Asymmetrische Verschlüsselung

Kryptografie

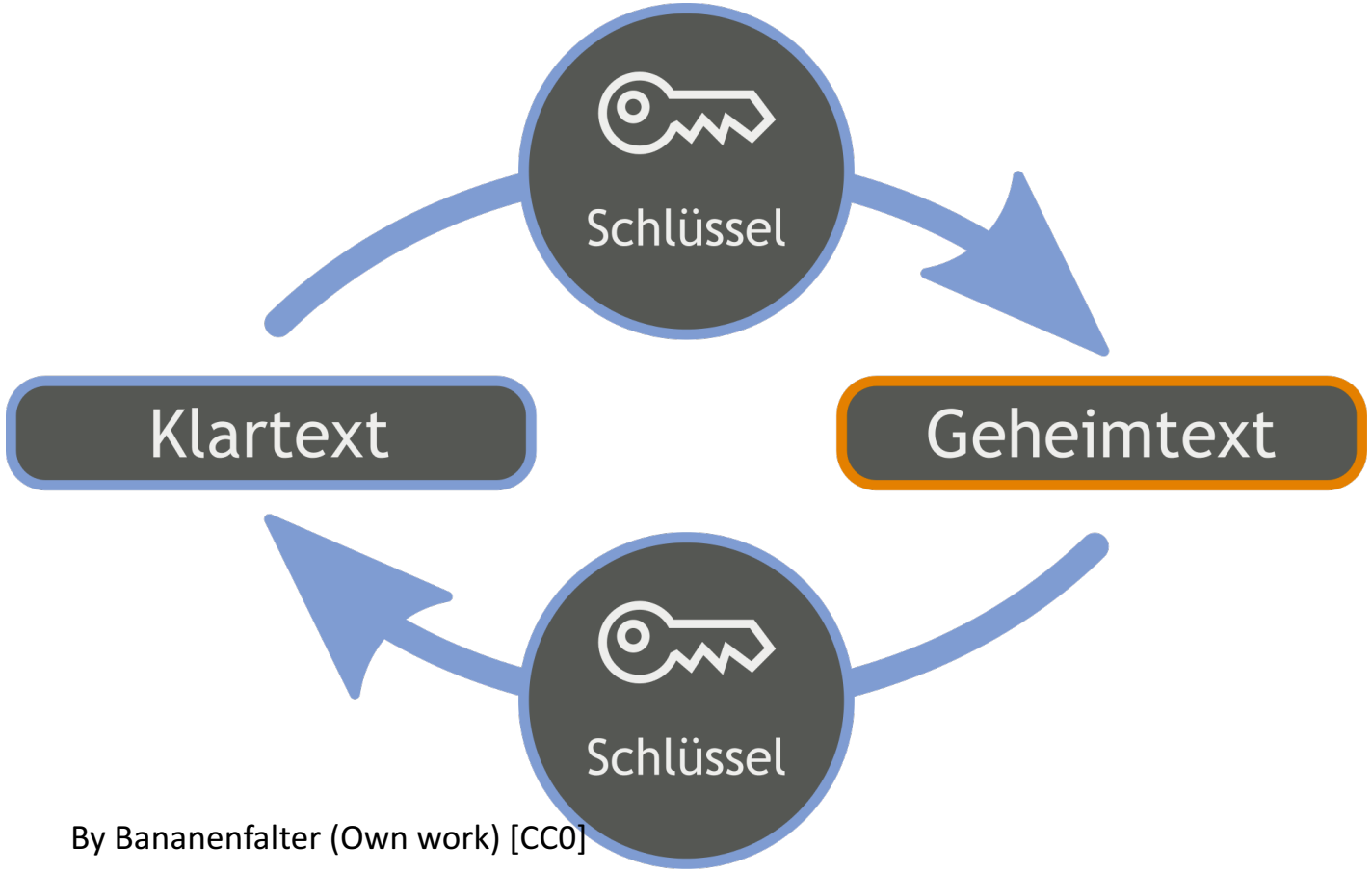
- Vertraulichkeit (Confidentiality)
- Authentifizierung (Authentication)
- Integrität (Integrity)
- Verbindlichkeit (Non-Repudiation)

Wie sicher ist Verschlüsselung?

