# Verschlüsselung von Emails


## Digitale Selbstverteidigung

Gefahren aus dem Internet

Teil 3

Gunter Bauer
https://cryptoparty.at/graz

30.11.2017



URANIA
Bildung bewegt

# Zwei Begriffe

## Verschlüsselung

- Briefgeheimnis
- Kuvert für Emails
- Vertrauliche Informationen sind nicht einsehbar

## Signatur

- Nachricht stammt sicher vom Sender
- Nachricht wurde nicht verändert

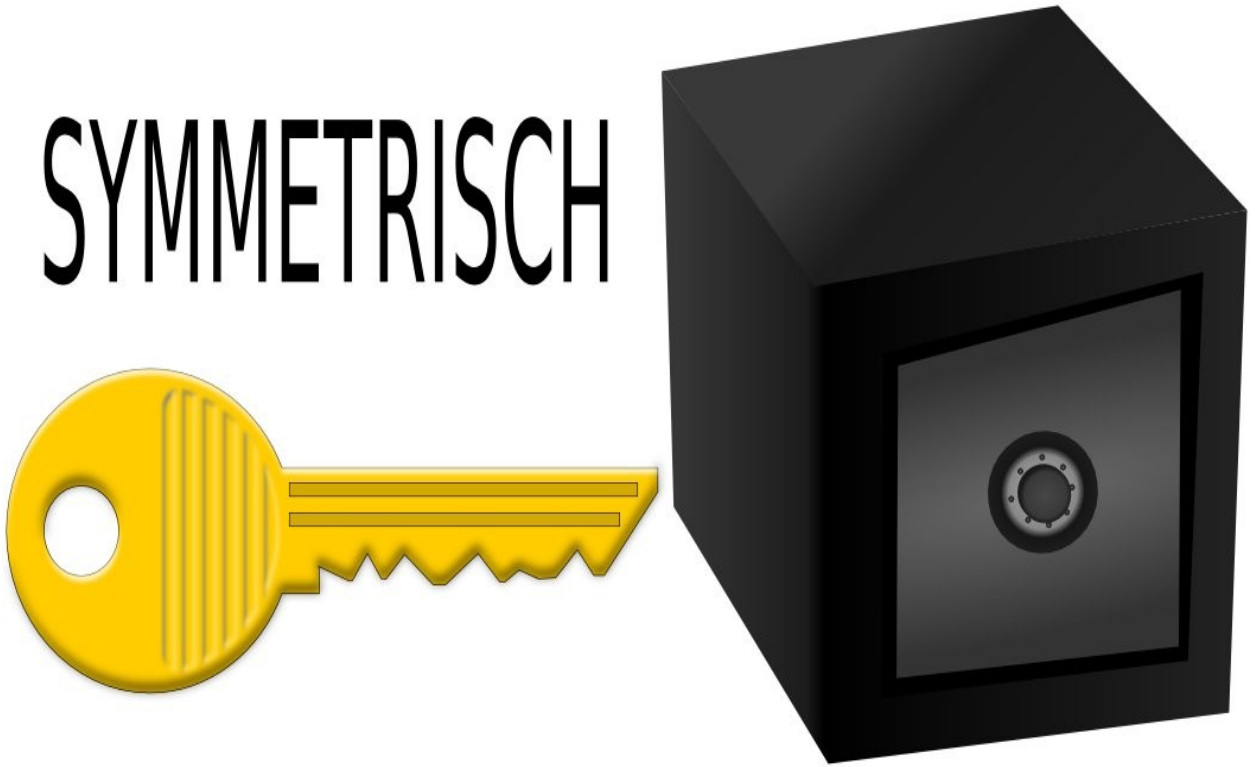
# Warum ist gute Verschlüsselung schwer zu „knacken“?

