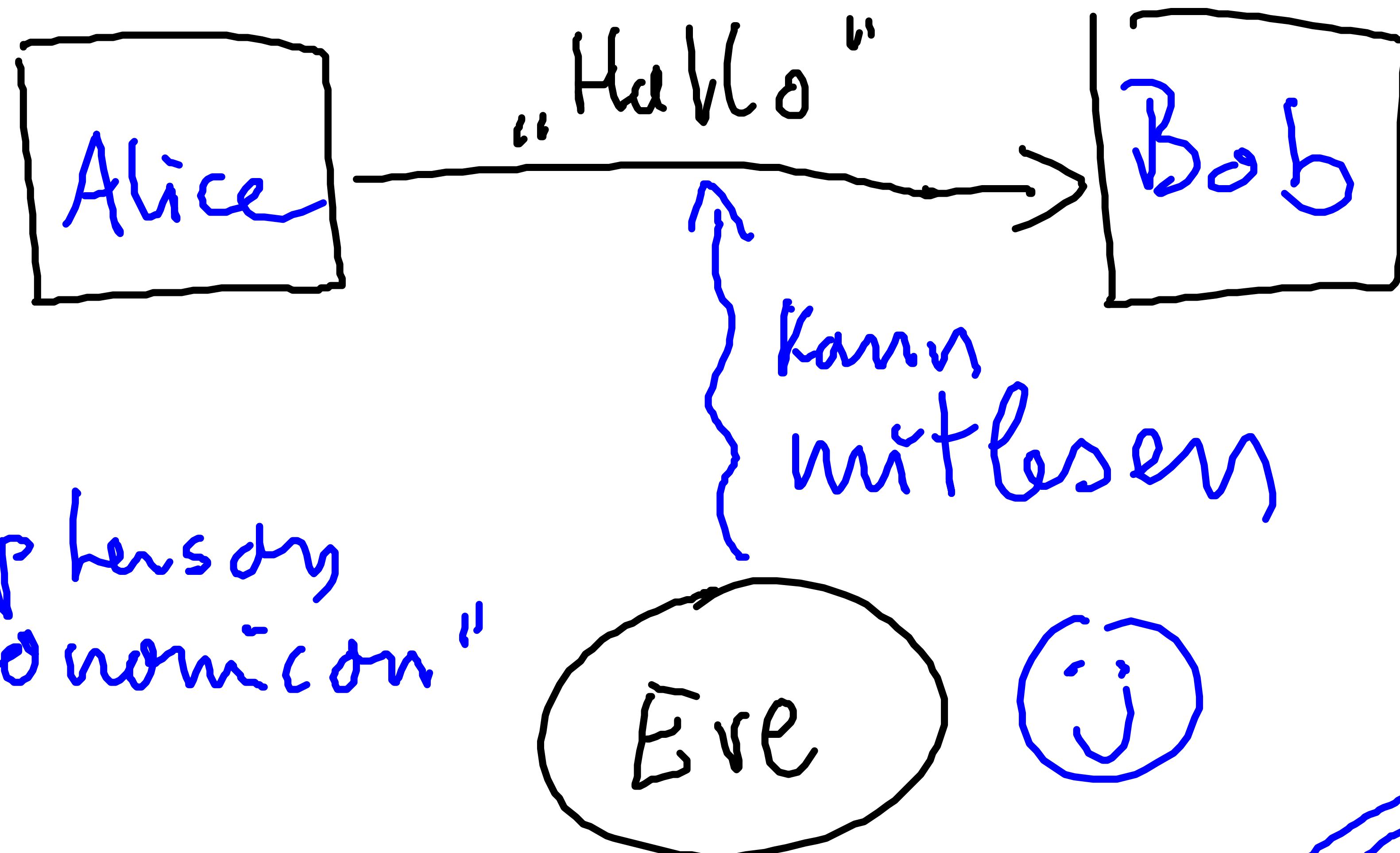
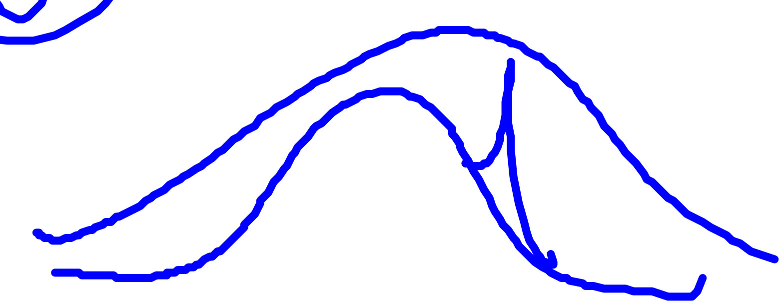
