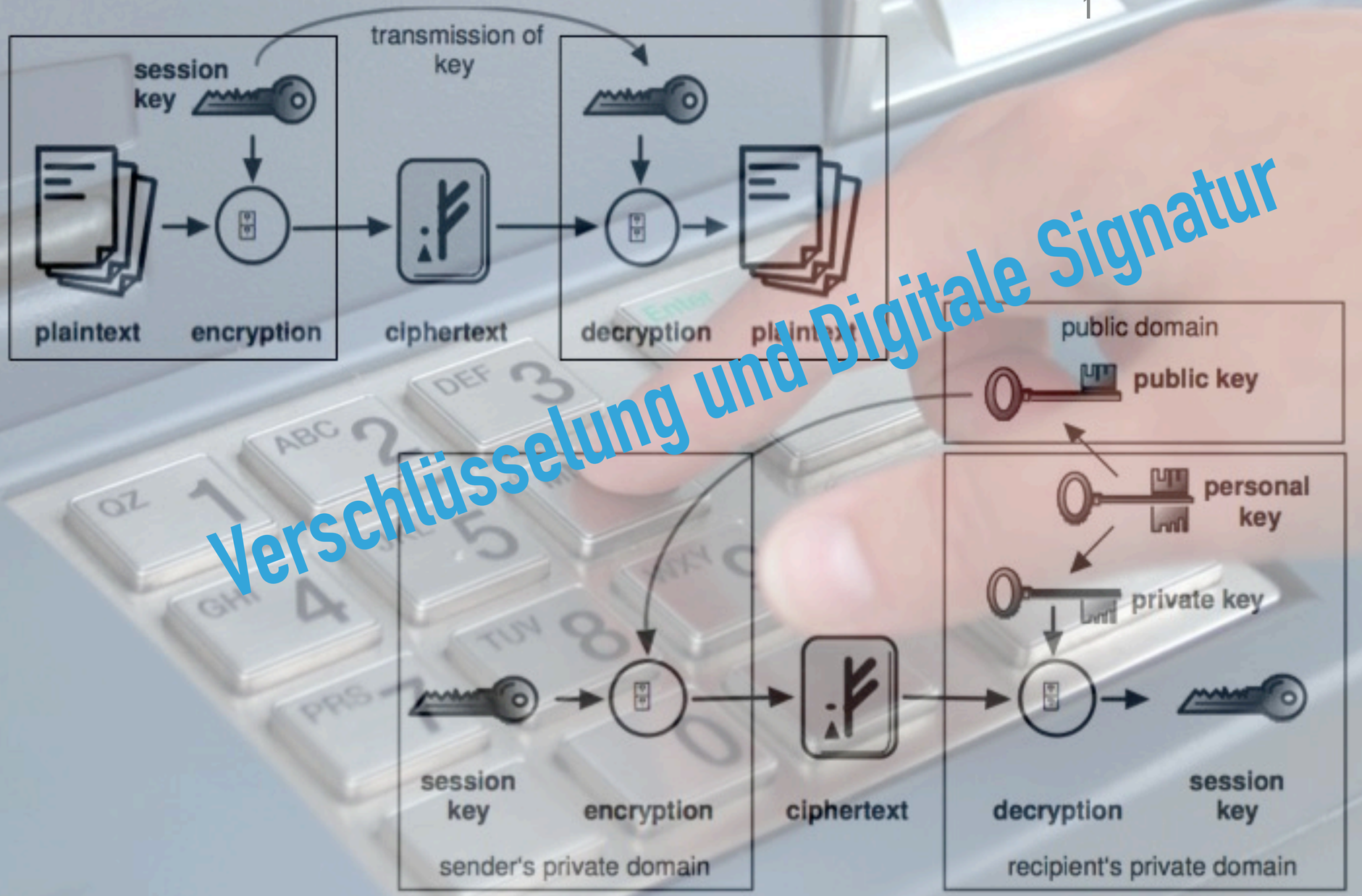
TecDay, 26. März 2019

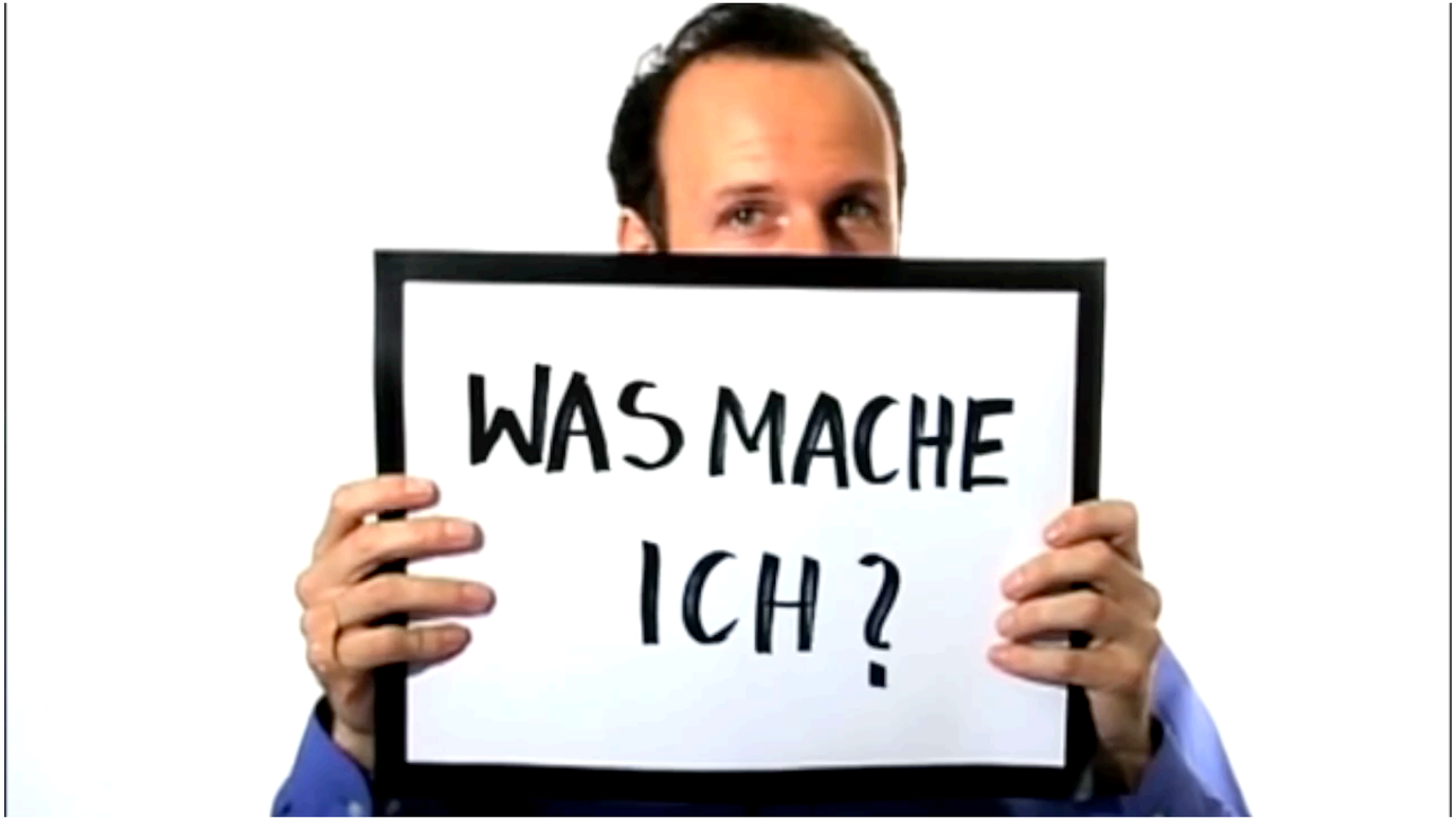
Bruno Wenk

Verschlüsselung und Digitale Signatur



Streng geheim!

- Verheiratet mit Doris Wenk-Keller
- Vater von Rahel, Jonas, Rea Selina und Luisa
- Grossvater von Awa Arjen Joscha, Zoé Laetizia und Valérie
- Dipl.El.-Ing. ETH Zürich (1978)
- Tätigkeit als Elektroingenieur in Forschung und Entwicklung an zwei Hochschulen und in mehreren unterschiedlichen Unternehmen