Das Prinzip der Verschlüsselung beruht auf **Einweg-Funktionen**

Beispiel:

- Multiplikation von 2 Zahlen ist einfach
- Zerlegung des Produkts in Faktoren ist schwierig

# Symmetrische Verschlüsselung

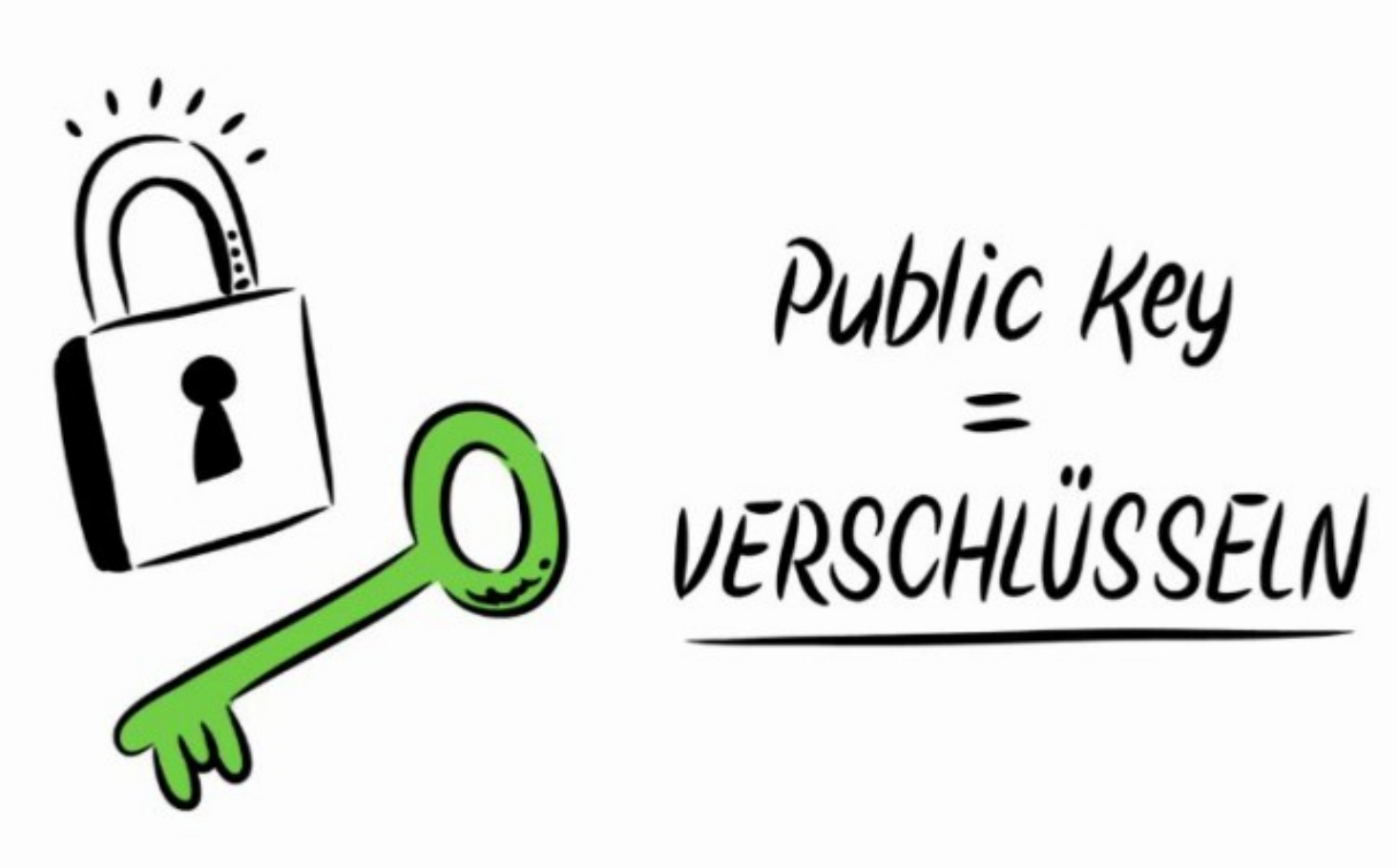


# Asymmetrische Verschlüsselung

- öffentlicher und privater Schlüssel
- **Öffentlicher Schlüssel** kann/soll frei verteilt werden (Webseite, Email, Visitenkarte)
- **Privater Schlüssel** MUSS geheim gehalten werden!

