RSA

1978 von Rivest, Shamir, Adleman erfunden

Rechnen mod n,

$n = p \cdot q$, $p, q \in \mathbb{P}$

n: öffentlich

p, q: geheim

Exponenten

d geheim

e öffentlich

$\varphi(n)$

Faktorisieren komplexitätstheoretisch vermutlich nicht polynomiell

Setup:

- p, q Primzahlen ≥ 1024 Bit, $n = p \cdot q$
- e öff. Exponent mit $ggT(e, \varphi(n)) = 1$
- $d \equiv \frac{1}{e} \bmod \varphi(n)$
- öffentlicher Schlüssel (n, e)

Verschlüsselung:

m Klartext

$$m' \equiv m^e \bmod n$$

Entschlüsselung:

$$m = m'^d \bmod n$$

Beispiel:

$p = 7$, $q = 11 \Rightarrow n = p \cdot q = 77$

$\varphi(n) = \varphi(77) = \varphi(7) \cdot \varphi(11) = 6 \cdot 10 = 60$

e mit $ggT(e, \varphi(n)) = 1$

$e = 7$

$d \equiv \frac{1}{7} \bmod 60$

$\equiv 43 \bmod 60$

$7 \cdot 43 \equiv 301$

$7 \cdot x \equiv 1 \bmod 60$

$61, 121, 181, 241, 301$

öffentlich $(n, e) = (77, 7)$ geheim $d = 43$

Nachricht $m = 6$ verschlüsseln

$m' \equiv m^e \equiv 6^7 \bmod 77$

$\equiv 6^3 \cdot 6^3 \cdot 6 \bmod 77$

$\equiv (-15) \cdot (-15) \cdot 6 \equiv (-15) \cdot (-13) \equiv 195$

$\equiv 41 \bmod 77$

Entschlüsseln:

$m'^d \equiv 41^{43} \bmod 77$ — mod 11 / mod 7

$41^{43} \bmod 11$

$\equiv (-3)^3 \bmod 11$

$\bmod 11$

$41^{43} \bmod 7$

$\equiv (-1)^1 \equiv 6 \bmod 7$

$m \bmod 77$ mit chinesischem Restsatz