- Keine absolute Sicherheit
- Beruht nicht auf Geheimhaltung des Verfahrens
- Abhängig von der Schlüssellänge

Niekverlaan, CC0

Symmetrische Verschlüsselung



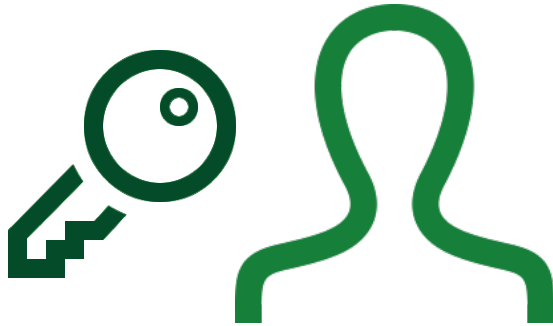
By Bananenfalter (Own work) [CC0]

- Kann abgefangen werden
- Hohe Schlüsselanzahl:

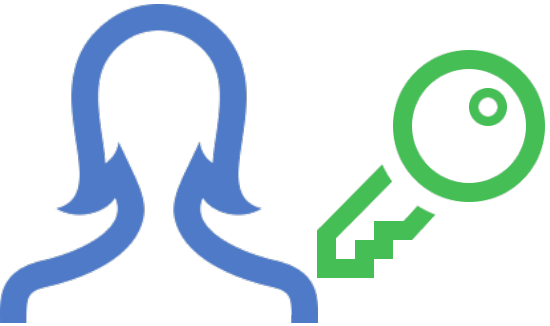
$$\frac{n(n-1)}{2}$$

- Relativ schnell

ALICE

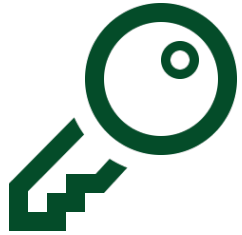


BOB

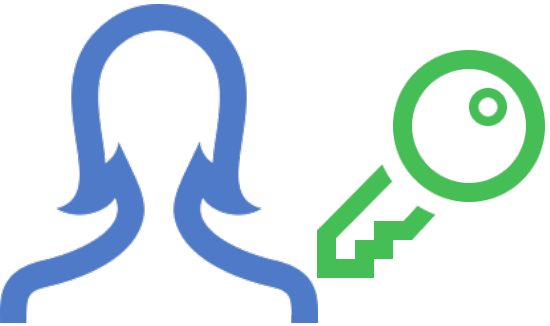


ALICE

BOB

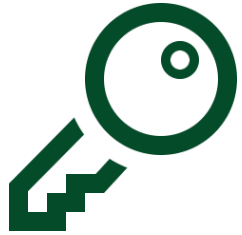


HALLO
WELT

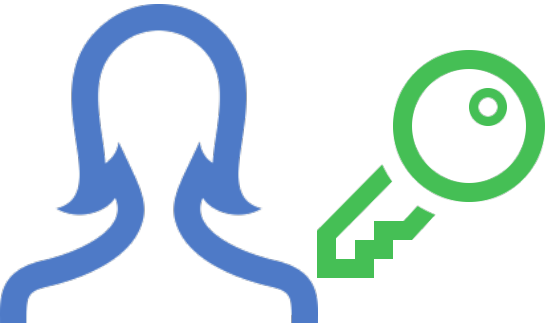