- Professor em. für Multimedia-Kommunikationssysteme an der HTW Chur (1990 - 2018)



Quelle: https://www.youtube.com/watch?v=q5ymi1ehypU

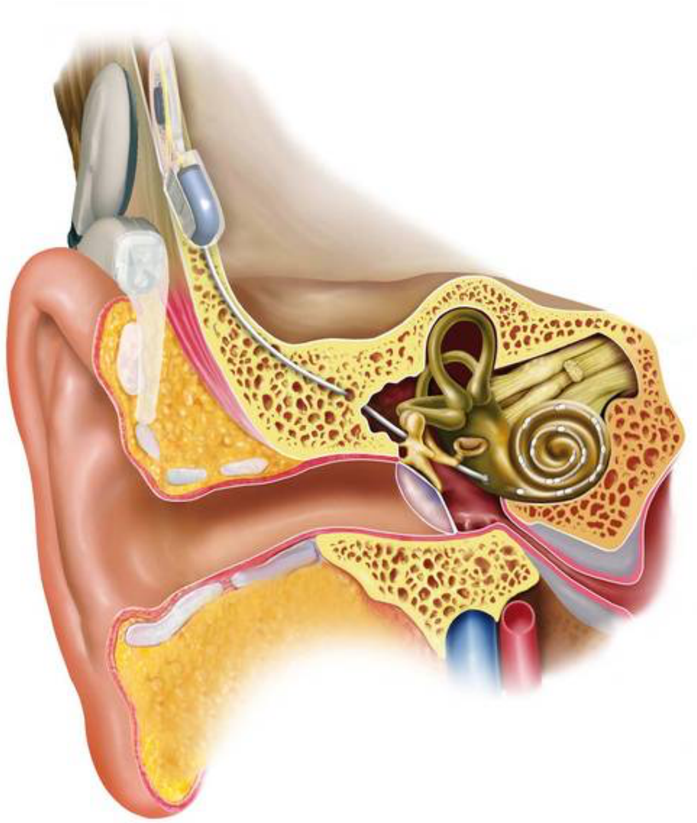
Ingenieurinnen und Ingenieure führen Forschungs- und Entwicklungsprojekte durch und lösen dabei Probleme …

… in Disziplinen wie z.B. :

- Informatik
- Bauwesen
- Elektrotechnik
- Energietechnik
- Maschinenbau
- Fahrzeugtechnik
- Medizintechnik
- Raumfahrt
- Automatisierungstechnik
- Fertigung und Produktion
- Umwelttechnik
- Wirtschaftsingenieurwesen