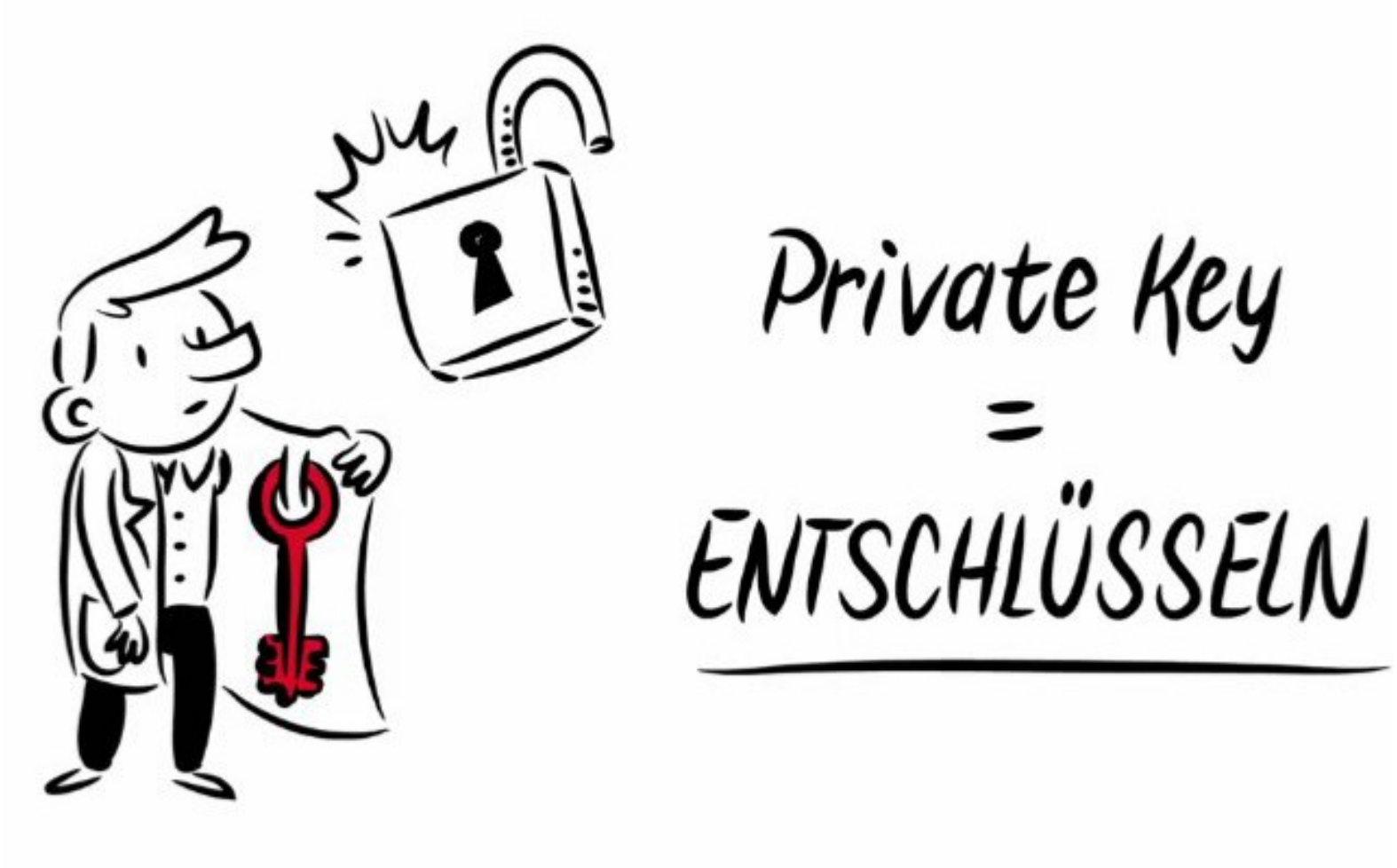
- Signatur möglich
- Verfahren: RSA, Elgamal, ...

