# **RSA-Algorithmus**

privater Schlüssel: a | öffentlicher Schlüssel: n und b

#### 1. Zwei Primzahlen wählen + Produkt berechnen

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

### 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:

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

ggT(180, 101) = 1privater 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

$$ggT(\varphi(n), a) = 1 \to t \cdot a \equiv 1 mod\varphi(n)$$

 $a^{-1}$  in  $\mathbb{Z}_{180}$ : r t  $\mathbf{X}$ q  $\mathbf{v}$ 79 | 1 0 180 101 1101 79  $1 \ 22 \ 0 \ 0$ -1 1 79 22 $3 \ 13 \ 0$ 0 -1 22 1 9  $0 \quad 0$ 2 -7 13 13 1  $0 \quad 0$ -7 2 0 9 9 4 1 0 -16 1 4 0 0 0 -16 41

öffentlicher Schlüssel: n = 209, b = 41

## Verschlüsseln/Entschlüsseln

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

Öffentlicher Schlüssel:	n	33	b	7						
Die Nachricht (Buchstaben B <sub>i</sub> ):	M	Α	Т	Т	Ε	R	Н	0	R	Ν
	13	1	20	20	5	18	21	15	18	14
(nach Buchstabentabelle)										
Verschlüsseln mit $d_i = c_i^b \mod n$	7	1	26	26	14	6	2	27	6	20
	Die Nachricht (Buchstaben B <sub>i</sub> ): Zahlenwerte der Buchstaben (Zahlen c <sub>i</sub> ) (nach Buchstabentabelle)	Die Nachricht (Buchstaben B <sub>i</sub> ): M Zahlenwerte der Buchstaben (Zahlen c <sub>i</sub> ) 13 (nach Buchstabentabelle)	Die Nachricht (Buchstaben B.): M A Zahlenwerte der Buchstaben (Zahlen c.) 13 1 (nach Buchstabentabelle)	Die Nachricht (Buchstaben B.): M A T Zahlenwerte der Buchstaben (Zahlen c.) 13 1 20 (nach Buchstabentabelle)	Die Nachricht (Buchstaben Bı): M A T T Zahlenwerte der Buchstaben (Zahlen cı) 13 1 20 20 (nach Buchstabentabelle)	Die Nachricht (Buchstaben B <sub>1</sub> ): M A T T E Zahlenwerte der Buchstaben (Zahlen c) 13 1 20 20 5 (nach Buchstabentabelle)	Die Nachricht (Buchstaben B.): M A T T E R Zahlenwerte der Buchstaben (Zahlen c.) 13 1 20 20 5 18 (nach Buchstabentabelle)	Die Nachricht (Buchstaben B.): M A T T E R H Zahlenwerte der Buchstaben (Zahlen c.) 13 1 20 20 5 18 21 (nach Buchstabentabelle)	Die Nachricht (Buchstaben B.): M A T T E R H O Zahlenwerte der Buchstaben (Zahlen c.) 13 1 20 20 5 18 21 15 (nach Buchstabentabelle)	Die Nachricht (Buchstaben B.): M A T T E R H O R Zahlenwerte der Buchstaben (Zahlen c.) 13 1 20 20 5 18 21 15 18 (nach Buchstabentabelle)

Beispiele:  $13^7 = 7 \mod 33$ ,  $20^7 = 26 \mod 33$ ,  $5^7 = 14 \mod 33$ 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  $e_i = d_i^a \mod n$  13 1 20 20 5 18 8 15 18 14 Nur ich kann entschlüsseln: M A T T E R H O R N