Cochlea-Implantat

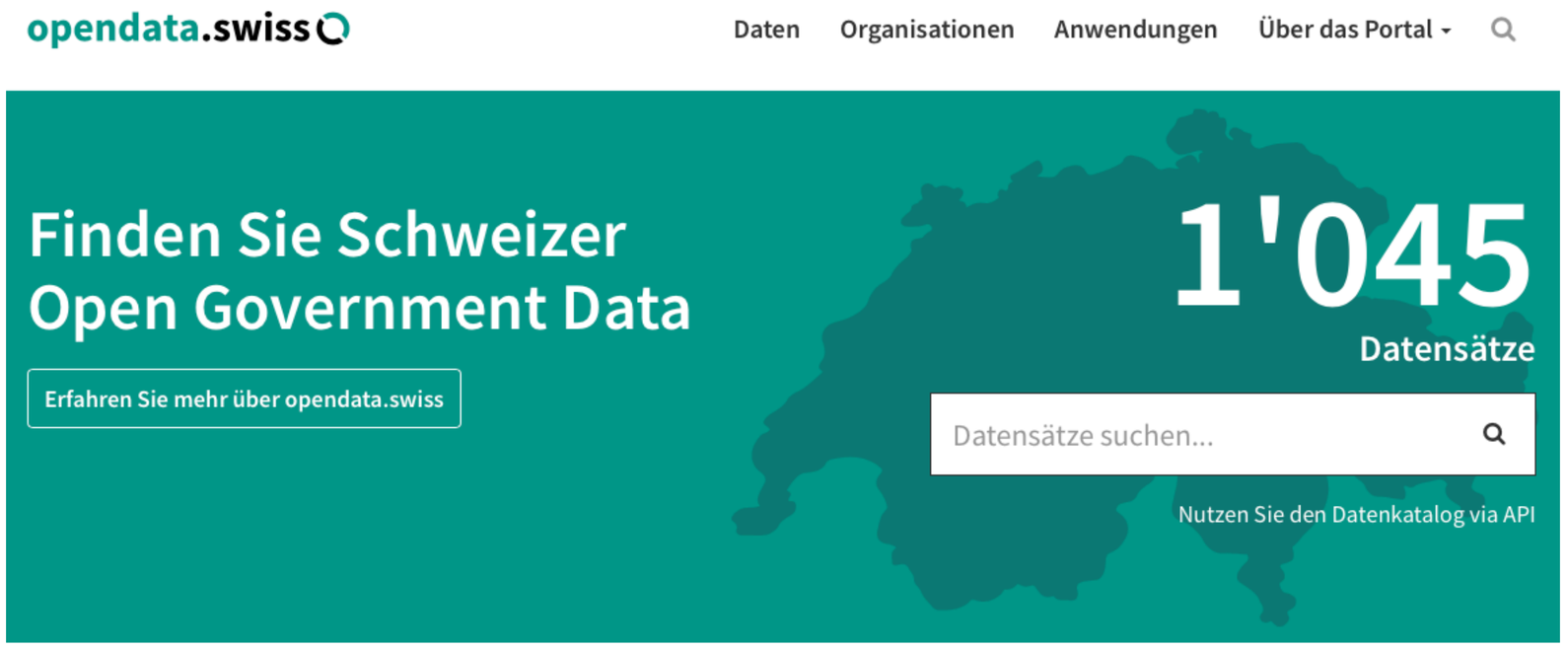
1982



Quelle:
http://www.medizin.uni-halle.de/typo3temp/pics/bac54c4fe1.jpg

Fahrgast-Informationssystem der Rhätischen Bahn (RhB)

Schweizer Plattform für offene Verwaltungs-Daten



Kategorien

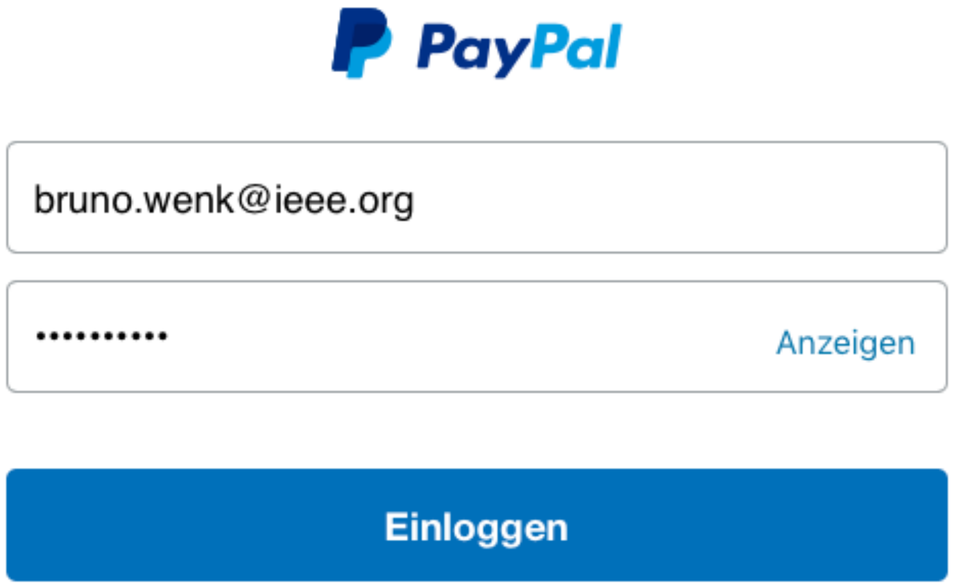
Arbeit, Erwerb 111
Bau- und Wohnungswesen 54
Bevölkerung 108
Bildung, Wissenschaft 57
Gesundheit 43
Handel 1
Industrie, Dienstleistungen 20
Kriminalität, Strafrecht 18
Politik 133
Preise 6
Raum und Umwelt 266
Soziale Sicherheit 38

Was ist eine digitale Signatur?

Wie funktioniert Verschlüsselung?

Wie sicher sind unsere Passwörter?

Passwörter dienen dazu, persönliche Bereiche
im Web gegen unbefugten Zugriff zu schützen
(z.B. E-Banking Konto, E-Mail Konto,
Social Media Plattformen).



Der Benutzername ist meist bekannt.

Schutz vor unerlaubtem Zugriff bietet nur das Passwort.

Welche Bedingungen muss ein Passwort mindestens erfüllen, damit der Schutz vor unerlaubtem Zugriff genügend gross ist?

Bedingungen

- Komplexes, nicht einfach zu erratendes Passwort
- Enthält Gross- und Kleinbuchstaben und Ziffern
- Umfasst mindestens 8 Zeichen
- Immer wieder wechselndes Passwort

} **Warum ?**

James Bond 007 - On Her Majesty’s Secret Service (1969)

Quelle: https://www.youtube.com/watch?v=ctxpzf5-XuU

Nehmen wir an, ich hätte als Passwort nur eine Zahl mit 4 Grossbuchstaben (z.B. AZWU oder FYYR).

Wie viele Versuche müssten Sie maximal durchführen, bis Sie mein PayPal-Konto „geknackt“ hätten?

A
B
C
D
.
.
X
Y
Z

26

AA, AB, AC, . . . , AY, AZ
BA, BB, BC, . . . , BY, BZ
CA, CB, CC, . . . , CY, CZ
DA, DB, DC, . . . , DY, DZ
. . .
. . .
XA, XB, XC, . . . , XY, XZ
YA, YB, YC, . . . , YY, YZ
ZA, ZB, ZC, . . . , ZY, ZZ