# Der öffentliche Schlüssel

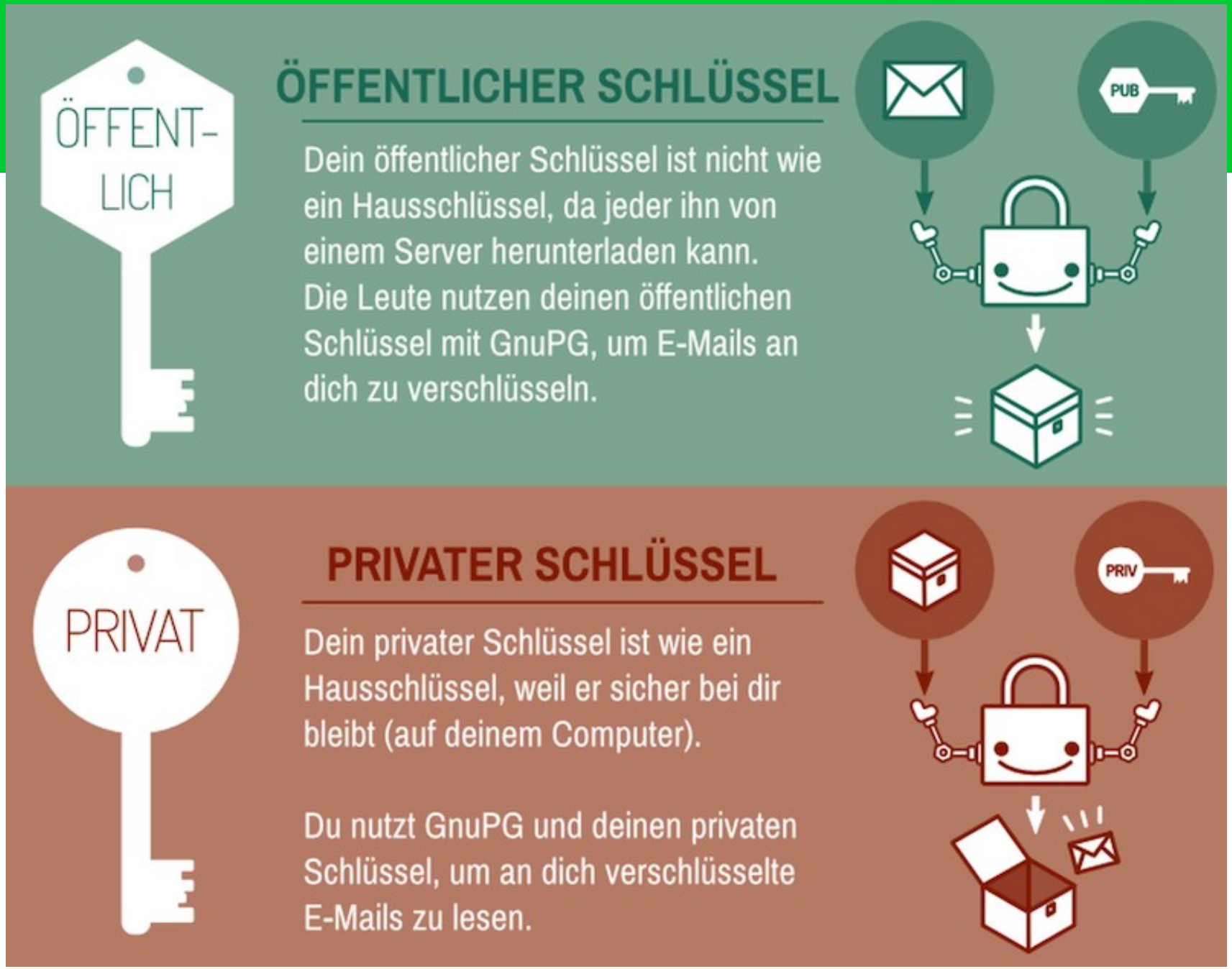



https://mailbox.org/wp-content/uploads/public-key-verschluesseln.png

# Der private Schlüssel



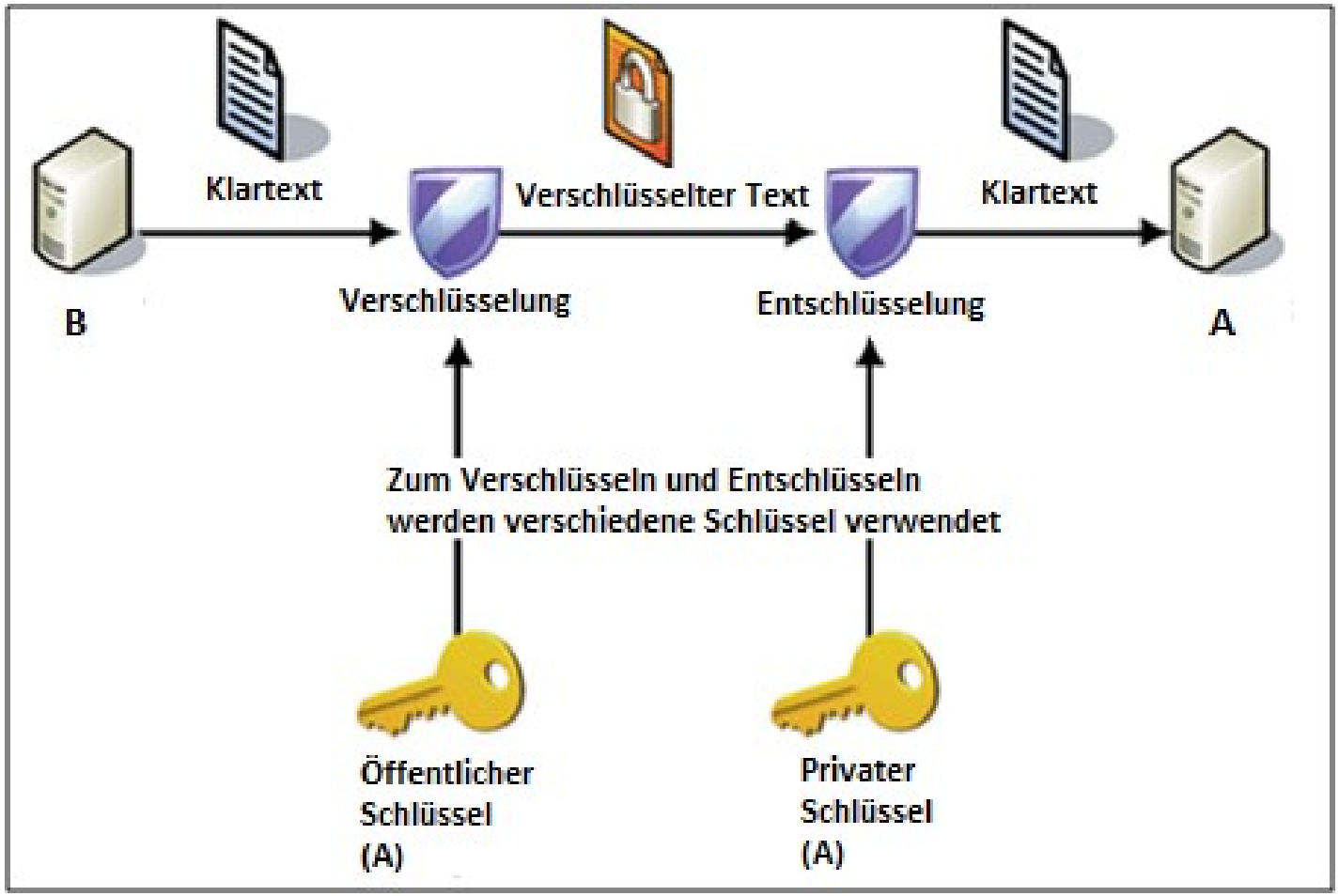

https://mailbox.org/wp-content/uploads/private-key-entschluesseln.png





