

# RSA - ein asymmetrisches Verschlüsselungsverfahren

Eine Präsentation von Christfried Posselt

Christian Weise Gymnasium

Informatik – Herr Hans

# Gliederung

- Allgemeines
- Grundprinzip
- Mathematische Grundlagen:
  - Einwegfunktion
  - Modulo-Rechnung
  - Verschlüsseln
  - Entschlüsseln
- Demonstration mit CrypTool
- Fragen

# Allgemeines

- 1977 von R. Rivest, A. Shamir und L. Adleman
- 1. asymmetrische Verschlüsselungsverfahren
- 1983 Patent angemeldet - 2000 ausgelaufen
- Verwendung in effizienten, symmetrischen Verschlüsselungsverfahren gewährleistet den sicheren Schlüsselaustausch
  - Internet Telefonie
  - E-Mail und Datentransfer
  - Chipkarten

# Das Grundprinzip

- Empfänger hat Schloss und Schlüssel
- Der Sender erhält erst das Schloss  
→ Public Key
- Er verschlüsselt damit die Nachricht
- Die Nachricht kann nun sicher verschickt werden, da niemand außer dem Empfänger den Schlüssel je gesehen hat
- Knacken des Codes nahezu unmöglich ist  
→ Einwegfunktion
- Entschlüsseln beim Empfänger mit dem Schlüssel  
→ Private Key

# Mathematische Grundlagen

- Einwegfunktion = einfach zu berechnen, aber sehr schwer umkehrbar
- Beispiel: Produkt aus 2 Primzahlen

$$14803 = \_p\_ * \_q\_ \quad //p=113; q=131$$

- Modulo Rechnung:  $a \bmod b = r$

r ist der Rest, den a bei Division durch b lässt.

$$a = n * b + r$$

- Beispiel:  $21 \bmod 6 = 3$   
 $1 \bmod 3 = 1$

# Mathematische Grundlagen

- Verschlüsseln:  $C = M^e \bmod N$
- Public Key =  $(N; e) \rightarrow$  zum Verschlüsseln
- $M$  = Zahl im ASCII-Code für das zu verschlüsselnde Zeichen
- $C$  = übertragbares, verschlüsseltes Zeichen
- Beispiel: Buchstabe „L“ = 76  
Public Key  $(187; 7)$   
 $C = 76^7 \bmod 187 = 32$

# Mathematische Grundlagen

- Entschlüsseln:  $M = C^d \bmod N$   
Private Key =  $d \rightarrow$  zum Entschlüsseln
- $e * d \bmod (p-1) * (q-1) = 1$
- Es ist unmöglich  $d$  zu berechnen ohne  $p$ ;  $q$  zu kennen
- Beispiel:  $7 * d \bmod (11-1) * (17-1) = 1$   
 $\rightarrow 7 * d = 161 \rightarrow d = 23$   
 $M = 32^{23} \bmod 187 = 76$   
76 entspricht dem Buchstaben „L“



**Jetzt ist Zeit für Rückfragen!**

Vielen Dank für eure Aufmerksamkeit