RSA

Luc Spachmann

Friedrich-Schiller-Universität Jena

21.12.2023

RSA

- Schlüssel (e, n) und (d, n) gegeben mit

$$ed = 1 \mod \varphi(n)$$

  und n Produkt zweier Primzahlen
- φ ist Eulersche φ-Funktion
- Für Produkt zweier Primzahlen pq gilt

$$\varphi(pq) = (p-1)(q-1)$$

- Text wird dargestellt als Folge von Zahlen $x_1, \ldots, x_n < n$
- Verschlüsselung jeder Zahl $y_i = x_i^e \mod n$
- Entschlüsselung $x_i = y_i^d \mod n$
- Frage: Effektive Berechnung von x^e

Quadrieren und Multiplizieren

- Effektiver Algorithmus für Potenzen Modulo n
- Ähnlich russischer Bauernmultiplikation
- Berechnen $x^m \mod n$
- Sei $m = b_0 + b_1 \cdot 2 + b_2 \cdot 2^2 + ... + b_r \cdot 2^r$ mit $b_i \in \{0, 1\}$

Pseudocode

Require: x, m, n

1: $y = 1$
2: **for** $i = 0, ..., r$ **do**
3: **if** $b_i = 1$ **then**
4: $y = y \cdot x \mod n$
5: **end if**
6: $x = x^2 \mod n$
7: **end for**
8: **return** y

Aufgaben

- Implementiert RSA mithilfe Quadrieren und Multiplizieren
- Erlaubt Zahlen in Größenordnungen von bis zu 2^{2000}
- Programmname [Input] [Schlüssel] [Output]
- Input: Datei mit einer Zahl (Dezimal)
- Schlüssel: Zwei Zeilen
  - Erste Zeile: e bzw d
  - Zweite Zeile: n (beides Dezimal)
- Output: Verschlüsselter Text in Dezimal