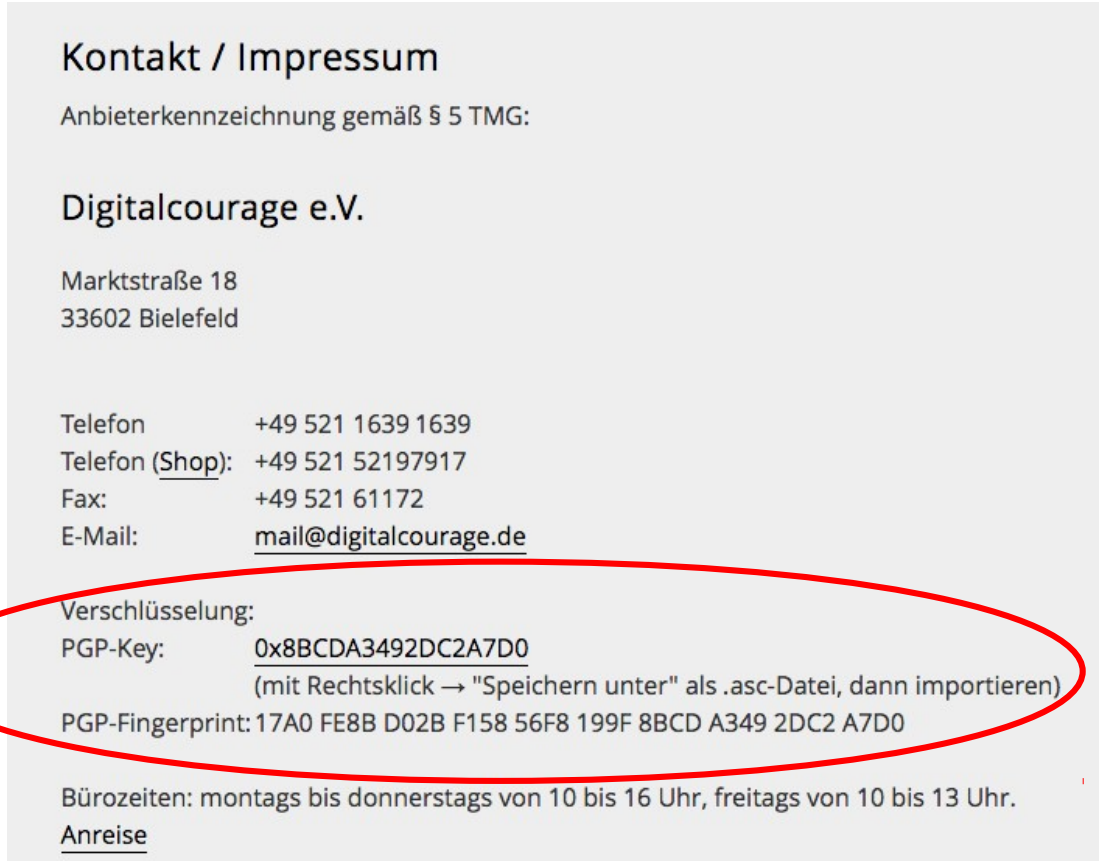

https://emailselfdefense.fsf.org/de/infographic.html

# Versenden einer verschlüsselten Mail




https://dienste.soziologie.uni-muenchen.de/faq-pmwiki/data/emailverschl.png

# Beispiel 1 (für öffentlichen Schlüssel)



## Kontakt / Impressum

Anbieterkennzeichnung gemäß § 5 TMG:

### Digitalcourage e.V.

Marktstraße 18
33602 Bielefeld

Telefon +49 521 1639 1639
Telefon (Shop): +49 521 52197917
Fax: +49 521 61172
E-Mail: mail@digitalcourage.de