ALICE

BOB

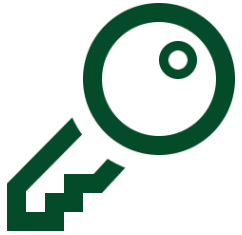


SZGGEX
hiGO

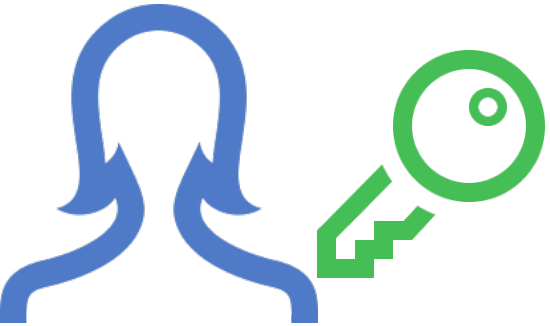


ALICE

BOB



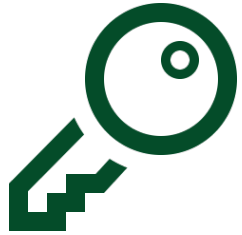
SZGGEX
hiGO



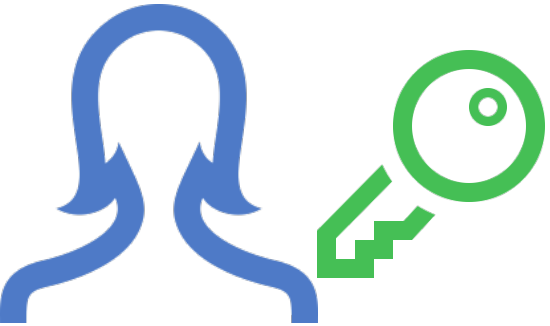
ALICE

SZGGEX
hiGO

BOB



SZGGEX
hiGO

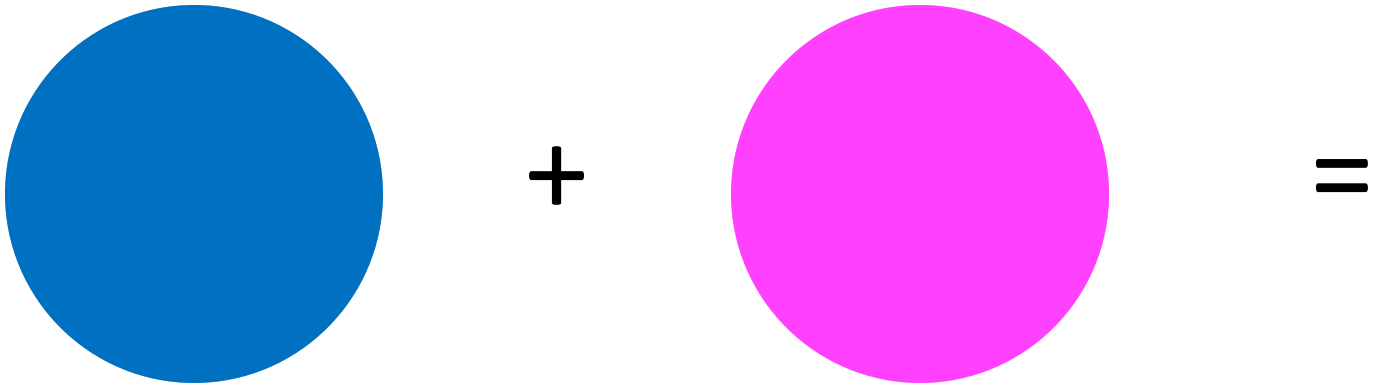


ALICE

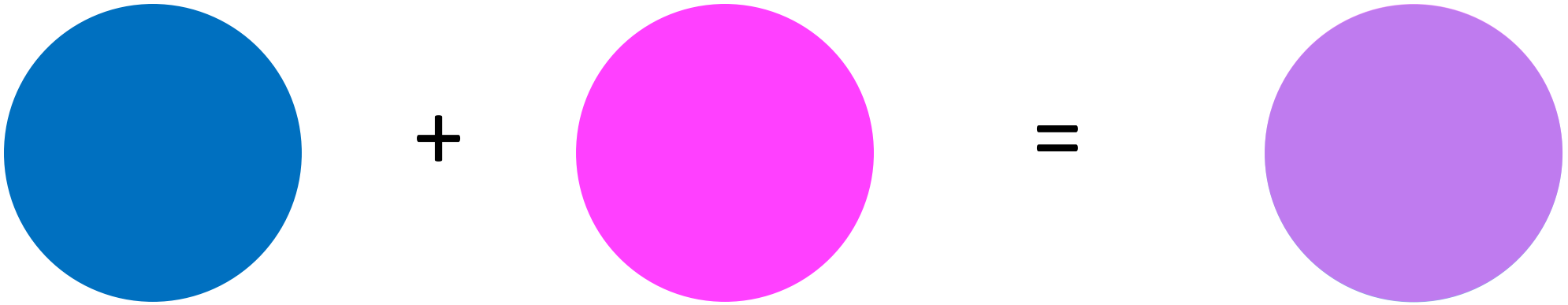
HALLO
WELT

BOB

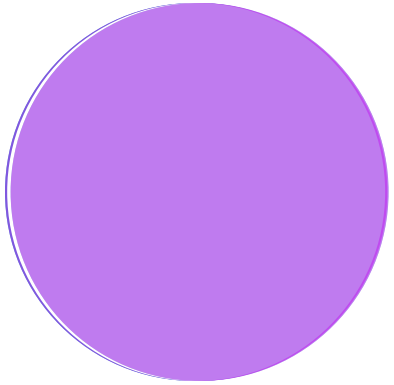
Einwegfunktion



Einwegfunktion



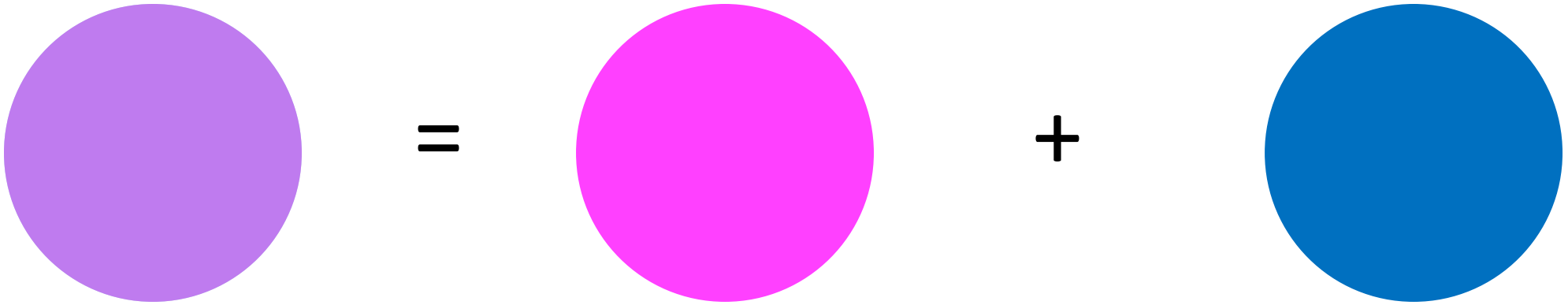
Einwegfunktion



=

+

Einwegfunktion



Verschlüsseln

$$m^e \ mod \ N = ?$$

Entschlüsseln

$$? \,^{e} \; mod \; N = c$$

Verschlüsseln

$$m^{\,e} \; mod \; N = c$$

Entschlüsseln

$$c^{\,d} \bmod N = m$$

$$m^{e^d} \bmod N = m$$

$$m^{ed} \bmod N = m$$

Primfaktorzerlegung

$$30 = 5 \times 3 \times 2$$

Primfaktorzerlegung

$$19 \times 31 = 589$$

Primfaktorzerlegung

$$589 = 19 \times 31$$

Primfaktorzerlegung

P1 = 646411

P2 = 660769

N = P1 * P2

N = 427128350059

Phi-Funktion

$\Phi(x)$

Phi-Funktion

$$\Phi(8) = \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \end{matrix} = 4$$

