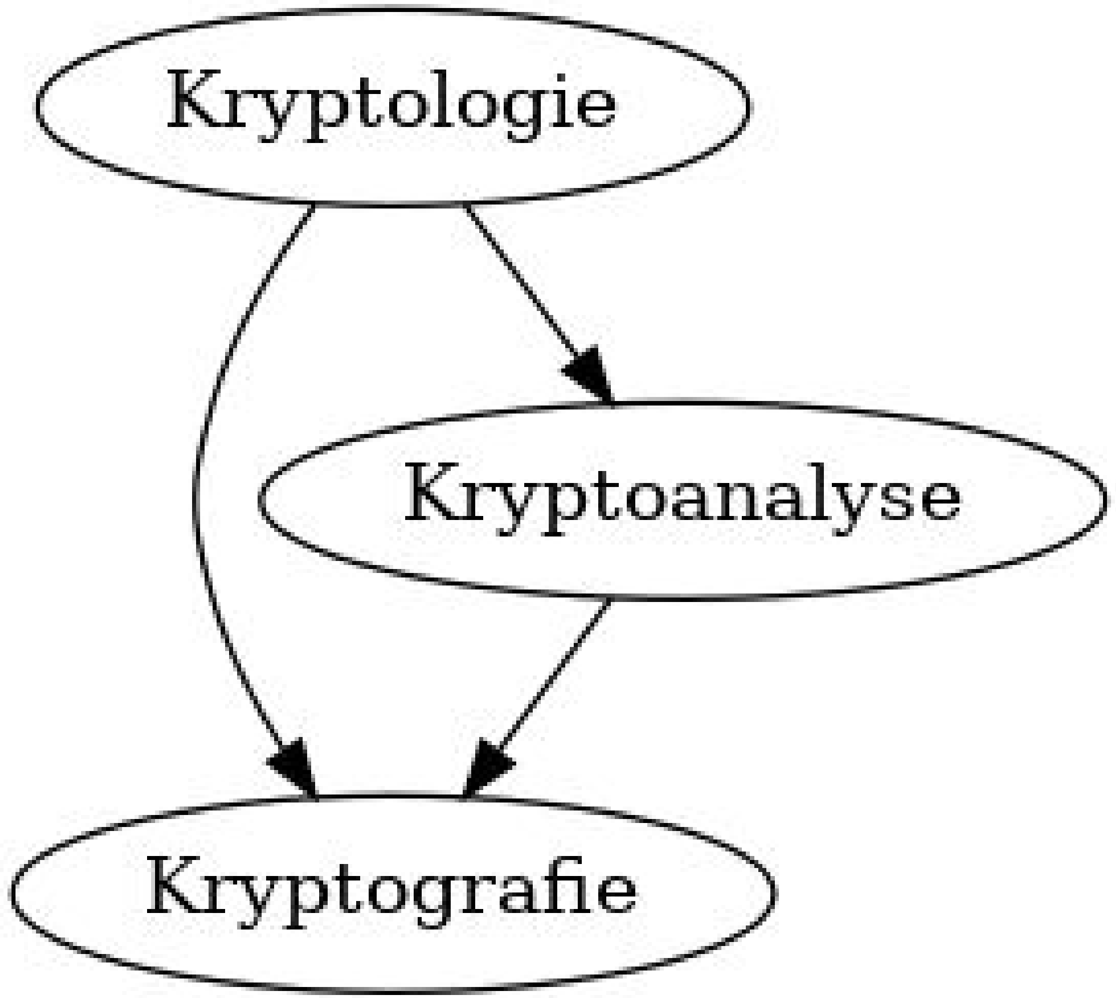
WARUM KRYPTOGRAFIE?

Max Braun - Whisper (CC BY-SA 2.0)



_dChris - Imitation Game (CC BY 2.0)

BEGRIFFE



GESCHICHTE DER KRYPTOGRAPHIE

HANDVERSCHLÜSSELUNG

- 3. Jahrtausend vor Christus in Ägypten
- Skytale Verschlüsselungsstab der Griechen

Wikimedia Commons - Skytale (CC BY-SA 3.0)

MASCHINEN

Sebastian Hempel - Enigma (CC BY-SA 4.0)

COMPUTER

Pretty Good Privacy

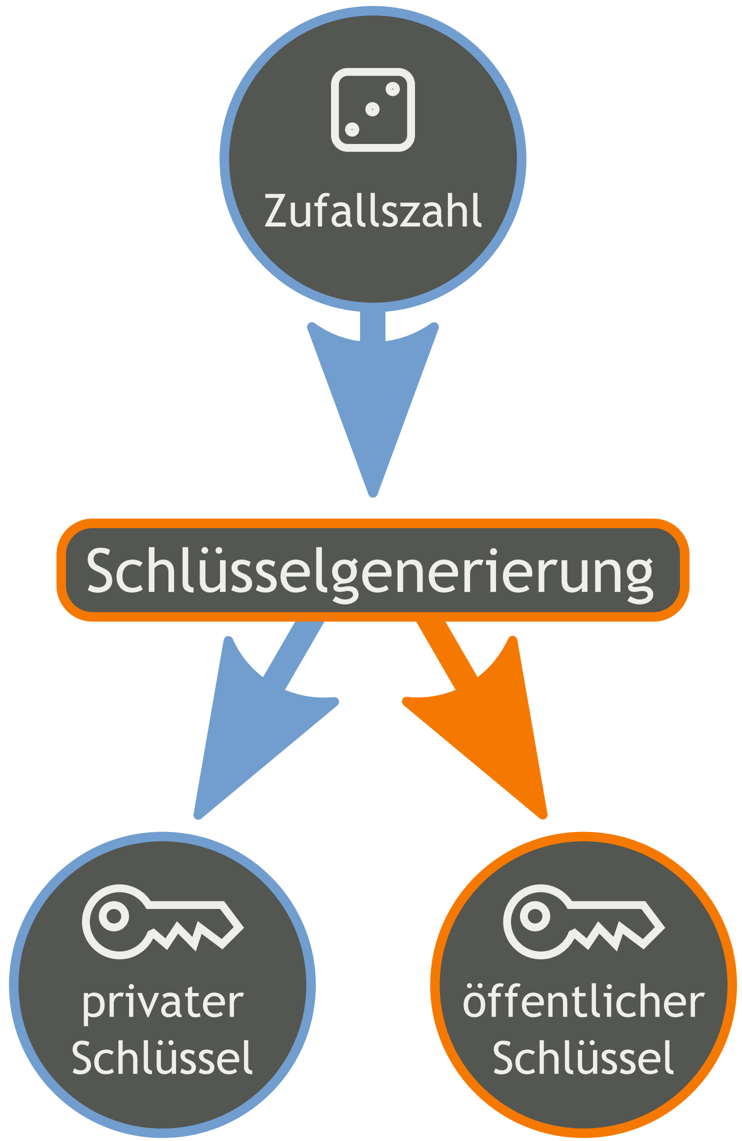
Matt Crypto - PRZ closeup (CC BY-SA 3.0)

