

RSA

---

- Erfunden 1977 von Ronald Rivest, Adi Shamir, Leonard Adleman
  - Patentierte von 1983 bis 2000
- Nicht das erste asymmetrische Verfahren
  - Am britischen GCHQ wurde bereits Anfang der 1970er ein Verfahren entwickelt, unterlag aber lange Zeit der Geheimhaltung

## Aufgabe 1

- Erarbeite selbständig das RSA-Verfahren unter <http://www.matheprisma.uni-wuppertal.de/Module/RSA/>

# Der Algorithmus

1. Wähle zufällig zwei große Primzahlen  $p$  und  $q$  mit  $p \neq q$
2. Berechne  $N = p \cdot q$  (der sogenannte RSA-Modul)
3. Berechne  $\varphi(N) = (p - 1) \cdot (q - 1)$  (Eulersche Phi-Funktion)
4. Wähle eine Zahl  $e$ , die teilerfremd zu  $\varphi(N)$  ist, mit  $1 < e < \varphi(N)$ 
  - Das Zahlenpaar  $(e, N)$  ist der öffentliche Schlüssel
5. Bestimme eine Zahl  $d$  für die gilt  $e \cdot d \equiv 1 \pmod{\varphi(N)}$  (Modulare Inverse)
  - Das Zahlenpaar  $(d, N)$  ist der private Schlüssel

Nach Erzeugung des Schlüsselpaars können (und sollten)  $p$ ,  $q$  und  $\varphi(N)$  gelöscht werden.

- Verschlüsseln einer Nachricht  $m$  (mit  $m < N$ ):
  - $c \equiv m^e \pmod{N}$
- Entschlüsseln einer Nachricht  $c$ :
  - $m \equiv c^d \pmod{N}$

- Gesucht ist  $d$  mit  $e \cdot d \equiv 1 \pmod{\varphi(N)}$
- Da  $e$  teilerfremd zu  $\varphi(N)$  ist gilt  $\text{ggT}(e, \varphi(N)) = 1$
- Es gibt Zahlen<sup>1</sup>  $x, y \in \mathbb{Z}$ , so dass  $x \cdot e + y \cdot \varphi(N) = 1$ 
  - $x$  und  $y$  können mit dem erweiterten euklidischen Algorithmus bestimmt werden

---

<sup>1</sup>Der größte gemeinsame Teiler zweier Zahlen  $a$  und  $b$  lässt sich immer darstellen als  $x \cdot a + y \cdot b = \text{ggT}(a, b)$  ( $x, y \in \mathbb{Z}$ )

## Beispiel (1)

1. Wähle  $p = 7$  und  $q = 13$
2.  $N = p \cdot q = 7 \cdot 13 = 91$
3.  $\varphi(N) = 6 \cdot 12 = 72$
4. Suche  $e$  zwischen 1 und 72 mit  $\text{ggT}(e, 72) = 1$ , z. B.  $e = 5$ 
  - $(5, 91)$  ist der öffentliche Schlüssel

## Beispiel (2)

5. Suche  $d$  mit  $d \cdot 5 \equiv 1 \pmod{72}$ , also  $d \cdot 5 = k \cdot 72 + 1$  bzw.  
 $d \cdot 5 - k \cdot 72 = 1$

- Da  $\text{ggT}(5, 72) = 1$ , gibt es Zahlen  $x, y \in \mathbb{Z}$ , so dass gilt:

$$x \cdot 5 + y \cdot 72 = 1$$

- Erweiterter euklidischer Algorithmus:

$$(1) \quad 72 = 14 \cdot 5 + 2$$

$$(2) \quad 5 = 2 \cdot 2 + 1$$

$$(3) \quad 2 = 2 \cdot 1 + 0$$



## Beispiel (3)

5. Suche  $d$  mit  $d \cdot e \equiv 1 \pmod{72}$ , also  $d \cdot e = k \cdot 72 + 1$  für ein  $k \in \mathbb{N}$

- Umformen und einsetzen:

- Aus (2) folgt:  $1 = 5 - 2 \cdot 2$

- Aus (1) folgt:  $2 = 72 - 14 \cdot 5$

- Erste in zweite Gleichung einsetzen:

- $$1 = 5 - 2 \cdot (72 - 14 \cdot 5) = 5 - 2 \cdot 72 + 28 \cdot 5 = 29 \cdot 5 - 2 \cdot 72$$

- Also  $1 = 29 \cdot 5 - 2 \cdot 72 \Rightarrow x = 29, y = -2$

- $y$  brauchen wir nicht, aber  $d = x = 29$

- $(29, 91)$  ist der private Schlüssel

## Beispiel (4)

- Verschlüsseln von  $m = 50$ :

$$\cdot c = m^e \bmod N = 50^5 \bmod 91 = 85$$

- Entschlüsseln von  $c = 85$ :

$$\cdot m = c^d \bmod N = 85^{29} \bmod 91 = 50$$