$26 \times 26 = 26^2$

AAA, AAB, AAC, . . . , AAY, AAZ
ABA, ABB, ABC, . . . , ABY, ABZ
. .
AZA, AZB, AZC, . . . , AZY, AZZ

BAA, BAB, BAC, . . . , BAY, BAZ
BBA, BBB, BBC, . . . , BBY, BBZ
. .
BZA, BZB, BZC, . . . , BZY, BZZ

ZAA, ZAB, ZAC, . . . , ZAY, ZAZ
ZBA, ZBB, ZBC, . . . , ZBY, ZBZ
. .
ZZA, ZZB, ZZC, . . . , ZZY, ZZZ

$26^2 \times 26 = 26^3$

Anzahl Passwörter

26 verschiedene Zeichen

Passwort mit 1 Stelle → 26^1 Passwörter

Passwort mit 2 Stellen → 26^2 Passwörter

Passwort mit 3 Stellen → 26^3 Passwörter

Passwort mit 4 Stellen → 26^4 Passwörter

n verschiedene Zeichen

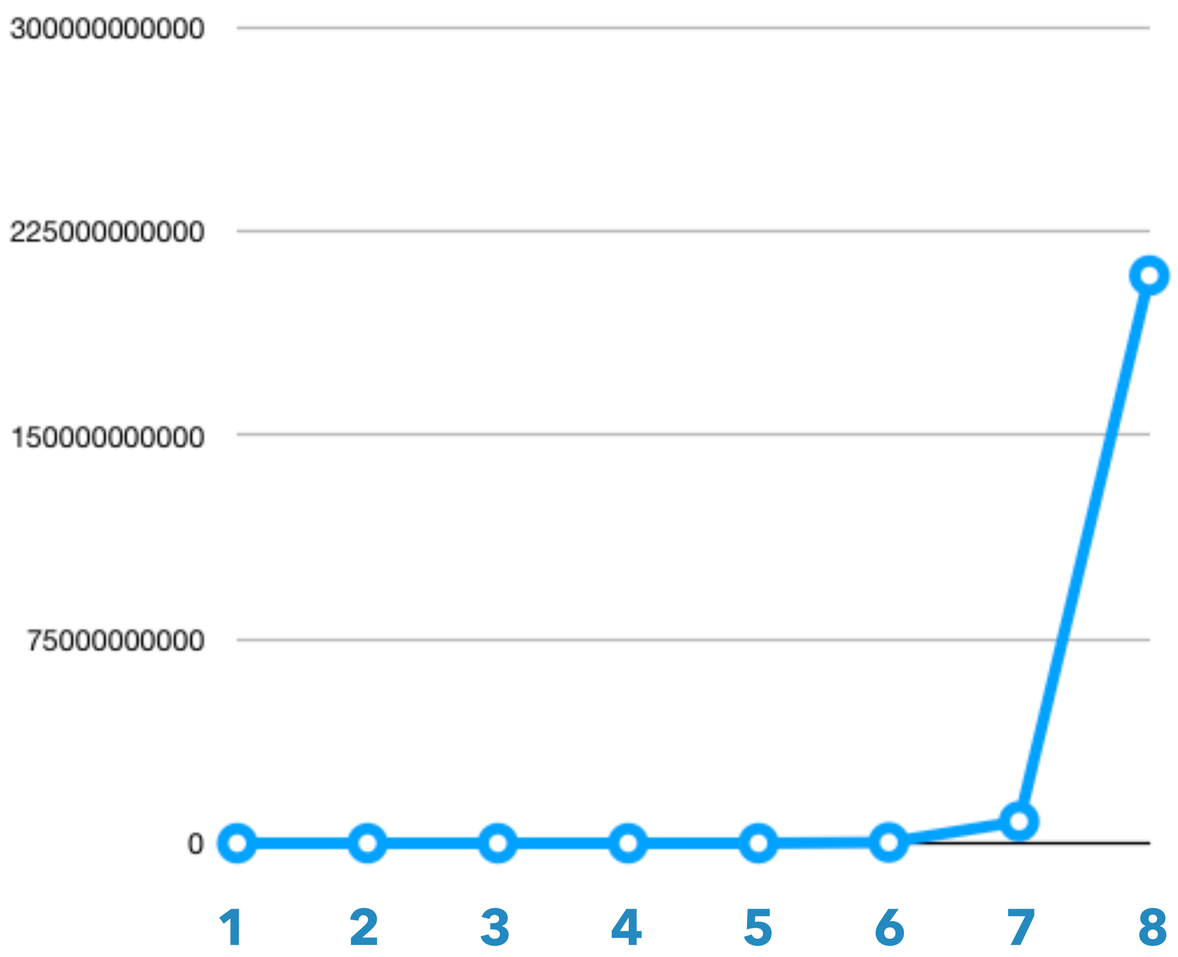
Passwort mit **k** Stellen → $\mathbf{n^k}$ Passwörter

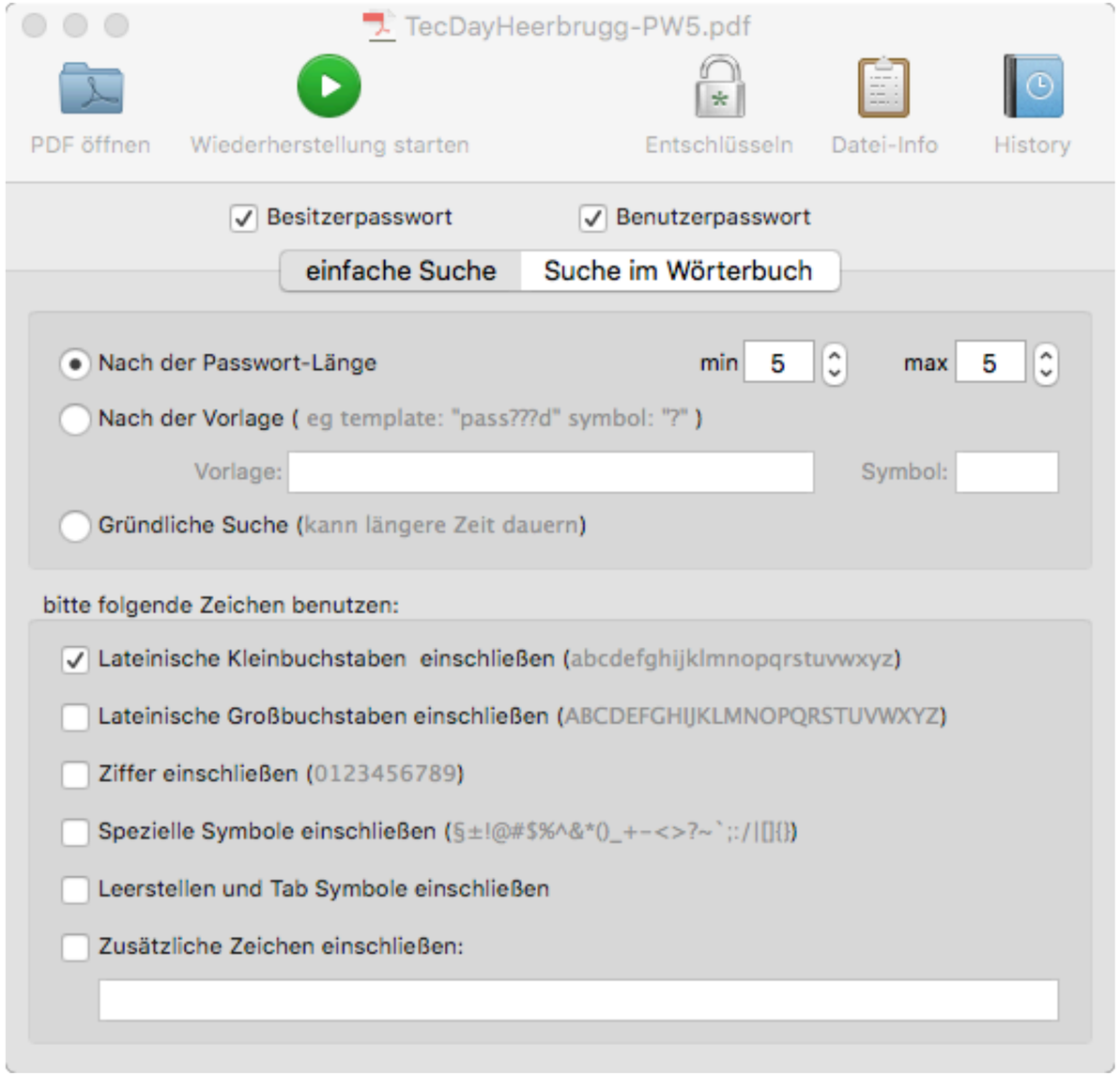
Anzahl Variationen von k Symbolen aus einer Menge von n Symbolen (mit Wiederholung) -> n^k