BAUSTEINE DER MODERNE KRYPTOGRAFIEN

ZUFALL

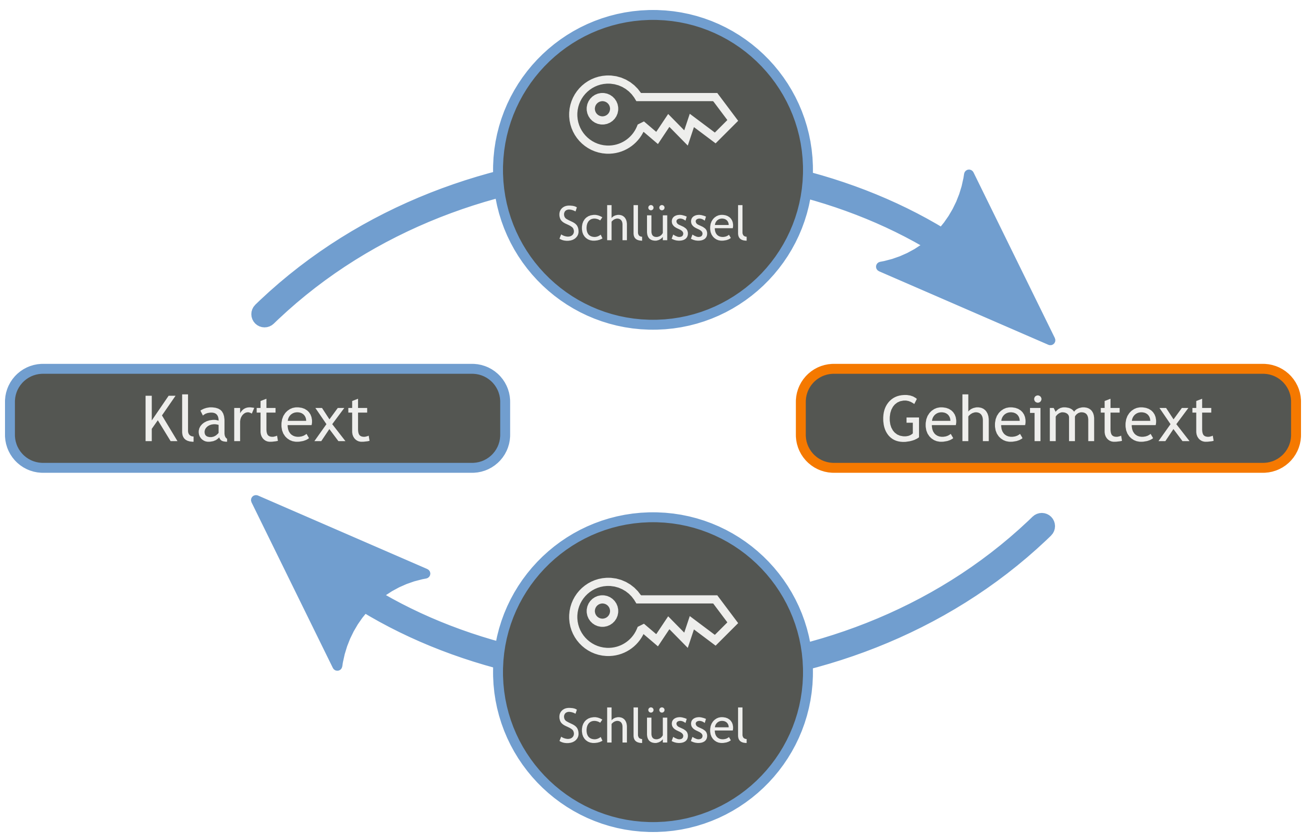
Wichtiges Element der Kryptografie

> *Schlüssel basieren auf Zufallszahlen*



Bananenfalter, Orange_blue_public_private_keygeneration_de

SYMMETRISCHE VERSCHLÜSSELUNG

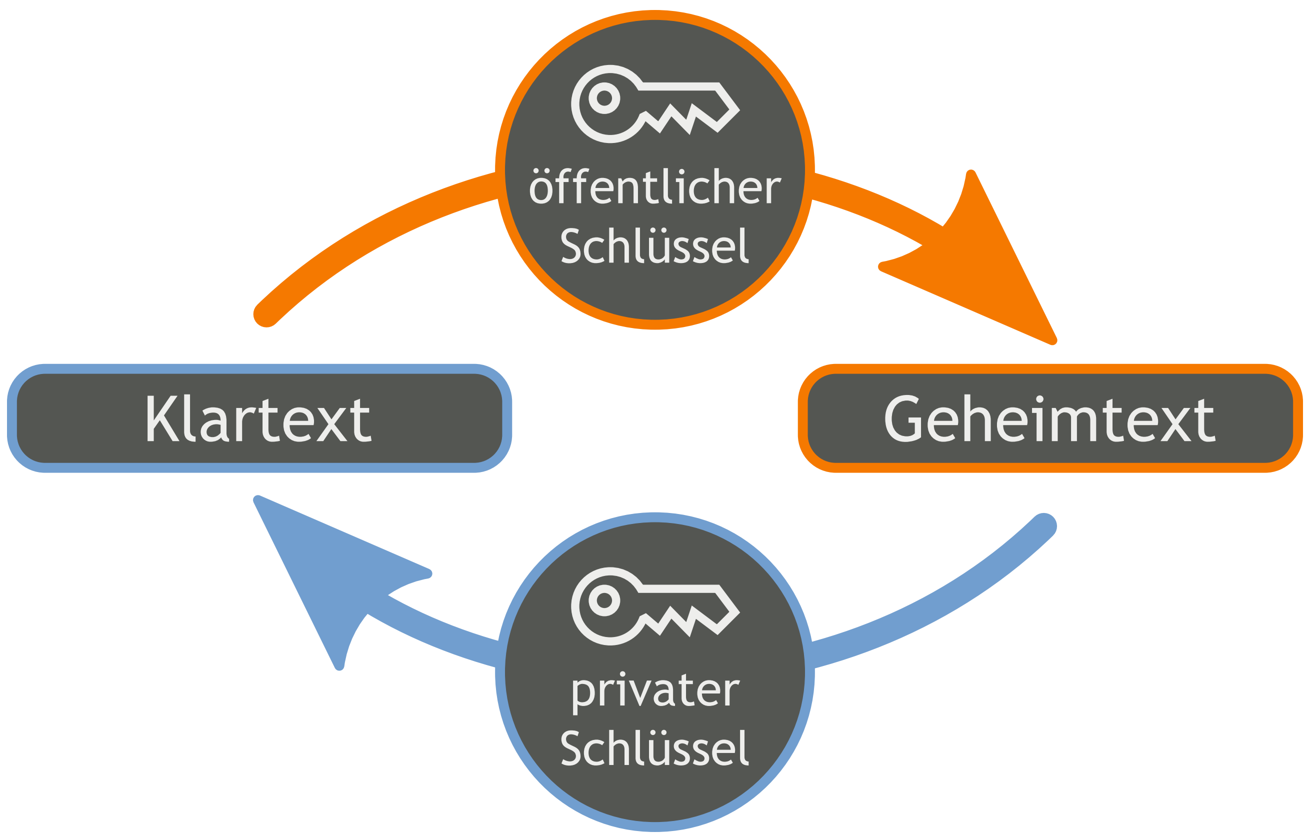