Phi-Funktion

$$\Phi(P) = P - 1$$

Phi-Funktion

$$\Phi(A \times B) = \Phi(A) \times \Phi(B)$$

Phi-Funktion

$$\Phi(A \times B) = \Phi(A) \times \Phi(B)$$

$$N = P1 \times P2$$

Phi-Funktion

$$\Phi(N) = \Phi(P1) \times \Phi(P2)$$

Phi-Funktion

$$\Phi(N) = (P1 - 1) \times (P2 - 1)$$

Satz von Euler

$$m^{\Phi(n)} = 1 \; mod \; n$$

Satz von Euler

$$m^{\mathrm{k} * \Phi(n)} = 1 \, mod \, n$$

Satz von Euler

$$m * m^{\mathrm{k} * \Phi(n)} = m \; mod \; n$$

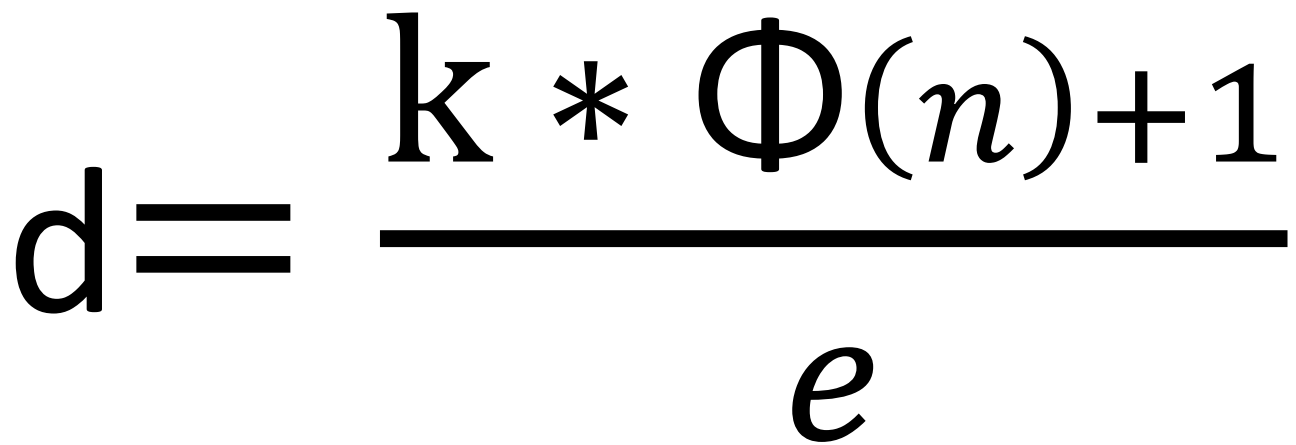
Satz von Euler

$$m^{\mathrm{k} * \Phi(n)+1} = m \; mod \; n$$

$$m^{\mathrm{k} * \Phi(n)+1} = m \bmod n$$

$$m^{ed} = m \bmod n$$

$$ed = \mathrm{k} * \Phi(n) + 1$$


d=
k * Φ(n)+1
e

Beispiel

- P1 = 5
- P2 = 7
- N = 5 * 7 = 35
- M = $\Phi(N) = (P - 1) * (Q - 1) = 24$
- E = 11
- K = ?

Beispiel

$$\mathrm{d} = \frac{\mathrm{k} * \Phi(n) + 1}{e}$$

Beispiel

- P1 = 5
- P2 = 7
- N = 5 * 7 = 35
- M = $\Phi(N) = (P - 1) * (Q - 1) = 24$
- E = 11
- K = 27

$$d = \frac{27 * 24 + 1}{11} = 59$$

Beispiel

- Öffentlicher Schlüssel:
  - N = 35
  - E = 11
- Private Schlüssel:
  - N = 35
  - D = 59

Beispiel: Verschlüsseln

- Text: HALLO
- In ASCII: 72 65 76 76 79

$$C = K^E \ \% \ \mathrm{N}$$

- $C_0 = 72^{11} \ \% \ 35 = 18$
- $C_1 = 65^{11} \ \% \ 35 = 25$
- $C_{2,3} = 76^{11} \ \% \ 35 = 6$
- $C_4 = 79^{11} \ \% \ 35 = 4$

18 25 06 06 04

Beispiel: Entschlüsseln

- 18 25 06 06 04

$$K = C^D \ \% \ \mathrm{N}$$

- $K_0 = \ 18^{59} \ \%\ 35 = 72$
- $K_1 = \ 25^{59} \ \%\ 35 = 65$
- $K_{2,3} = \ 6^{59} \ \%\ 35 = 76$
- $K_4 = \ 4^{59} \ \%\ 35 = 79$