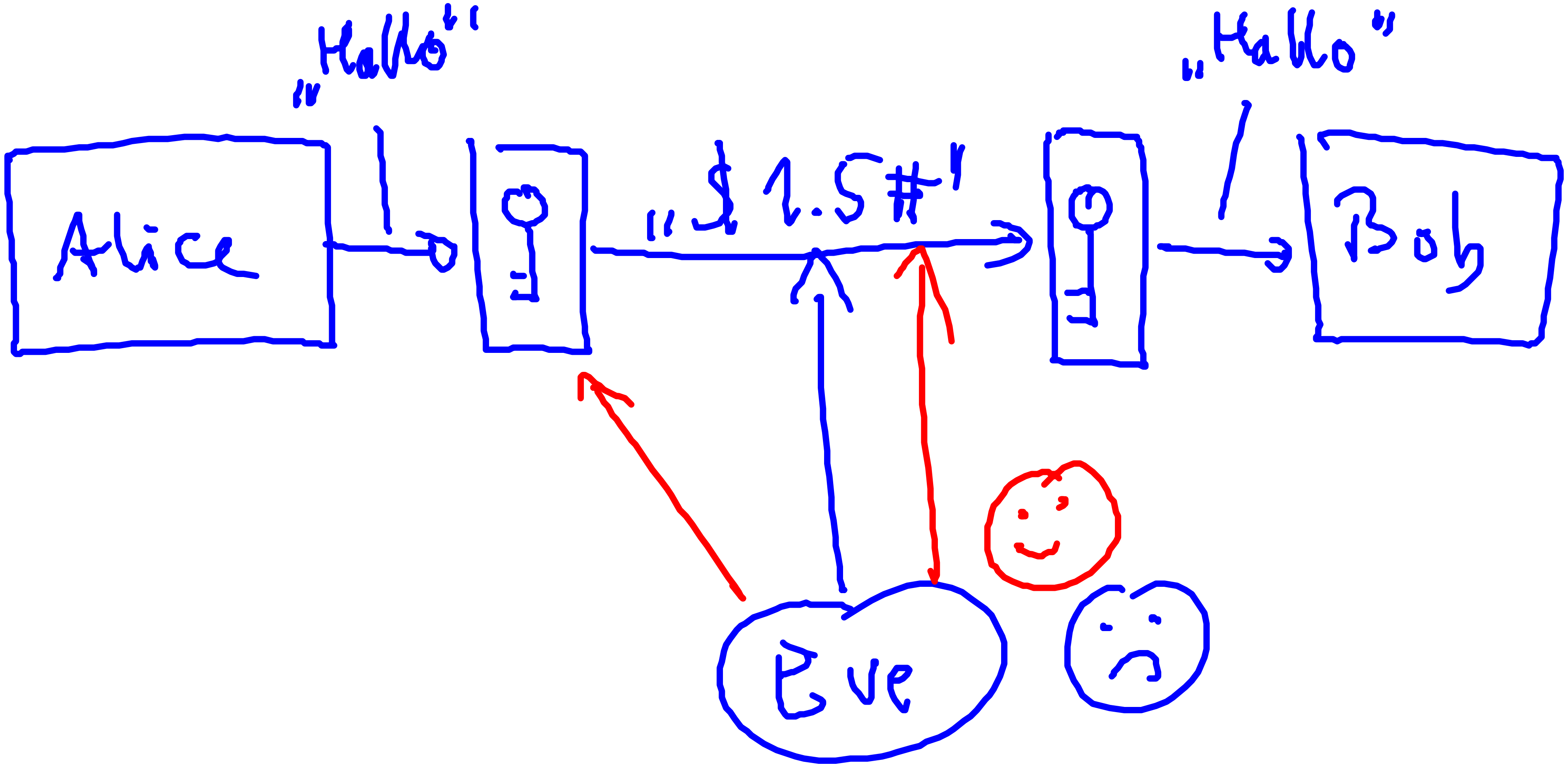
Einschub „Public key cryptography"