Bananenfalter, Eigenes Werk, (CC0)

SYMMETRISCHE VERFAHREN

- DES (1977)
- AES (2000)

ASYMMETRISCHE VERSCHLÜSSELUNG

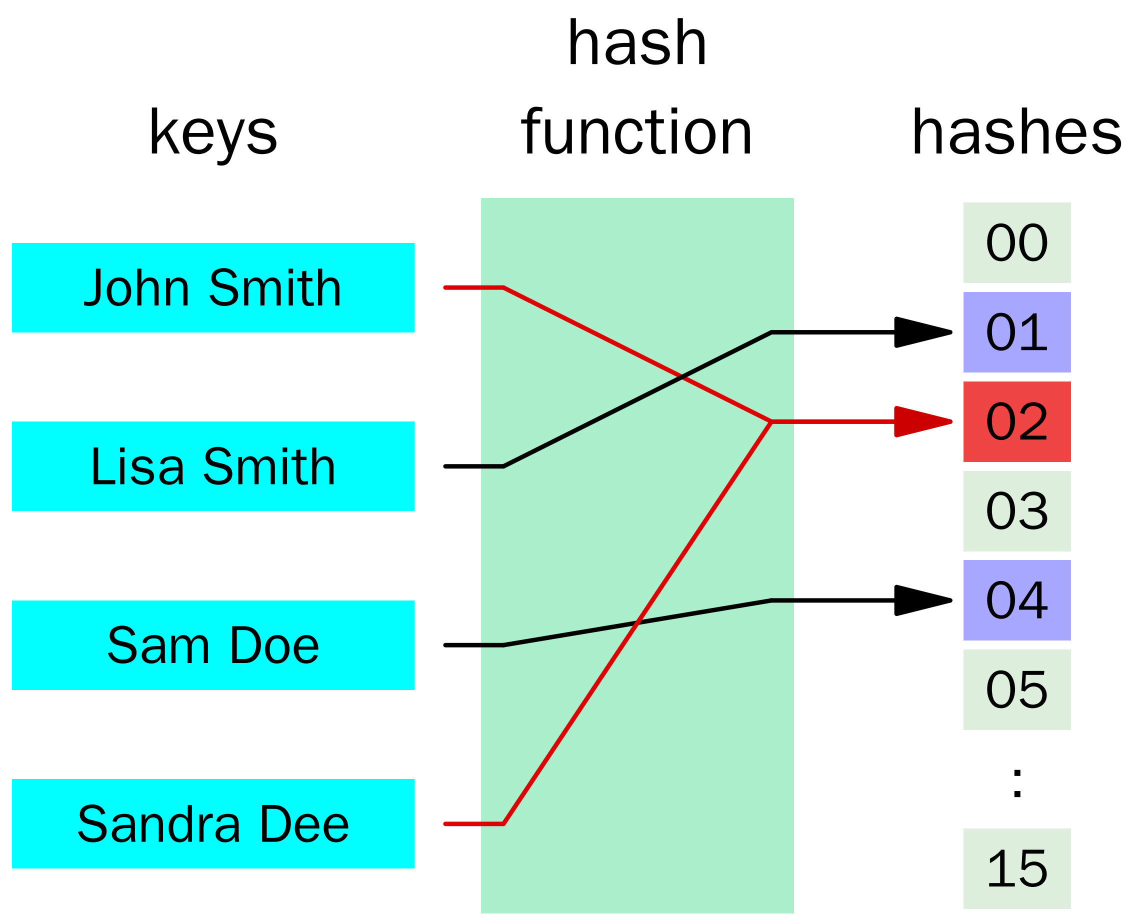


Bananenfalter, Eigenes Werk (CC0)

ASYMMETRISCHE VERFAHREN

- RSA (1977)
- Elliptische Kurven / ECC (Mitte der 1980er)