Verschlüsselung:
PGP-Key: 0x8BCDA3492DC2A7D0
(mit Rechtsklick → "Speichern unter" als .asc-Datei, dann importieren)
PGP-Fingerprint: 17A0 FE8B D02B F158 56F8 199F 8BCD A349 2DC2 A7D0

Bürozeiten: montags bis donnerstags von 10 bis 16 Uhr, freitags von 10 bis 13 Uhr.
Anreise

https://digitalcourage.de/kontakt

# Beispiel 2 (für öffentlichen Schlüssel)

## Protecting Security Information

Due to the sensitive nature of security information, Apple provides a method for you to:

- Verify the authenticity of security notifications
- Encrypt messages to send to Apple via product-security@apple.com

### 1. Obtain PGP

You can obtain a commercial or free trial version of PGP Desktop from PGP Corporation. Additionally, GnuPG is available as freeware.

### 2. Apple Product Security key

This is our PGP key which is valid until May 15, 2018

Key ID: 0x346CB446
Key Type: RSA
Expires: 5/15/18
Key Size: 4096/4096
Fingerprint: 72E5 F8AE DA11 7B85 FADB 25A5 83A3 EF8C 346C B446
UserID: Apple Product Security

https://support.apple.com/en-us/HT201214

# Beispiel 2

## 2. Apple Product Security key

This is our PGP key which is valid until May 15, 2018

Key ID: 0x346CB446
Key Type: RSA
Expires: 5/15/18
Key Size: 4096/4096
Fingerprint: 72E5 F8AE DA11 7B85 FADB 25A5 83A3 EF8C 346C B446
UserID: Apple Product Security


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG/MacGPG2 v2.0.22 (Darwin)

