

KRYPTOGRAPHIE

Fragen? \



encryption exponent

RSA. $p=61,\ q=53,\ \dot{e}=17.$ Ver- und Entschlüsseln Sie die Nachrichten T=61 und

(Bemerkung: Bei https ist T meist der AES-Schlüssel, der ausgetauscht wird.)

Lösung.

1. Schlüsselerzengung

RSA-Modul
$$N = p \cdot q = 61.53 = 3233$$
. ($\approx 3.10^3 \approx 2^{11}$ 11-Bit-Zahl)

•
$$\psi(N) = \psi(3233) = \psi(61) \cdot \psi(53) = 3120$$
.

EEA mit a = 17 und b = 3120 :
a = q * b + r | x | y | ggT = a * x + b * y |
17 = 0 * 3120 + 17 |
$$-367$$
 | 2 | 1 = 17 * -367 + 3120 * 2 |
3120 = 183 * 17 + 9 | 2 | -367 | 1 = 3120 * 2 + 17 * -367 | 17 = 1 * 9 + 8 | -1 | 2 | 1 = 17 * -1 + 9 * 2 | -1 + 9 * 2 | -1 + 1 * 1 | 1 | -1 | 1 = 9 * 1 + 8 * -1 | 8 = 8 * 1 + 0 | 0 | 1 | 1 = 8 * 0 + 1 * 1

$$d = -367 \equiv 2753 \mod 3120$$

2. Ver-/Estschlusrely

Schnelles Potensleven:
$$61^{17} = 61^{16} \cdot 61 = |((61^2)^2)^2|^2 \cdot 61 = (2928)^2 \cdot 61 = 610 \text{ mod } 3233$$

$$= 2501$$

$$455 8.225$$

$$452 8.225$$

$$= 2501$$
Whitely!

•
$$G = 610 \longrightarrow G^d = 610^{2753} \mod N$$

Analog: T=65 -> Te=65# = 2790 = G -> G = 2790 = 65 (mod N)

Eigener Lösungsversuch.