

ERGÄNZENDE STICHPUNKTE: KRYPTOGRAPHISCHE VERFAHREN

Symmetrische Verfahren.

DES / AES: • Block-Chiffer

- Permutation, Substitution, Garbage in between
- Schlüssellänge 126 / 256
- On-chip / Kerberos
- <http://www.itl.nist.gov/fipspubs/fip46-2.htm>

Geteiltes Geheimnis / Höhlengeheimnis: • Zero-Knowledge Proof

- Graph-Isomorphismen
- Foliensatz

Asymmetrische Verfahren.

Fiat Shamir Protokoll: • Sieb des Erasthosteles

- Quadratwurzel
- $x^2 = v \pmod n$ mit $n = p \cdot q$, $p, q \in \text{Prim}$, wobei Prim die Menge aller Primzahlen in $\mathbb{Z} \setminus \{0\}$ sei
- Zero-Knowledge Proof
- Block-Chiffer
- Primfaktor-Zerlegung
- Schlüssellänge 128 / 256
- Schlüsselerzeugung
- Foliensatz

RSA-Verfahren: • Euklidischer Algorithmus (ggT)

- schnelle Multiplikation
- Primfaktor-Zerlegung
- diskreter Logarithmus
- $a^z = a^{z \pmod{\varphi(n)}} \pmod n$ mit $n = p \cdot q$, $p, q \in \text{Prim}$, $a, z \in \mathbb{N}_0$
- Block-Chiffer
- Verschlüsselung von Nachrichten, z.B. PGP
- Unterlagen aus H. Scheid, A. Frommer: Zahlentheorie. München 2007, 4. Aufl.

Protokoll RSA-Verfahren.

Ziel.

- (1) Alice sendet eine Nachricht $m \in \mathbb{N}$ chiffert als $c \in \mathbb{N}$ an Bob.
- (2) Bob rekonstruiert m aus c .
- (3) Die gesamte Kommunikation ist öffentlich.

Protokoll.

- (1) Vorbereitung. Alice teilt Bob mit, dass sie ihm eine Nachricht senden will.
- (2) Bob wählt zwei Primzahlen $p, q \in \text{Prim}$. Zudem bestimmt Bob ein e mit $ggT(e, (p-1) \cdot (q-1)) = 1$.
- (3) Bob berechnet $d = e^{-1} \pmod{(p-1) \cdot (q-1)}$ und $n = p \cdot q$.
- (4) Bob sendet n und e an Alice. Bob behält die Zahlen p, q und d geheim.
- (5) Alice berechnet $c = m^e \pmod{n}$.
- (6) Alice sendet c an Bob.
- (7) Bob berechnet $m = c^d \pmod{n}$.

Beispiel.

- (1) Alice teilt Bob mit, dass sie ihm eine Nachricht senden will.
- (2) Bob wählt zwei Primzahlen $p = 23$ und $q = 29$. Damit ist $n = p \cdot q = 23 \cdot 29 = 667$. Zudem bestimmt Bob e mit $\varphi(n) = (p-1) \cdot (q-1) = 22 \cdot 28 = 616$ und $ggT(e, (p-1) \cdot (q-1)) = ggT(e, 22 \cdot 28) = ggT(e, 616)$. Weiter muss gelten $ggT(e, 616) = 1$. Damit ist $e = 15$.
- (3) Bob berechnet $d = e^{-1} \pmod{(p-1) \cdot (q-1)}$ und $n = p \cdot q$. Die Berechnung von d ist abhängig vom gewählten Wert von e , s. a. $ggT(15, 616) = 1$, denn $615 : 15 = 41$ und wiederum $575 = 41 \pmod{616}$.) Damit ist $e^{-1} = 575$.
- (4) Bob sendet $n = 667$ und $e = 15$ an Alice. Bob behält die Zahlen p, q und d geheim.
- (5) Alice berechnet $c = m^e \pmod{n}$. Sei $m = 11$. Dann ist $c = 11^{15} \pmod{667} = 424$.
- (6) Alice sendet $c = 424$ an Bob.
- (7) Bob berechnet $m = c^d \pmod{n} = 424^{575} \pmod{667} = 11$.