HASHFUNKTIONEN



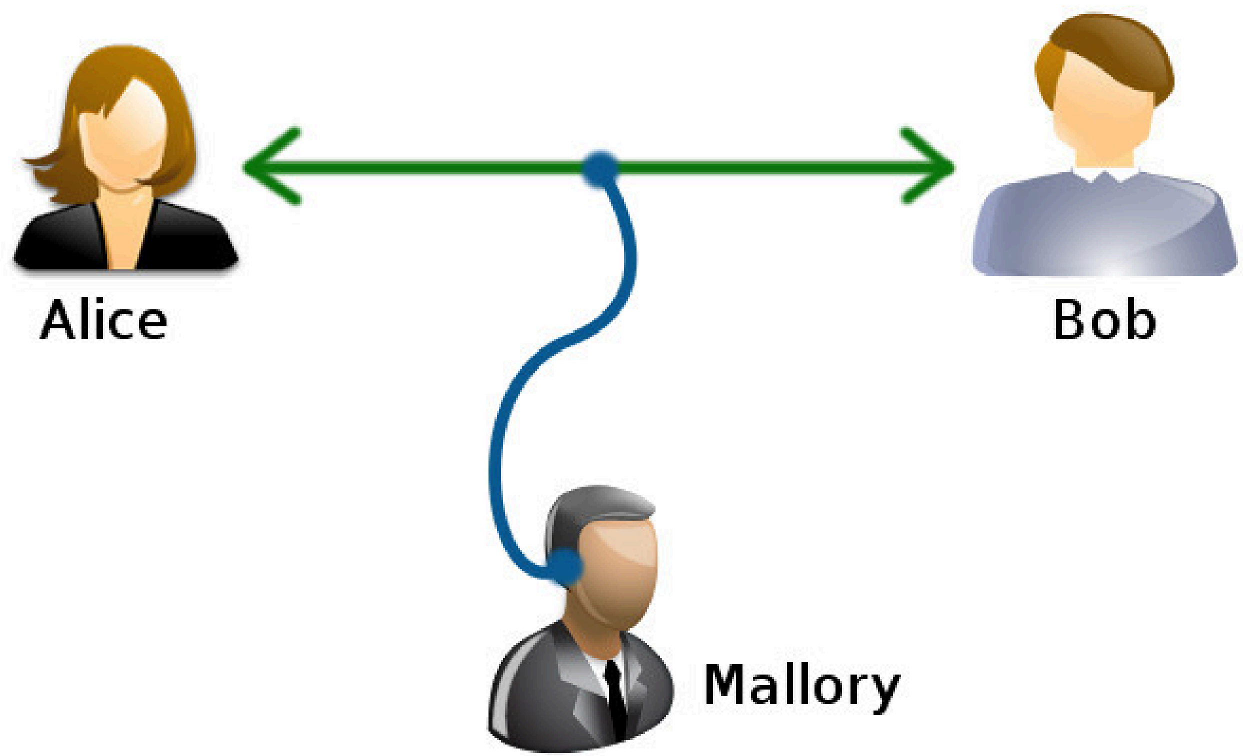
Jorge Stolfi, Eigenes Werk (Gemeinfrei)

KRYPTOGRAPHISCHE HASHFUNKTION

- MD5 (1992)
- SHA (1993)