26 verschiedene Zeichen

Passwort mit 1 Stelle	→	26 Passwörter
Passwort mit 2 Stellen	→	676 Passwörter
Passwort mit 3 Stellen	→	17’576 Passwörter
Passwort mit 4 Stellen	→	456’976 Passwörter
Passwort mit 5 Stellen	→	ca. 12 Millionen Passwörter
Passwort mit 6 Stellen	→	ca. 309 Millionen Passwörter
Passwort mit 7 Stellen	→	ca. 8 Milliarden Passwörter
Passwort mit 8 Stellen	→	ca. 209 Milliarden Passwörter

Anzahl Passwörter in Funktion der Länge





Passwort-Länge:

k = 5

Anzahl möglicher Zeichen:

n = 26 (A, B, C, D, … , X, Y, Z)

Anzahl möglicher Passwörter:

ca. 12 Millionen

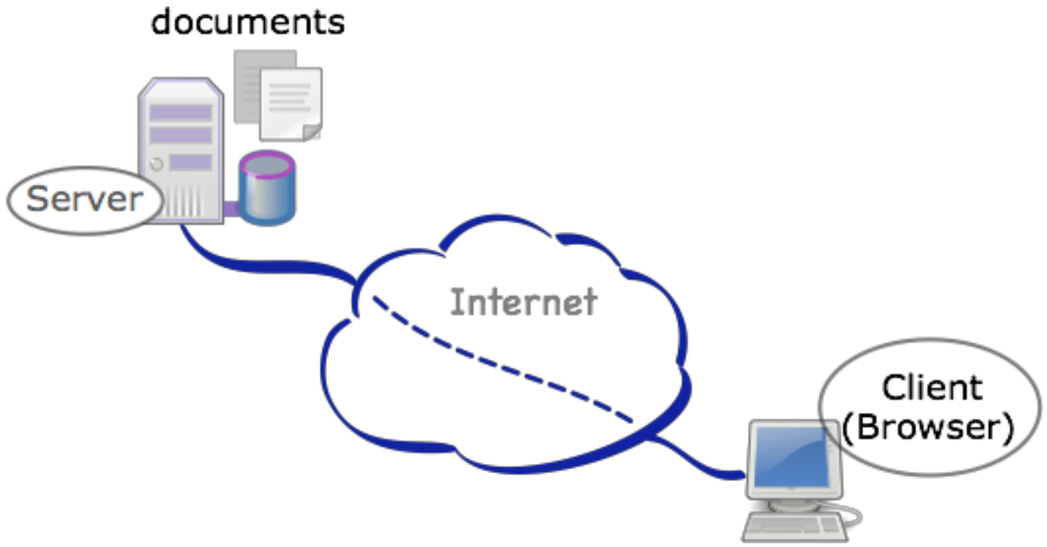
Geprüfte Passwörter pro Sekunde:

ca. 25 Tausend

Passwort gefunden nach:

48 Sekunden

Lange komplexe Passwörter kann man auch mit heutigen Computern nicht in nützlicher Frist „knacken“.



Aber „Hacker“ könnten die Passwörter auf dem Server (z.B. von PayPal) entdecken, stehlen und ev. sogar veröffentlichen.

E-Mail-Adresse bruno.wenk@fh-htwchur.ch

Betroffener Dienst	Datum	Verifiziert	Betroffene Nutzer	Passwort	Vor- und Zuname	Geburtsdatum	Anschrift	Telefonnummer	Kreditkarte
Unknown (Collection #1-#5)	Jan. 2019		2.191.498.885	Betroffen	–	–	–	–	–
	Dieser Datensatz wurde im Januar 2019 veröffentlicht und enthält riesige Listen von Zugangsdaten unbekannter Herkunft, ältere Leaks und kleinere Datenbankabzüge.								
Onliner Spambot (Spamlist)	Aug. 2017		128.471.704	–	–	–	–	–	–
Unknown (Anti-Public Combolist)	Dez. 2016		541.567.187	Betroffen	–	–	–	–	–
adobe.com	Okt. 2013	✓	152.375.851	Betroffen	–	–	–	–	–
last.fm	Jun. 2012	✓	39.329.766	Betroffen	–	–	–	–	–
linkedin.com	Jun. 2012	✓	160.144.040	Betroffen	–	–	–	–	–

Prüfung auf der Webseite https://sec.hpi.uni-potsdam.de/ilc/search?lang=de

Anstatt Passwort im Klartext nur dessen Hash-Wert speichern!