mQINBFctAtIBEADf5rX+xJMuOcHWoJZY4RPXGC30kUQi8gpGbXs7Pc8maAloX7uL
Ju8I+UMhs5CdaciCom8lYplNgH+6XoI3joVIDXjZblktKuUSnRm29GVvGPB/eGIo
em9wISOwh5lBaOd8px/D11MsvHXoIkLkxkqoAElxsdb2GW9OAw1ciVmx0vQaRbSz
fYNm5ZGK3G5GX0VCIc4JJ1ppjIHAkRGTgX+PGwcUUcbTjqjatbIC6alBphvYBxB4
TSRnvvCK9vOcLa/+NQDajTKpHnAyi/tZZTBmD7uc/pl9R/SXBxKoMpQUpTUgg4pK
9m7YRW9tyQ6UeKg1dpHI6gPhhOT6lk6aR6zAEzyPbq03oYEW1uUY2qKrbPB0bpn5
ygHWns3pQ5/T1GCj9gEZvcg0uXxroOJjwG6uzLJW7aVM1m4Q33ehjYUNxdWPpPfm
kNg5UXVuv9LszV6yADoAo/1Hm78m5/E/I7EgHJNefB1cimz1ZRngtjoMCOAFc+8a
g0NnM/e4NcYr6jFREUSt+lxsR146syXe30UlVxcRrAb5X7iXr6gbYy/2r9hRC3Uz
AvTK8h6oSe3nqVXPf8Oc5aJDVdslfdl3FS9r5Z5v66H+ZJHE+hWqRzTR+KynYiZy
pe9L7hIzCM3ymllMGkCeNP/cbTuoOT2XECrRcjStYswSNEX6Z7CqAi4DfQARAQAB
tGlBcHBsZSBQcm9kdWN0IFNlY3VyaXR5IE5vdGlmaWNhdGlvbnMgKGZvciBzZWN1
cml0eSBhZHZpc29yaWVzKSA8cHJvZHVjdC1zZWN1cml0eS1ub3JlcGx5QGxpc3Rz
LmFwcGxlLmNvbT6JAj0EEwEKACcFAlctA0ECGwMFCQPORIAFCwkIBwMFFQoJCAsF
FgIDAQACHgECF4AACgkQg6PvjDRstEZ7ExAAgFVvzm8Jqvu+Snoq5sBAeqlzAuof
5KSDtIFCyZemUdSQLDLHmjGFDUKllMKVta0udFD/+ara/0JqDhP5kv+XI7DGCk96
Zx5OeWs62qju4xxeDIQYQu6OIEnzpNBsskYG/gK1IaVpOjb7w80OK0sv7RBajrd4
Ct8SjHnCo4iqYoBE/fVMgbmZK0ka9pxBPqUm5eCI4W+Gj4jtk0qZd12zlwE5JpA4
```




URANIA
Bildung bewegt

# E-MAIL-SELBSTVERTEIDIGUNG

Wie konfiguriere ich mein Email-Programm für **Verschlüsselung** ?

Anleitung:

https://emailselfdefense.fsf.org/de/windows.html

**Am besten**: Laptop zu einer Crypto-Party mitbringen.

Wir helfen gerne !

# E-MAIL-SELBSTVERTEIDIGUNG

## #1 INSTALLIERE DIE PROGRAMME

### SCHRITT 1.A

- Konfiguriere dein **E-Mail-Programm** für dein Konto
- https://www.mozilla.org/de/thunderbird/

### SCHRITT 1.B

- Hol dir **GNUPG**, indem du GPG4WIN herunterlädst
- https://www.gpg4win.org/

### SCHRITT 1.C

- Installiere das **ENIGMAIL-PLUGIN** für dein E-Mail-Programm
-

# E-MAIL-SELBSTVERTEIDIGUNG

## #2 ERSTELLE DEINE SCHLÜSSEL

### SCHRITT 2.A

- Erstelle ein Schlüsselpaar

### SCHRITT 2.B

- Lade deinen öffentlichen Schlüssel auf einen Schlüsselserver

# E-MAIL-SELBSTVERTEIDIGUNG

## #3 PROBIER ES AUS!

**SCHRITT 3.A**

- Schicke Edward deinen öffentlichen Schlüssel
- Schreibe die Nachricht an edward-de@fsf.org. Schreibe mindestens ein Wort in den Betreff und in den Text der E-Mail.

**SCHRITT 3.B**

- Sende eine verschlüsselte Test-E-Mail

**WICHTIG:**

- Der Betreff wird nicht verschlüsselt

**SCHRITT 3.C**

- Empfange eine Antwort

# E-MAIL-SELBSTVERTEIDIGUNG

## #4 VERSTEHE DAS WEB OF TRUST

### SCHRITT 4.A

- Signiere einen Schlüssel

### WICHTIG:

- Überprüfe die Identität der Leute, deren Schlüssel du signierst.

# E-MAIL-SELBSTVERTEIDIGUNG

## #5 NUTZE ES RICHTIG

- Wann soll ich verschlüsseln ?

**WICHTIG:**

- Nimm dich vor ungültigen Schlüsseln in Acht
- Speichere dein Widerrufszertifikat an einem sicheren Ort
- Reagiere schnell, wenn jemand deinen privaten Schlüssel bekommt
- Mache deinen öffentlichen Schlüssel zu einem Teil deiner Online-Identität

https://www.reddoxx.com/wp-content/uploads/Infografik-E-Mailverschl%C3%BCsselung-mit-PGP.jpg

# PGP

(Pretty Good Privacy)


✔ Alice E-Mail ist vor dem Mitlesen Dritter geschützt.

# Alice Bob


Beide haben einen **öffentlichen**
und einen **privaten Schlüssel**

# Schlüsseltausch


Alice & Bob tauschen
ihre öffentlichen Schlüssel.

# Verschlüsselung


Alice verschlüsselt ihre E-Mail
mit Bobs öffentlichem Schlüssel.

# Mail-Versand


Danach sendet Alice die verschlüsselte E-Mail an Bob.

# Entschlüsselung


Bob entschlüsselt die E-Mail mit seinem privaten Schlüssel.