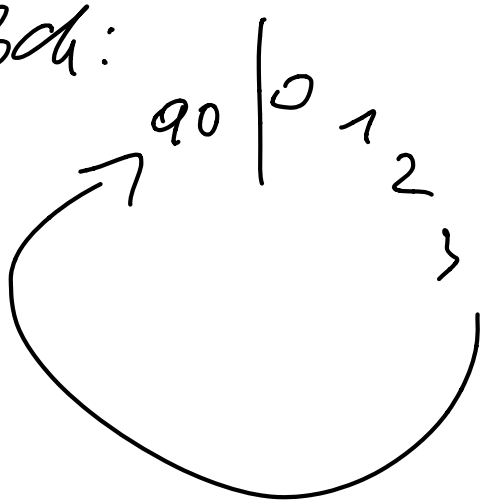
RSA an Beispiel

Modulare Arithmetik

Mod:



$7 \times 13 = 91$

Primzahl

Magic zw. 0..90 z.B.: 18

$18^5 = 44 \mod 91$ (z.B. Wolfram Alpha)

$44^{29} = 18 \mod 91$ ← decrypt

^29 ist das Inverse zu ^5

5 public key

29 private key

? Woher kommt 29 ?

① $91 = \underset{-1}{7} * \underset{-1}{13}$ ↙ 72h clock

$(7-1) * (13-1) = 72$

② wählen prim e mit $e \nmid 72$

z.B.: $e = 5$ public key

③ Suchen nun einen Wert d so dass:

$e * d = 1 \mod 72$

$\Rightarrow 5 * d = 1 \mod 72$

Erweiterter euklidischen Algorithmus

$72 = 14 \cdot 5 + 2$

$5 = 2 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

Darstellung des letzten Rests: $1 = \ldots$

(Rückwärts in die Reste einsetzen)

$1 = 5 - 2 \cdot 2$

↳ $72 = 14 \cdot 5 + 2 \Rightarrow$

$2 = 72 - 14 \cdot 5$

$\Rightarrow 1 = 5 - 2 \cdot (72 - 14 \cdot 5)$

$1 = 5 - 2 \cdot 72 + 28 \cdot 5$

$1 = 29 \cdot 5 - 2 \cdot 72$

↳ gesuchtes d

Probe: $5 * 29 = 1 \mod 72$ ✓

Warum funktioniert das?

d.h. warum $(a^5)^{29} = a \mod 91$?

$5 * 29 - 1 = 145 - 1 = 144 = 2 \cdot 72$

Vielfaches von 72

Wie kommen wir zu 72?

$72 = (7-1) \cdot (13-1)$

d.h. $5*29-1$ ist auch ein Vielfaches von $(7-1) \cdot (13-1)$

d.h. $e \cdot d - 1$ ist ein Vielfaches von ✳

- einer Primzahl -1, mal
- rechter Primzahl -1

Satz von Euler-Fermat (bzw. Folgerung daraus)

$$a^{(p-1)(q-1)} = 1 \mod p \cdot q$$

$$\Rightarrow a^{(7-1)(13-1)} = 1 \mod 7 \cdot 13$$

$$\Rightarrow a^{72} = 1 \mod 91$$

$$(18^5)^{29} = 18^{5 \cdot 29} \mod 91$$

$$= 18^{5 \cdot 29 - 1} \cdot 18$$

$$\left(2 \cdot \underbrace{(7-1)(13-1)}_{72} \right)$$

$$= (18^{72})^2 \cdot 18$$

$$= 1^2 \cdot 18$$

$$= 18 \quad \text{q.e.d.}$$

Diese Rechnung kann man für alle a $0, \ldots, 90$ machen!

Zusammenfassung:

$n = p \cdot q \Rightarrow e, d$

public key: n, e	p und q sind
private key: n, d	nicht länger relevant

? Warum ist das sicher ?

Um d zu finden waren p und q notwendig (um $(p-1) \cdot (q-1)$ zu berechnen)

Angreifer müsste aus n wieder $p * q$ herstellen (Faktorisierung) und das ist extrem aufwändig

z.B.: 900 CPU-Kern Jahre für n mit 240 Stellen (795 Bits)

Typisch: n RSA 2048 Bits ~ 600 dezimale Stellen