Hash-Wert = Eindeutige Abbildung eines Textes auf einen Zahlenwert

Beispiel-Algorithmus:

ASCII-Codes der Zeichen des Textes addieren und Summe ganzzahlig durch 113 dividieren; der Rest ist der Hash-Wert

h 8 L L o

104 + 56 + 76 + 76 + 111 = 423 | 423 : 113 = 3 Rest 84

Wenn der gespeicherte Hash-Wert eines Passworts den Wert 12 hat, kann dann das Passwort „Ry2b“ lauten?

(Voraussetzung: Beispiel-Algorithmus)

(ASCII-Codes der Zeichen des Textes addieren und Summe ganzzahlig durch 113 dividieren; der Rest ist der Hash-Wert)

Quelle: http://www.hr.ubc.ca/hr-networks/2017/10/october-is-cyber-security-awareness-month/

Ein Hash-Wert für ein ganzes Dokument (z.B. eine E-Mail-Nachricht oder ein Tabellenkalkulation-Blatt) gewährleistet dessen Integrität.

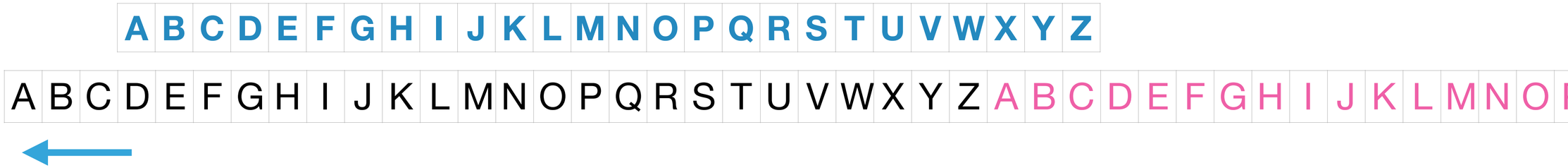
Das heisst: Der Empfänger kann prüfen, ob das empfangene Dokument dem gesendeten entspricht oder nicht.

Aber der Inhalt des Dokuments ist dabei auch für Unbefugte lesbar!

Um den Inhalt nur dem rechtmässigen Empfänger zugänglich zu machen, muss es verschlüsselt werden.

GDV VFKÖQVWH, ZDV ZLU HUOHEHQ NÖQQHQ, LVW GDV JHKHLPQLVYROOH.

(DOEHUW HLQVWHLQ)



Schlüssel = 3

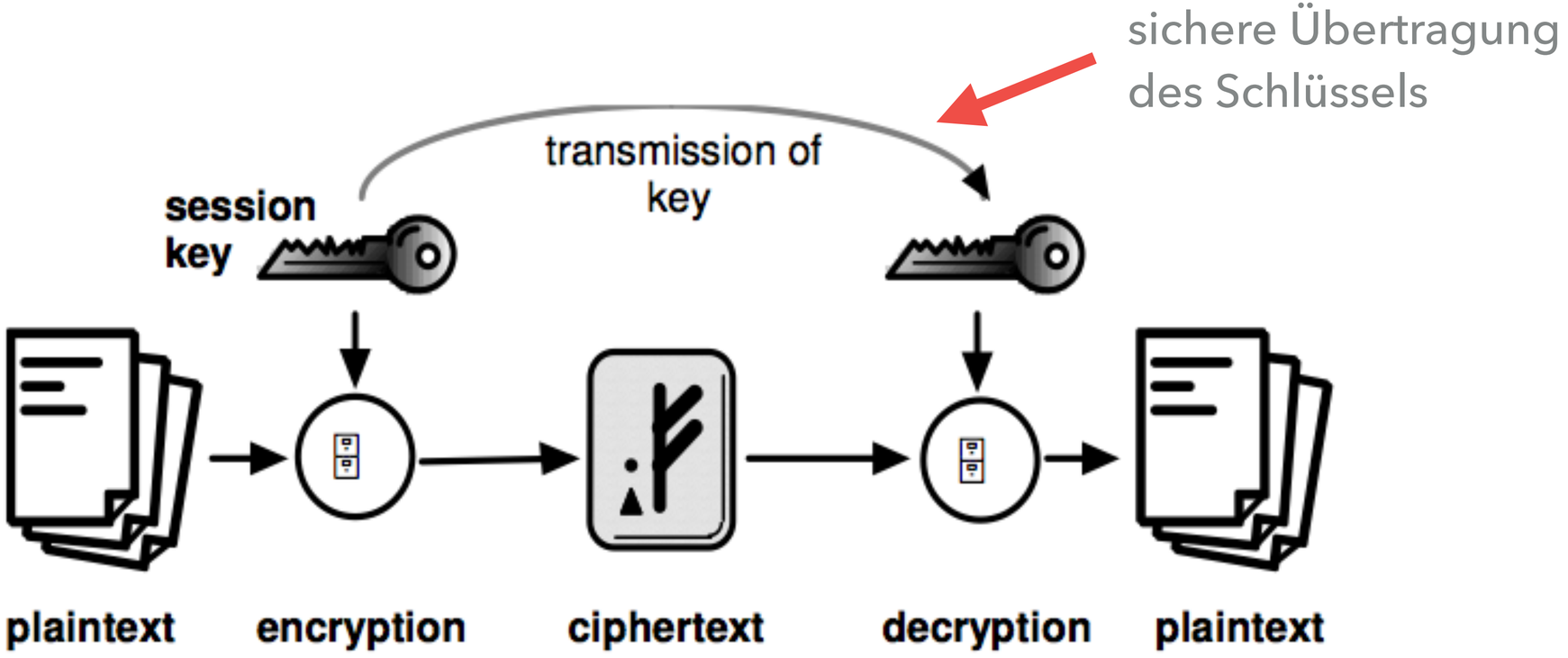
Das Schönste, was wir erleben können, ist das Geheimnisvolle. (Albert Einstein)

