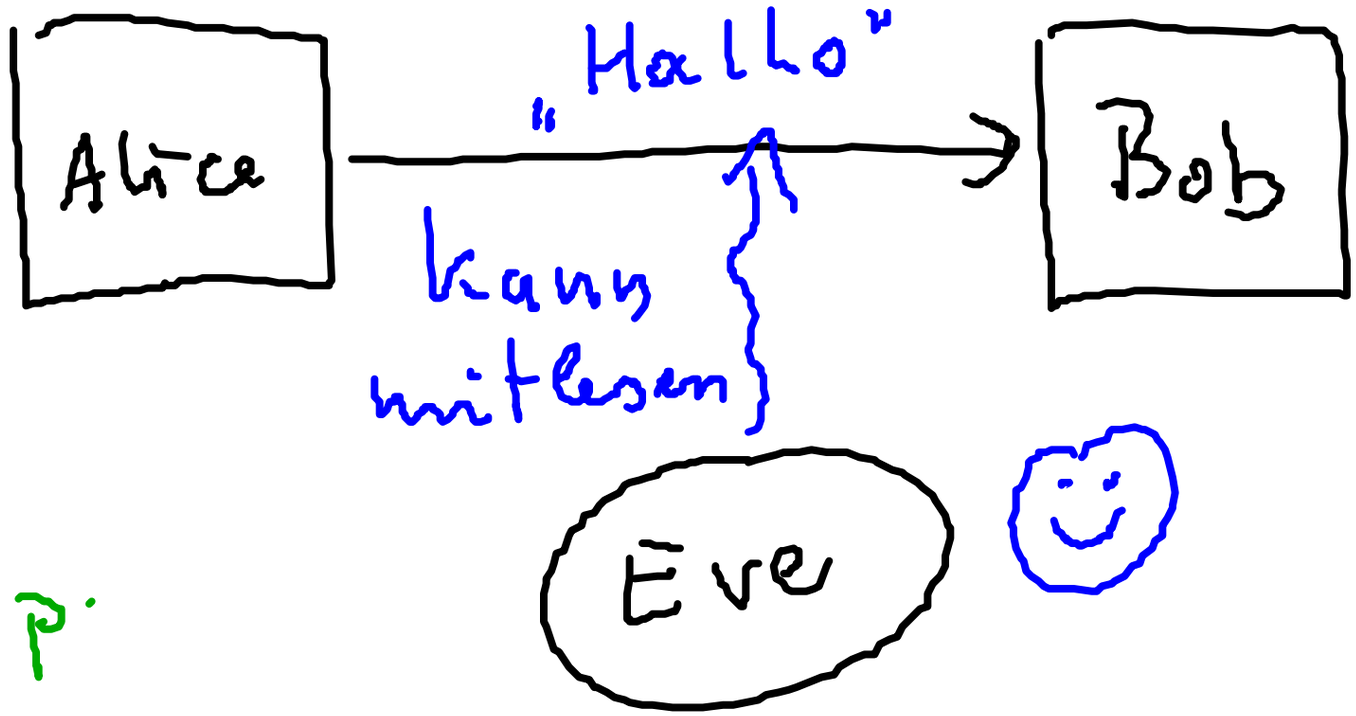
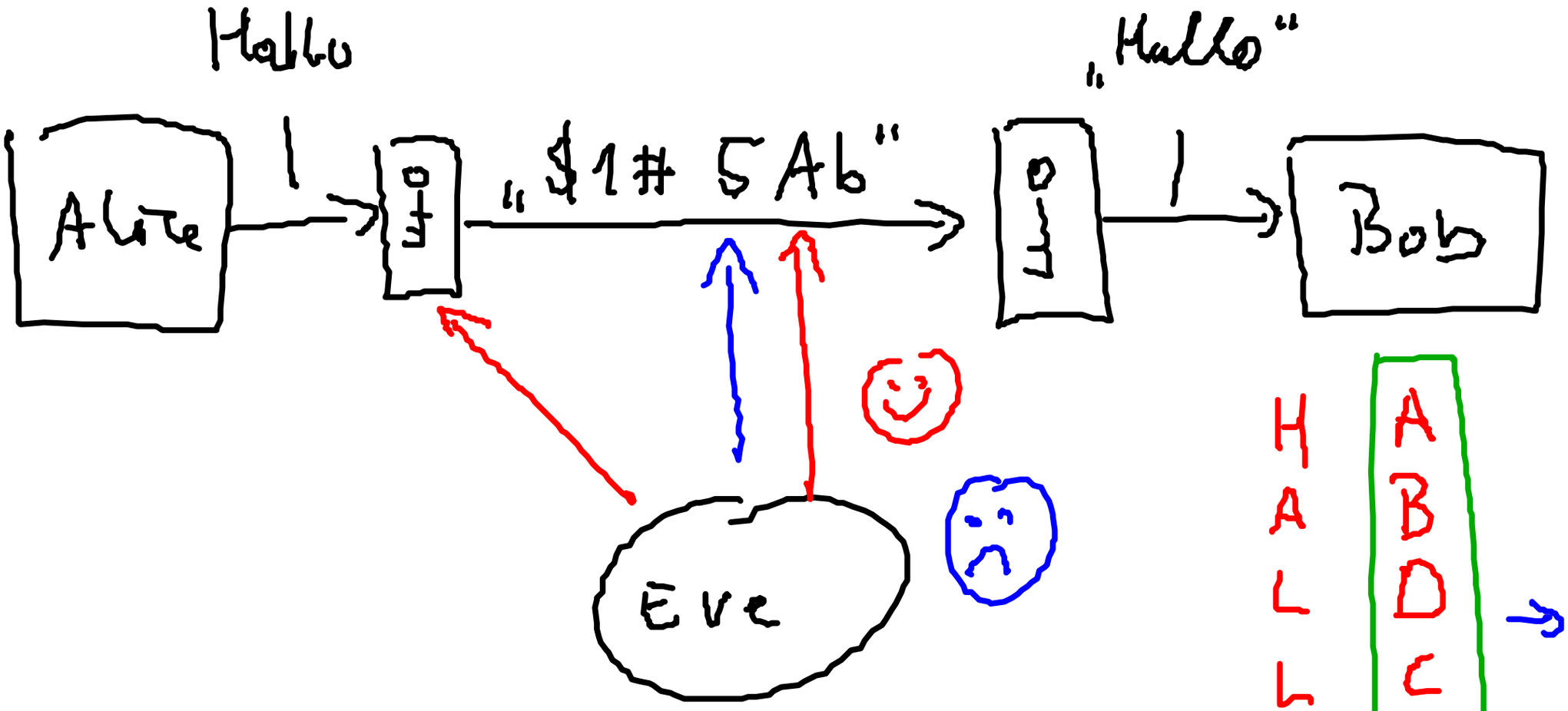
7. Bonbon: Public key cryptography