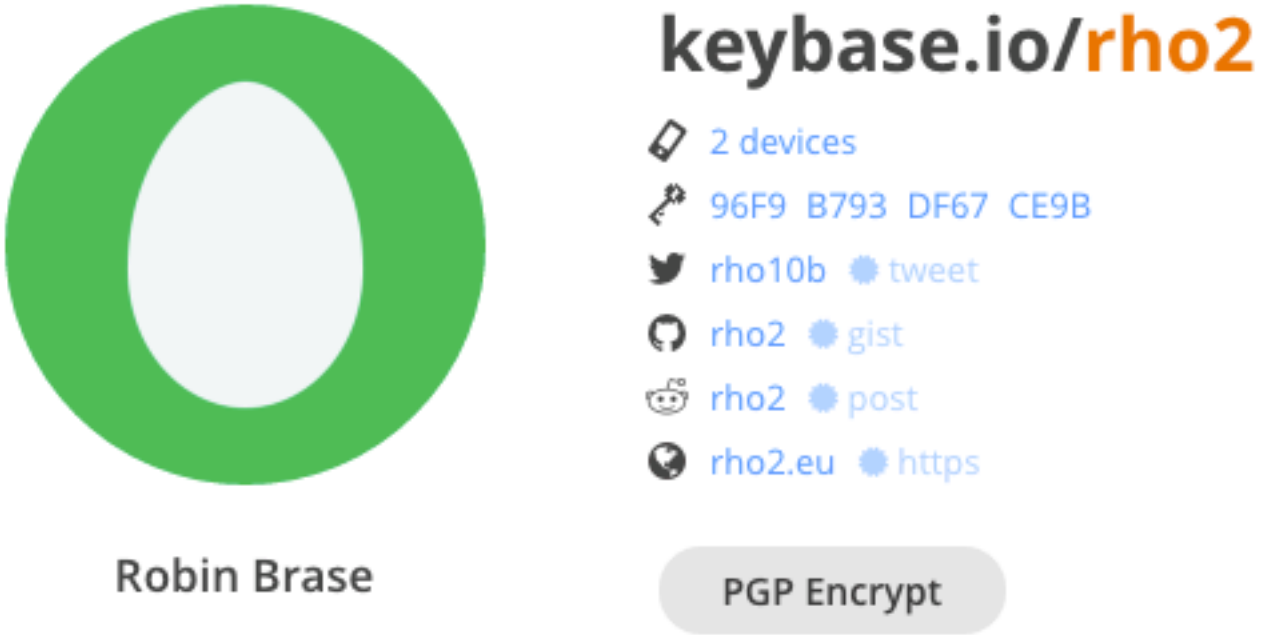
Hybridverfahren

- Symmetrisch verschlüsseln
- Schlüssel asymmetrisch versschlüsselt versenden

- Rechenaufwand nur einmal

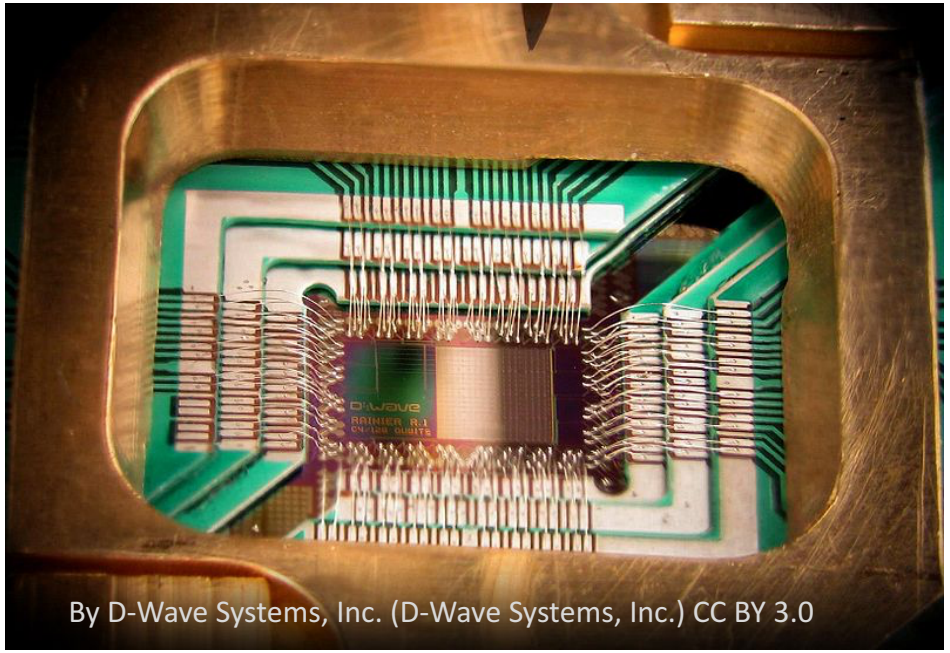
Echtheit des Public-Keys

- Persönliche Übergabe
- Verifizieren durch Dritte



Zukunft der Verschlüsselung

- Problem: Quantencomputer
- Idee: Künstliche Intelligenz



By D-Wave Systems, Inc. (D-Wave Systems, Inc.) CC BY 3.0

Quellen

- https://www.heise.de/security/artikel/Kryptographie-in-der-IT-Empfehlungen-zu-Verschluesselung-und-Verfahren-3221002.html [12.03.17 16:01]
- https://www.youtube.com/watch?v=wXB-V_Keiu8 [12.03.17 16:30]
- http://www2.ebe-online.de/verein/stammtsch_vortraege/verschluesselung_20131014.pdf [12.03.17 17:25]
- https://www.philipphauer.de/info/info/asymmetrische-verschluesselung/ [12.03.17 17:34]
- http://www.zeit.de/digital/datenschutz/2016-10/google-kuenstliche-intelligenz-erfindet-eigene-verschluesselung [12.03. 17 17: 53]
- Zahlen: Geschichte, Gesetze, Geheimnisse ; Albrecht Beutelspacher; 2015
- Informatik und Informationstechnik; Europa Lehrmittel; 2011

http://edu.rho2.eu/it/verschluesselung/