RSA-Algorithmus

privater Schlüssel: a	öffentlicher Schlüssel: n und b

1. Zwei Primzahlen wählen + Produkt berechnen

$p = 11, q = 19 \qquad n = p \cdot q = 209$

2. Satz von Euler $\varphi(n)$

Wird für 3. benötigt $\varphi(n) = \varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1)$
$\varphi(209) = \varphi(11) \cdot \varphi(19) = 10 \cdot 18 = 180$

3. Private Key bestimmen, Zahl a suchen

Bedingungen:

- $0 \leq a < \varphi(n)$
- $ggT(\varphi(n), a) = 1$

$ggT(180, 101) = 1$

privater Schlüssel: $a = 101$

öffentlicher Schlüssel vervollständigen, b bestimmen

Das multiplikative Inverse von a in $\mathbb{Z}_{\varphi(n)}$ ist gesucht
Erweiterter euklidischer Algorithmus verwenden
$t = b$
$ggT(\varphi(n), a) = 1 \rightarrow t \cdot a \equiv 1 mod \varphi(n)$

a^{-1} in $\mathbb{Z}_{180}$:

x	y	q	r	u	s	v	t
180	101	1	79	1	0	0	1
101	79	1	22	0	0	1	-1
79	22	3	13	0	0	-1	2
22	13	1	9	0	0	2	-7
13	9	1	4	0	0	-7	9
9	4	2	1	0	0	9	-16
4	1	4	0	0	0	-16	**41**

öffentlicher Schlüssel: $n = 209, b = 41$

Verschlüsseln/Entschlüsseln

Verschlüsseln: $d = c^b mod n$ Entschlüsseln $e \equiv d^a mod n$

Verschlüsseln:

Öffentlicher Schlüssel:	n	33	b	7						
Die Nachricht (Buchstaben B_i):	M	A	T	T	E	R	H	O	R	N
Zahlenwerte der Buchstaben (Zahlen c_i) (nach Buchstabentabelle)	13	1	20	20	5	18	21	15	18	14
Verschlüsseln mit $d_i = c_i^b \bmod n$	7	1	26	26	14	6	2	27	6	20

Beispiele: $13^7 \equiv 7 \bmod 33$, $20^7 \equiv 26 \bmod 33$, $5^7 \equiv 14 \bmod 33$

Übermittelte Nachricht:	7	1	26	26	14	6	2	27	6	20

Entschlüsseln:

Privater Schlüssel:	n	33	a	3						
Empfangene Nachricht (Zahlen d_i):	7	1	26	26	14	6	2	27	6	20
Entschlüsseln mit $e_i \equiv d_i^a \bmod n$	13	1	20	20	5	18	8	15	18	14
Nur ich kann entschlüsseln:	M	A	T	T	E	R	H	O	R	N