Problem Daten übermittlung!

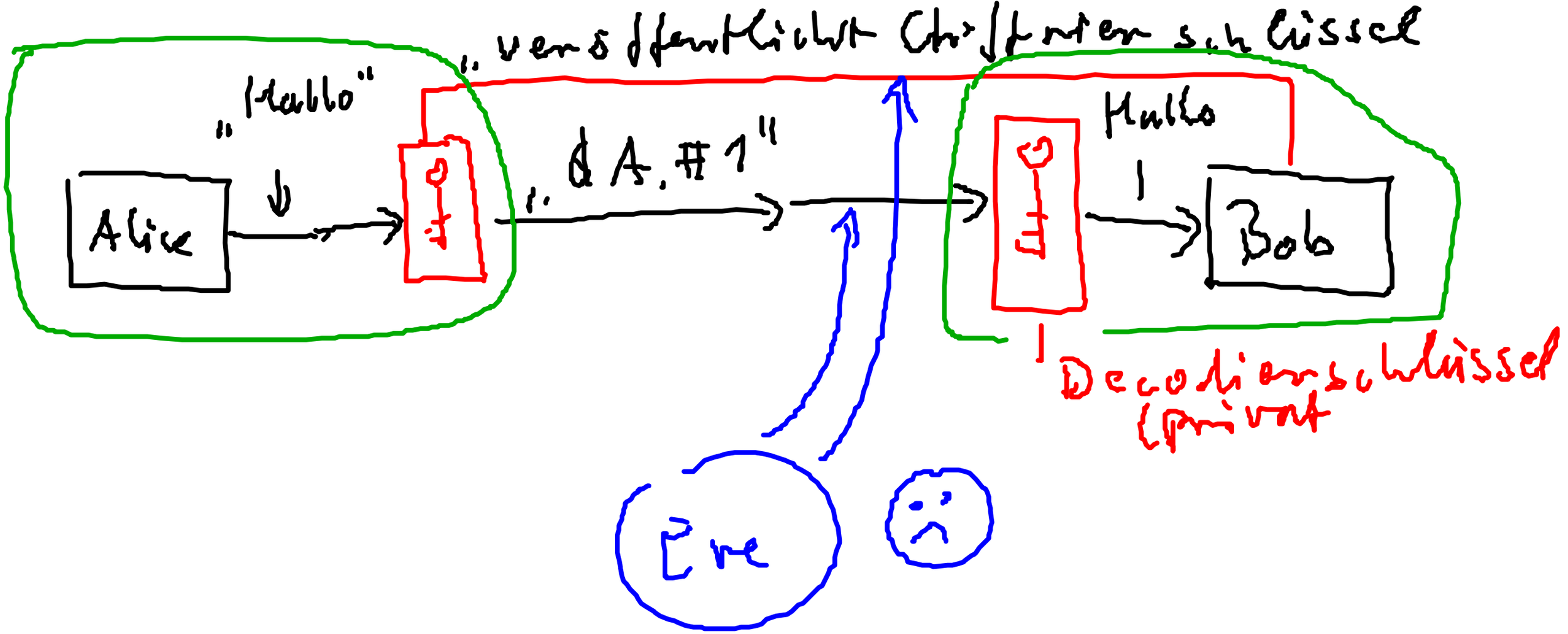


Literaturtip:
Neal Stephenson
„Cryptonomicon"