Problem Datenübermittlung



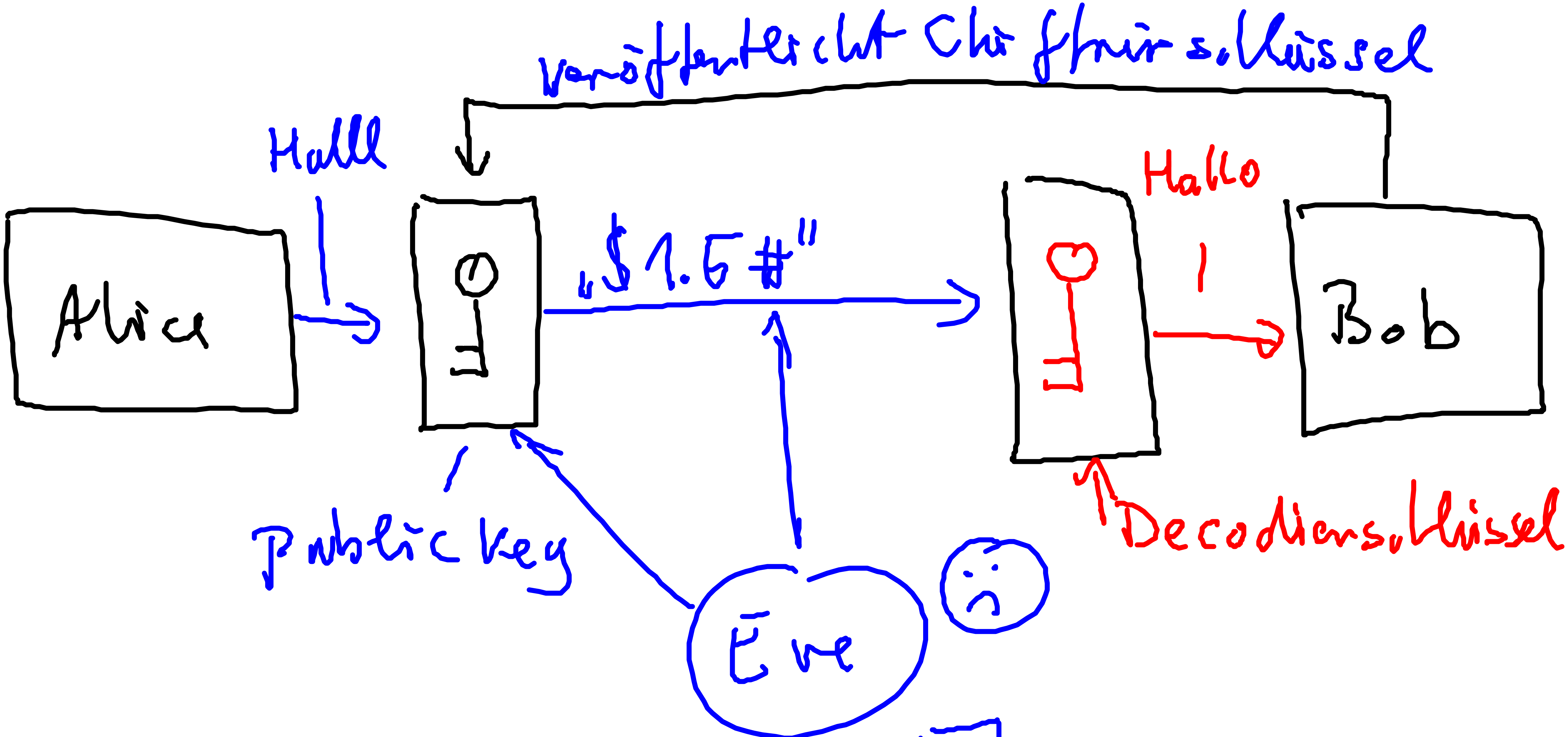
Neal Stephenson „Cryptonomicon"