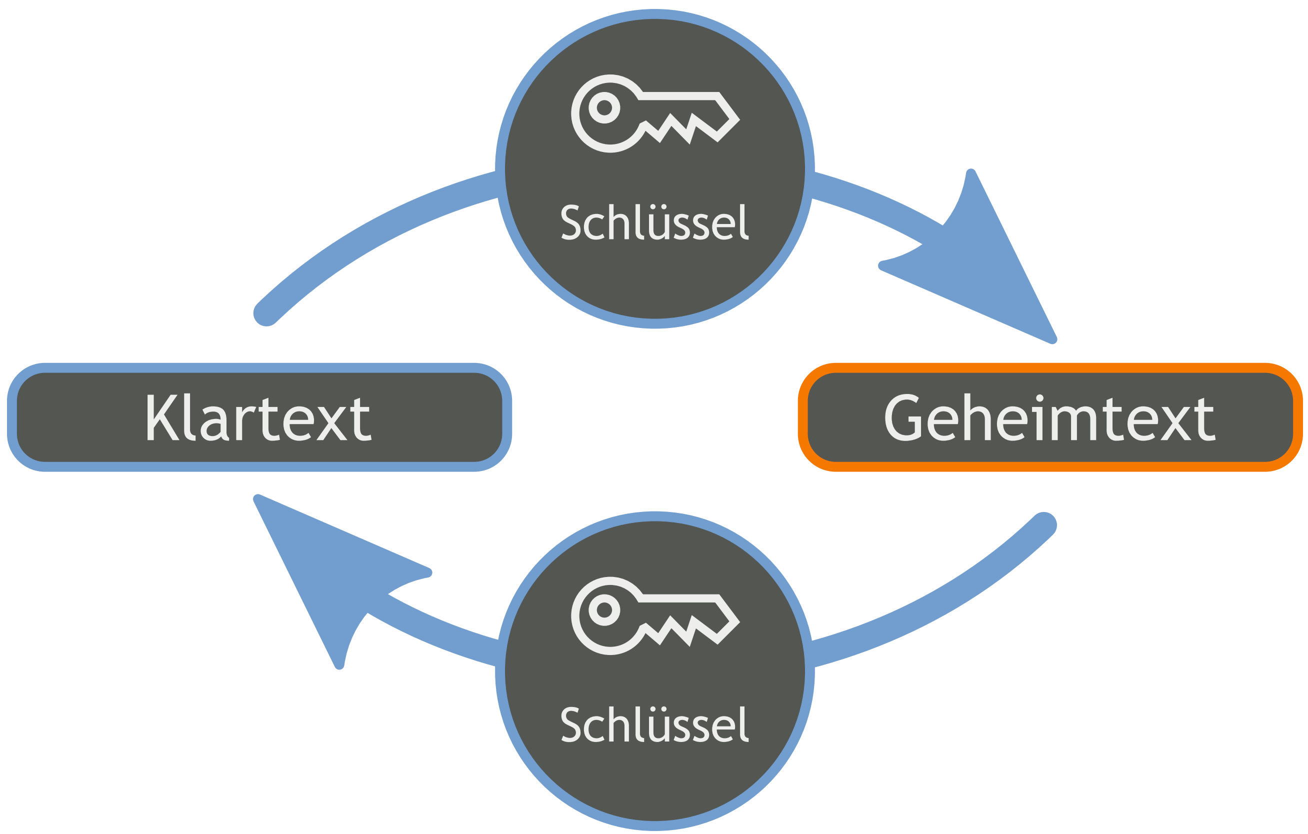
EINSATZ DER BAUSTEINE

ALICE UND BOB



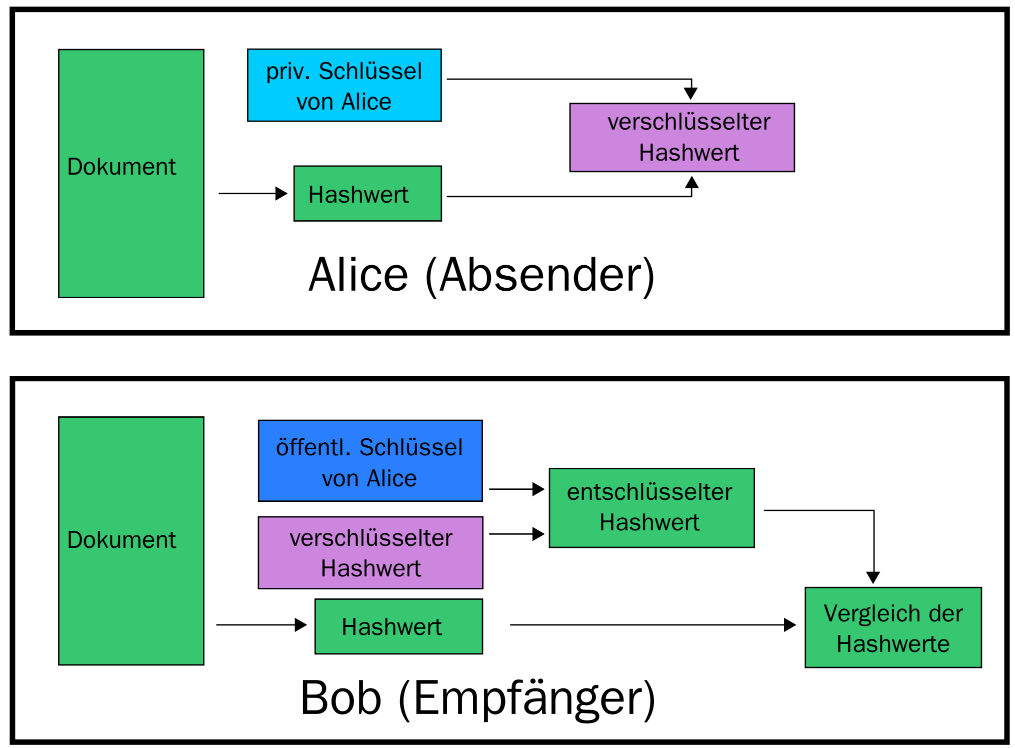
http://cryptocouple.com/

VERSCHLÜSSELN



Bananenfalter, Eigenes Werk (CC0)

SIGNIEREN



Priwo, Schemaskizze Elektronische Signatur (CC BY-SA 3.0)

KRYPTOGRAFIE IN DER PRAXIS

UMFANG

- Transport Verschlüsselung
- Ende-zu-Ende Verschlüsselung

TRANSPORT VERSCHLÜSSELUNG

Schutz der Daten bei der Übetragung

- HTTPS
- TLS
- SSH

ENDE-ZU-ENDE VERSCHLÜSSELUNG

Schutz bis zur endgültigen Verarbeitung

- S/MIME
- GnuPG
- WS-Security


https://

SCHLÜSSEL-MATERIAL

keys-2114366 (CC0 Creative Commons)

key-2114293 (CC0 Creative Commons)

key-2114047 (CC0 Creative Commons)

ZERTIFIKATE

Beglaubigter Public-Key

- self-signed
- eigene CA
- öffentliche CA

Vertrauenswürdige Ausgabestelle von Zertifikaten

approved-1966719 (CC0 Creative Commons)

TRUSTSTORE

Zertifikate vertrauenswürdiger CAs

key-2148476 (CC0 Creative Commons)

VERBINDUNGSAUFBAU

Validierung des Zertifikat

Aushandlung der Verschlüsselung

VALIDIERUNG - SUBJECT

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            03:9a:0f:f3:96:5a:39:62:6f:7c:4e:87:ff:30:c3:42:3b:d4
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3
        Validity
            Not Before: Aug 29 19:14:12 2018 GMT
            Not After : Nov 27 19:14:12 2018 GMT
        Subject: CN = herbstcampus.de
```

```
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                DNS:herbstcampus.de, DNS:www.herbstcampus.de
```

VALIDIERUNG - GÜLTIGKEIT

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            03:9a:0f:f3:96:5a:39:62:6f:7c:4e:87:ff:30:c3:42:3b:d4
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3
        Validity
            Not Before: Aug 29 19:14:12 2018 GMT
            Not After : Nov 27 19:14:12 2018 GMT
        Subject: CN = herbstcampus.de
```

VALIDIERUNG - CHAIN

```
CONNECTED(00000003)
depth=2 O = Digital Signature Trust Co., CN = DST Root CA X3
verify return:1
depth=1 C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3
verify return:1
depth=0 CN = herbstcampus.de
verify return:1
---
Certificate chain
 0 s:/CN=herbstcampus.de
   i:/C=US/O=Let's Encrypt/CN=Let's Encrypt Authority X3
 1 s:/C=US/O=Let's Encrypt/CN=Let's Encrypt Authority X3
   i:/O=Digital Signature Trust Co./CN=DST Root CA X3
---
```