Wenn Eve nur weiß wie verschlüsselt wurde, kann sie da abhören

→ So war das bis 1977



RSA-Algorithmus

Falltürverfahren mit Primfaktorzerlegung

Rivest
Shamir
Adleman

1977

2?? - 1974

RSA

Alice

Bob veröffentlicht zwei Zahlen (N, k)

Verschlüsselung: ← Zahlenfolge ist Nachricht

Nachricht: $a_1, a_2, a_3 \ldots\ldots$

Berechne: $A_i = a_i^k \bmod N$ für $i = 1, 2 \ldots$

Sende: $A_1, A_2, A_3 \ldots\ldots$

Bobs Entschlüsselung:

Bob

Empfängt: $A_1, A_2, A_3, \ldots$

Rechne: $a_i' = A_i^s \bmod N$

Nachricht: $a_1', a_2', \ldots$

Behauptung: $a_i = a_i'$

(N, s)

geheimer Schlüssel

---

p, q zwei große Primzahlen

$N = p \cdot q$

k sei teilerfremd zu $(p-1)(q-1)$

(N, k) öffentlicher Schlüssel

$r = s \cdot k - x \cdot (p-1)(q-1)$

(N, s) geheimer Schlüssel

Wenn a, b Teilerfremd

Bsp: s, r

$1 = s \cdot a - r \cdot b$

Lemma 1 (kleiner Satz von Fermat / Euler)

Sei p Primzahl $a < p \Rightarrow a^{p-1} \bmod p = 1$

Schreibweise: $a =_p b \Leftrightarrow a \bmod p = b \bmod p$

$\Leftrightarrow a - b = k \cdot p$

Bew.

Betrachte $1, 2, 3, 4, \ldots, p-1$

und $a \cdot 1, a \cdot 2, a \cdot 3, \ldots, a(p-1) \mid \bmod p$

Beh: gleiche Zahlen evtl andere Reihenfolge

Weil $(\mathbb{Z}_p - \{0\}, \odot_p)$ ist Gruppe

$\Rightarrow$ [redacted] = eine Spalte der Mult. Tabelle.

Bsp: $p = 7, a = 5$

$5^6 \bmod 7$

$= (25)^3 \bmod 7$

$= 4^3 \bmod 7$

$= 16 \cdot 4 \bmod 7$

$= 2 \cdot 4 \bmod 7$

$= 8 \bmod 7$

$= 1$

Lemma 2

p und q seien verschiedene Primzahlen. Dann gilt:

$$x \equiv_p y \quad \text{und} \quad x \equiv_q y \Rightarrow$$

$$x \equiv_{p \cdot q} y$$

Bew

$x - y = k \cdot p$

$\underbrace{x - y}_{} = r \cdot q$

hat eindeutige Primfaktorzerlegung: $x - y = p \cdot q \cdot a$

in der p und q als Faktoren auftreten

$\Rightarrow x \equiv_{p \cdot q} y$

Lemma 3 p, q verschiedene Primzahlen, $a < p$, $a < q$

$$a^{r \cdot (q-1)(p-1)} \equiv_{p \cdot q} 1$$

Beweis:

$$X = \left(a^{(p-1)}\right)^{r \cdot (q-1)} \overset{\text{Lem 1}}{\equiv_p} (1)^{r \cdot (q-1)} = 1$$

$$X = \left(a^{(q-1)}\right)^{r \cdot (p-1)} \overset{\text{Lem 1}}{\equiv_q} (1)^{r \cdot (p-1)} = 1$$

$$\overset{\text{Lem 2}}{\Rightarrow} X \equiv_{p \cdot q} 1$$

Warum funktioniert RSA

$A = a^k \bmod N$

$a' = A^s \bmod N \Rightarrow a = a'$

$a < N$

$N = p \cdot q$

$ggT(k, (p-1)(q-1)) = 1$

$k \cdot s - r(p-1)(q-1) = 1$

Bew: $a' = A^s \bmod N$

$= (a^k \bmod N)^s \bmod N$

$= a^{k \cdot s} \bmod N$

$= a^{(r \cdot (p-1)(q-1) + 1)} \bmod N$

$= a \cdot a^{r \cdot (p-1)(q-1)} \bmod N$

$= a \cdot a^{r \cdot (p-1)(q-1)} \bmod (p \cdot q)$

$= a \cdot 1 \bmod p \cdot q = a$