Wenn Eve nur weis wie chiffriert wurde kann sie den Code knacken

Bis 1977 war das so



RSA-algorithmus

Rivest 1977
Shamir
Adleman

???-1974

RSA

Alice

Bob veröffentlicht zwei Zahlen (N, k)

Verschlüsselung:

Zahlen sind Nachrichtfragmente

Nachricht: $a_1, a_2, a_3, a_4 \ldots$

Berechne $A_i = a_1^k \bmod N$ für $i=1,2,\ldots$

Sende $A_1, A_2, A_3 \ldots$

Bobs Entschlüsselung

Bob

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

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

(N, s)

Bobs geheimer Schlüssel

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

Behauptung: $a_i = a_i'$

p, q zwei große Primzahlen

$N = p \cdot q$

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

(N, k) öffentliche Schlüssel

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

Geheimer Schlüssel (N, s)

Der Trick: Falltürenfunktionen

Rechnungen die einfach auszuführen sind, aber schwer Rückgängig machbar.

Beispiel: Sei p, q Primzahlen

Berechne $N = p \cdot q$

Schwierig N zu zerlegen

Lemma 1 (Kleiner Satz von Fermat / Euler)

Sei p Primzahl $a < p$

$a^{p-1} \bmod p = 1$

Schreibweise: $a =_p b \Leftrightarrow a \bmod p = b \bmod p \Leftrightarrow a - b = k \cdot p$

Bsp

$p = 7$

$a = 5$

$5^6 \bmod 7$

$= (25)^3 \bmod 7$

$= 4^3 \bmod 7$

$= 16 \cdot 4 \bmod 7$

$= 2 \cdot 4 \bmod 7$

$= 8 \bmod 7$

$= 1$

Bew:

Betrachte: $1, 2, 3, 4, \ldots, (p-1)$ $\bmod p$

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

gleiche Zahlen, andere Reihenfolge

Also: $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) =_p (a \cdot 1) \cdot (a \cdot 2) \cdot \ldots (a \cdot (p-1))$

$1 \cdot 2 \cdot 3 \ldots (p-1) =_p a^{(p-1)} \cdot (1 \cdot 2 \cdot \ldots (p-1))$

$1 =_p a^{(p-1)}$

Lemma 2: p, q seien verschiedene Primzahlen

$x \equiv_p y, \quad x \equiv_q y$

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

Bew: $x - y = k \cdot p$

$x - y = r \cdot q$

hat primfaktorzerlegung

$x - y = p \cdot q \cdot a$

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

Lemma 3: p, q versch Primzahlen

$a < p, \quad a < q$

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

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

$\underline{\equiv_p \; 1}$

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

$\equiv_q 1$

Lemma 2 $\Rightarrow \quad X \equiv_{p\cdot q} 1$

Warum funktioniert RSA

$a < N$

$N = p \cdot q,$

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

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

$A = a^k \bmod N$

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

Bew: $A^s \bmod N$

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

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

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

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

$= a$

1.2 Rechnen in Gruppen

Zur Erinnerung Gruppenaxiome

$\circ$ zweistelligen Operator auf Menge G

(i) Es ex $e \in G$ Für alle $a \in G$: $a \circ e = a$

(ii) Für alle $a \in G$ existier $a' \in G$ mit $a \circ a' = e$ e aus (i)

(iii) Für alle $a, b, c \in G$ $a \circ (b \circ c) = (a \circ b) \circ c$

Dann ist $(G, \circ)$ eine Gruppe

Satz 1 Aus $a \circ a' = e$ folgt $a' \circ a = e$

Bew

$$a' \circ a \overset{(i)}{=} (a' \circ a) \circ e$$

$$\overset{(ii)}{=} (a' \circ a) \circ (a' \circ (a')')$$

$$\overset{(iii)}{=} ((a' \circ a) \circ a') \circ (a')'$$

$$\overset{(iii)}{=} (a' \circ (a \circ a')) \circ (a')'$$

$$\overset{Vor}{=} (a' \circ e) \circ (a')'$$

$$\overset{(i)}{=} a' \circ (a')'$$

$$\overset{(ii)}{=} e$$

Wenn a' Rechtsinvers ist, so ist es auch linksinvers