AUSHANDLUNG DER VERSCHLÜSSELUNG

```
DHE-RSA-AES256-AES256
```

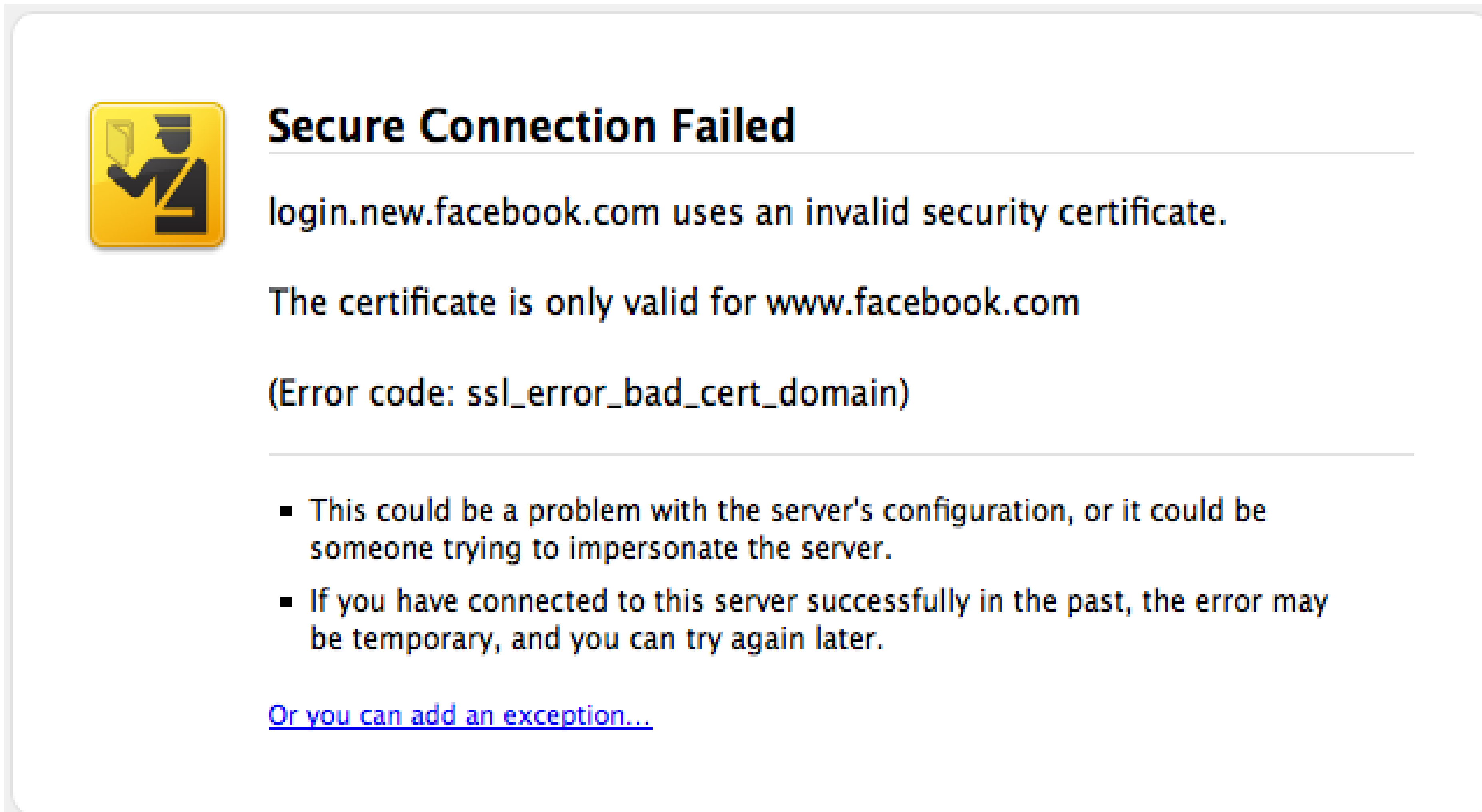
- Wie wird der Session-Key übertragen? - DHE
- Wie wird der Server Authentifiziert? - RSA
- Wie wird verschlüsselt? - AES256
- Wie wird Integrität geprüft? - AES256

DATEIFORMATE

- PEM (OpenSSL)
- PKCS12
- Java Keystore

FEHLERQUELLEN

Subject passt nicht zum Server

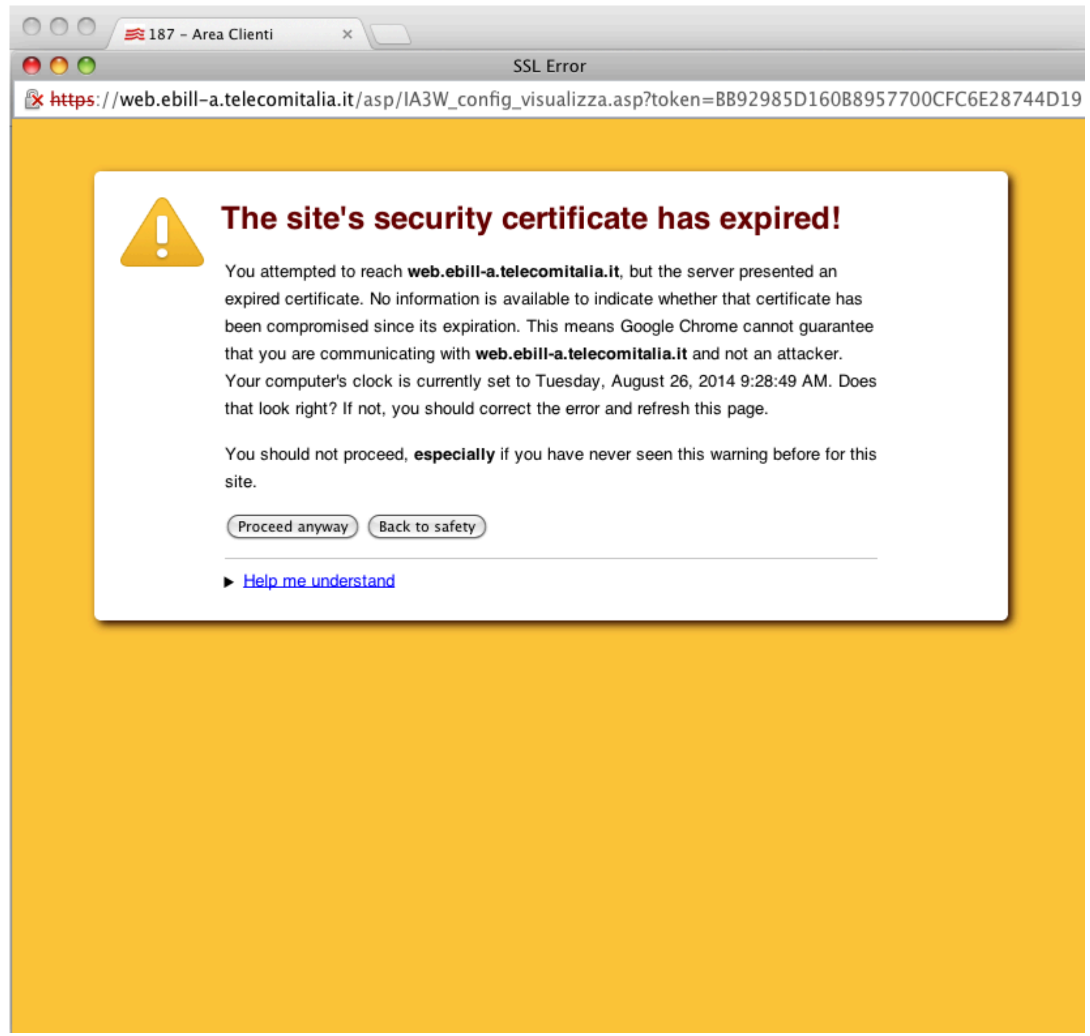


FEHLERHAFTES ZERTIFIKAT

```
Certificate:
    Signature Algorithm: sha256WithRSAEncryption
        Subject: CN = herbstcampus.de
```

```
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                DNS:herbstcampus.de, DNS:www.herbstcampus.de
```