Online-Tool: https://www.cryptool.org/de/cto-chiffren/caesar

Caesar-Chiffre „knacken“

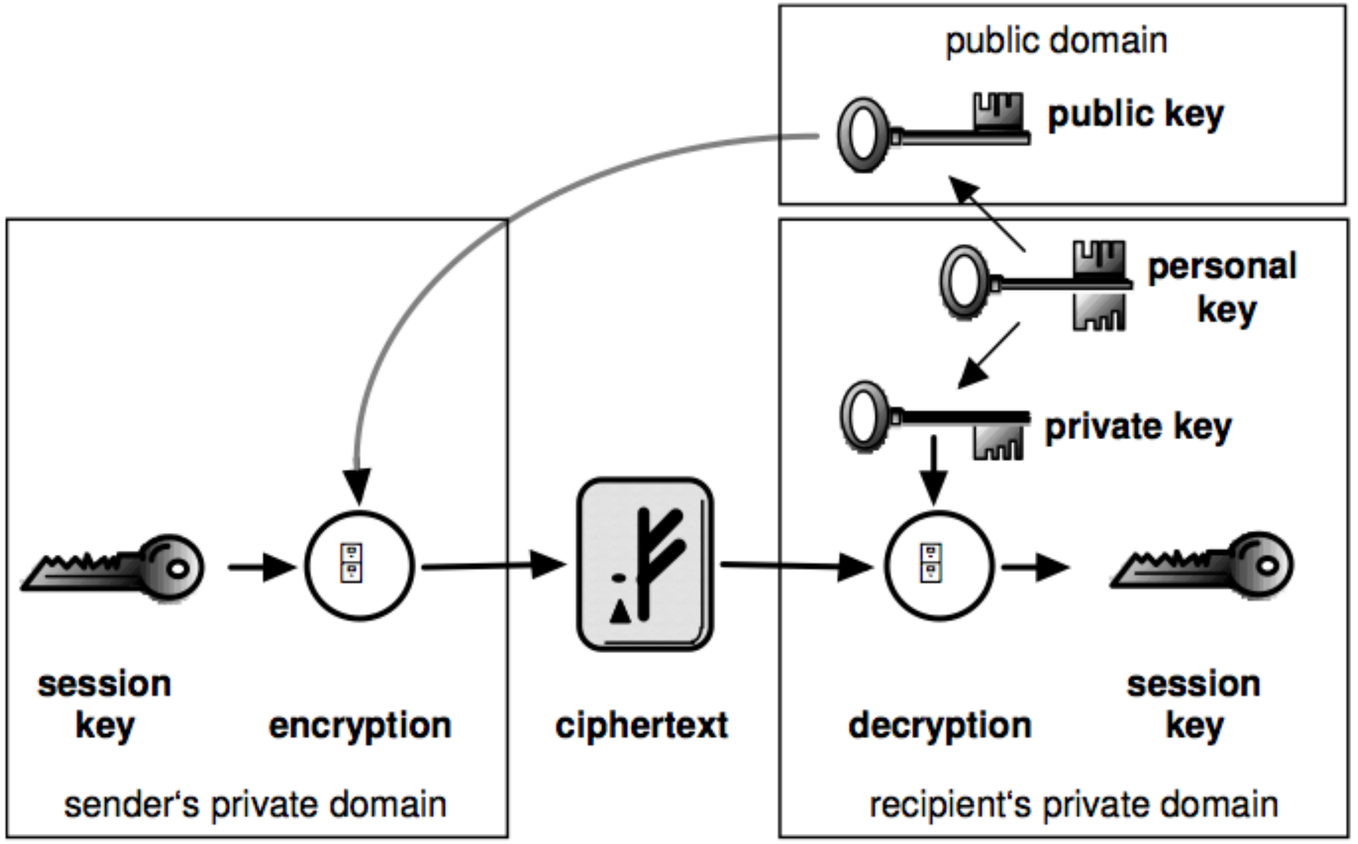
- Brute Force → maximal 26 Versuche
- Analyse der Buchstaben-Häufigkeit → 2 bis 3 Versuche
  (z.B. https://de.wikipedia.org/wiki/Buchstabenhäufigkeit)

Grundsätzliches Problem von symmetrischen Verschlüsselungs-Verfahren



HTTPS - HyperText Transfer Protocol Secure

Quelle: http://thehackernews.com/2012/09/crime-new-ssltls-attack-for-hijacking.html



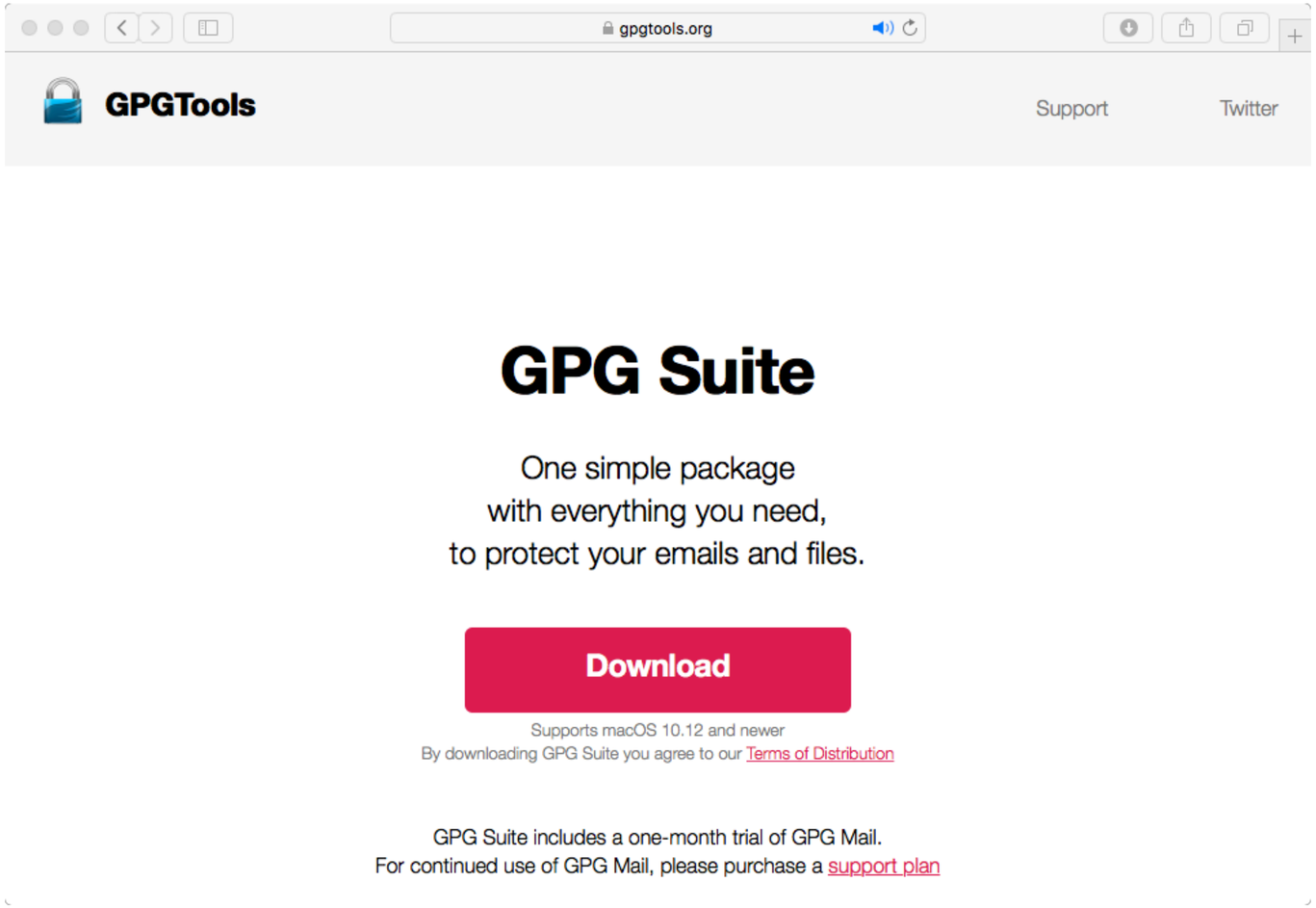
Schlüsselpaar → Public Key / Private Key