Zertifikat ist abgelaufen

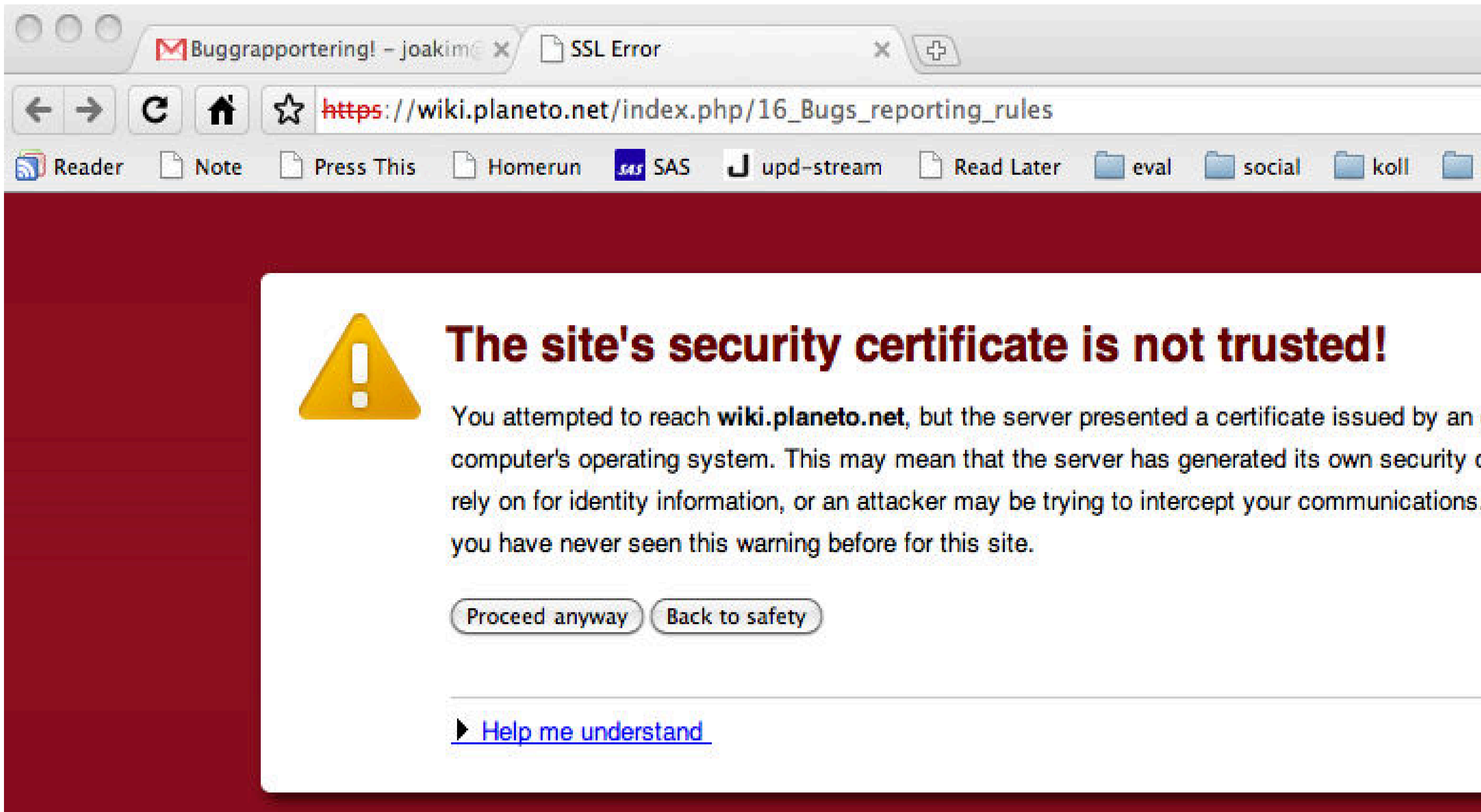


medithIT, Telecom HTTPS insicura (CC BY 2.0)

FEHLERHAFTES ZERTIFIKAT

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            03:9a:0f:f3:96:5a:39:62:6f:7c:4e:87:ff:30:c3:42:3b:d4
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3
        Validity
            Not Before: Aug 29 19:14:12 2018 GMT
            Not After : Sep 01 19:14:12 2018 GMT
        Subject: CN = herbstcampus.de
```

Kein Vertrauen zum Zertifikat

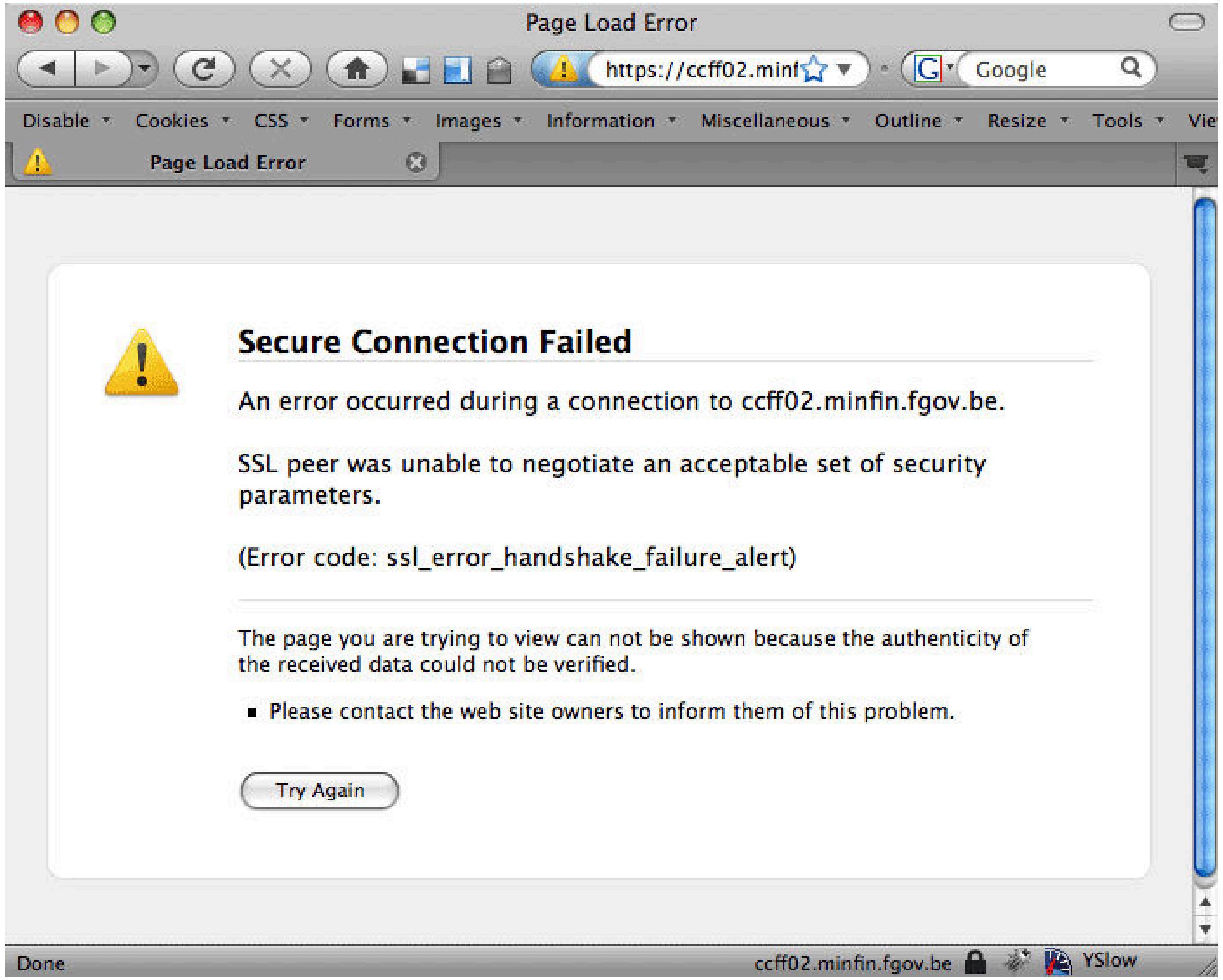


Joakim Jardenberg, SSL Error (CC BY 2.0)

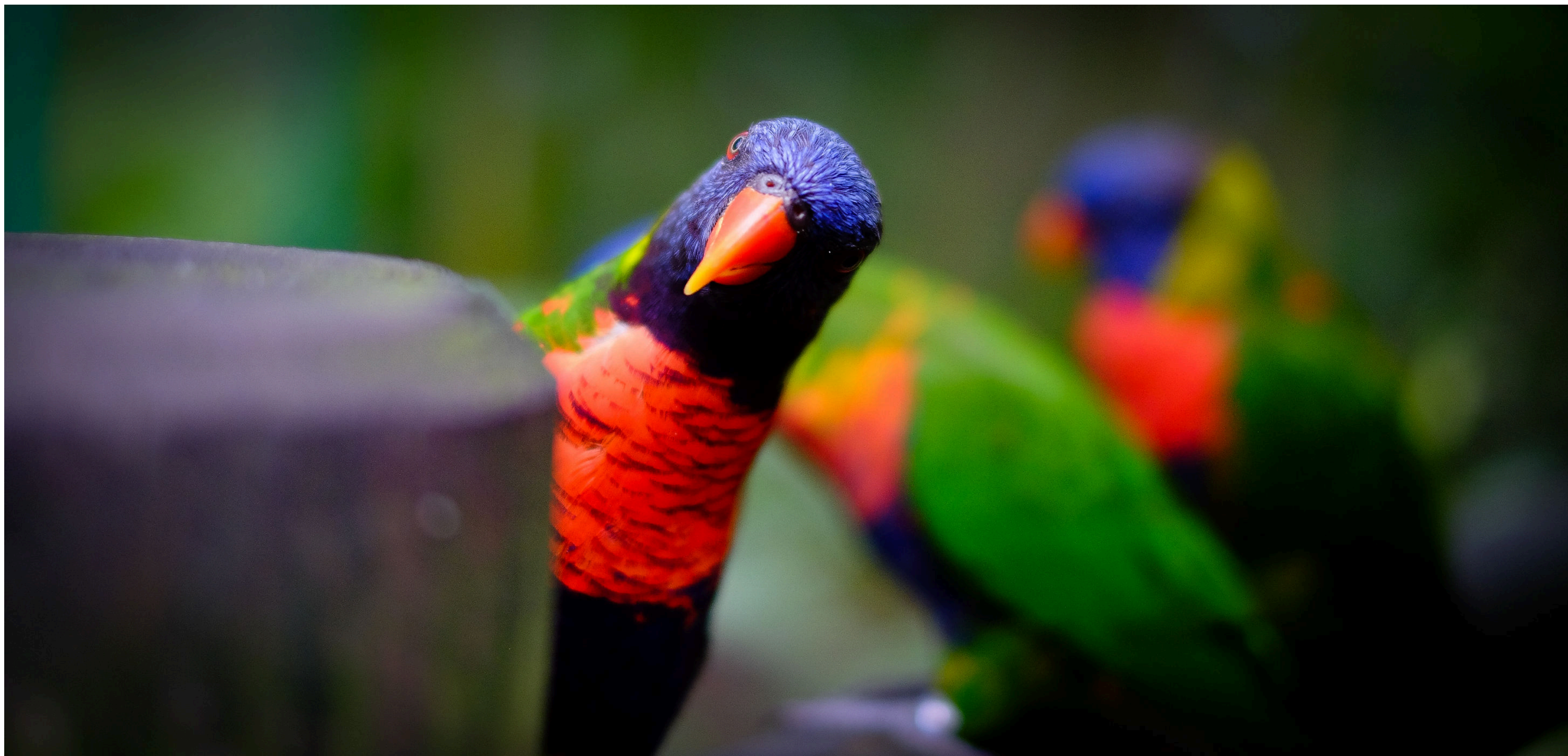
FEHLERHAFTE CHAIN

```
CONNECTED(00000003)
depth=2 O = Digital Signature Trust Co., CN = DST Root CA X3
verify return:1
depth=1 C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3
verify return:1
depth=0 CN = herbstcampus.de
verify return:1
---
Certificate chain
 0 s:/CN=herbstcampus.de
   i:/C=US/O=Let's Encrypt/CN=Let's Encrypt Authority X3
 1 s:/C=US/O=Let's Encrypt/CN=Let's Encrypt Authority X3
   i:/O=Digital Signature Trust Co./CN=DST Root CA X3
---
```

Keine gemeinsamen Ciphers



FRAGEN?



Matthias Ripp, any questions? (CC-BY)