Schreiben Sie mir eine (kurze) Nachricht und verschlüsseln Sie diese mit meinem „Public Key“.

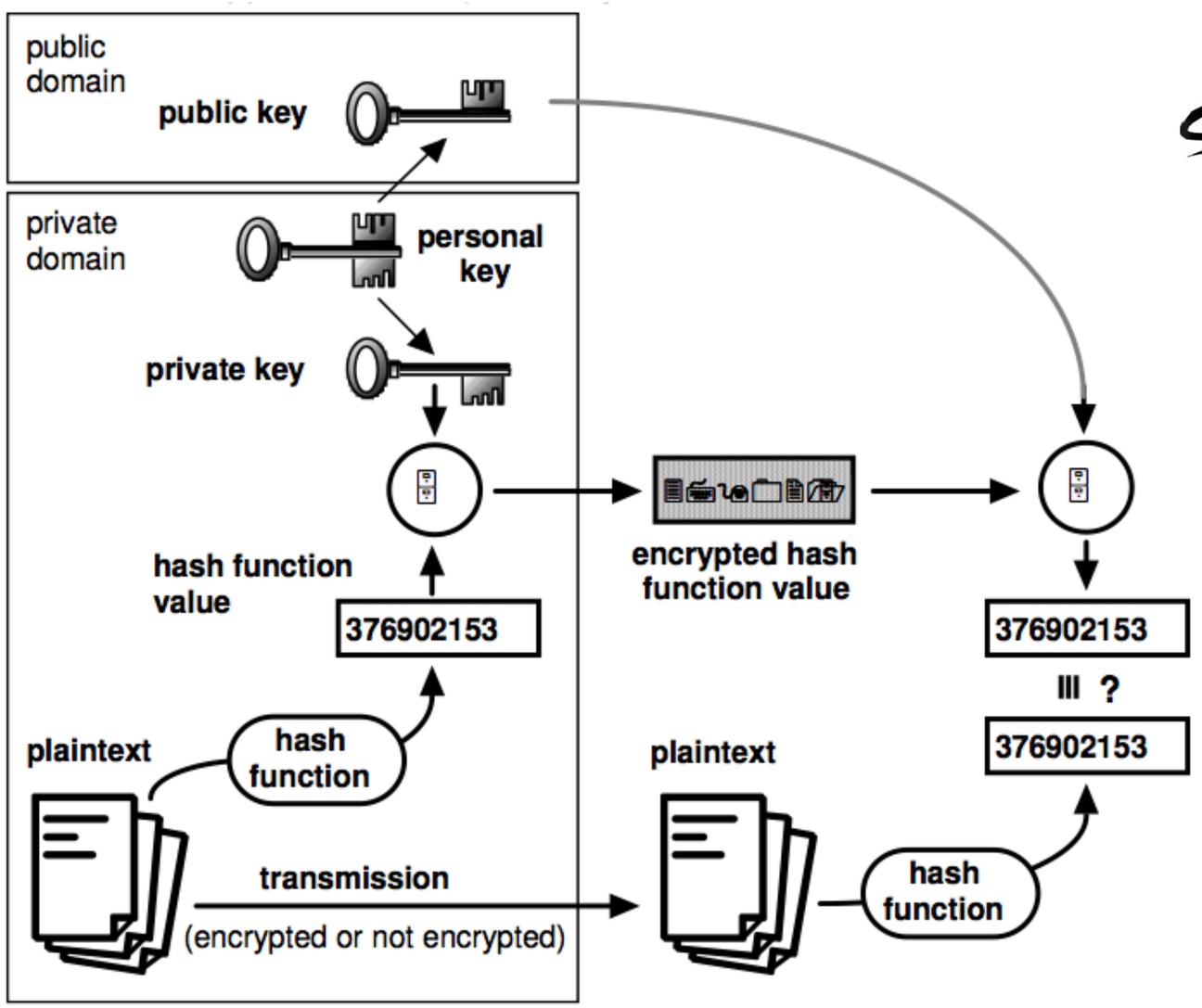
Public Key Table

Zeichen	zugeordnete Codes				
0	0062	0176	0174	0188	0199
1	0002	0005	0026	0082	0092
2	0013	0022	0053	0084	0156
3	0025	0045	0168	0115	0099
4	0121	0123	0131	0159	0201
5	0034	0042	0052	0211	0218

Wir prüfen danach, ob die verschlüsselte Nachricht auch mit dem „Public Key“ entschlüsselt werden kann.



https://gpgtools.org


public domain
public key
private domain
personal key
private key
hash function value
376902153
encrypted hash function value
376902153
III ?
376902153
plaintext
hash function
plaintext
transmission
(encrypted or not encrypted)
hash function


Signature

Herzlichen Dank
für Ihr Interesse!