SS 06
Priv.-Doz. Dr. S. Wewers

Kryptographie

Inhalt der Vorlesung

I Einführung in die Kryptographie

- symmetrische und asymmetrische Verschlüsselungsverfahren;
  Bsp.: die Verschiebungschiffre; Kryptoanalyse
- Blockchiffren;
  Bsp.: die Vigenere-Chiffre
- Perfekte Geheimhaltung;
  One-Time-Pad, der Satz von Shannon
- Kriterien für die Sicherheit eines Kryptosystems
- Angriffsarten: Ciphertex-Only, Known-Plaintext,
  Chosen-Plaintext, Chosen-Ciphertext
- Bsp.: Affine Chiffren
- Konfusion/Diffusion
- Moderne Blockchiffren:
  Produktch., Feistel-Ch., DES
- Pseudo-Zufallsfolgen:
  - Kryptographische Sicherheit
  - Randomisieren von Blockchiffren
  - Bsp.: der BBS-Generator
  - Bsp.: lineare u. nichtlineare Schieberegisterfolgen

II Elementare Zahlentheorie

- Teilbarkeit;
  Euklidischer Alg., Eindeutigkeit der Primfaktorzerlegung
- Rechnen mit Kongruenzen:
  - Chinesischer Restesatz
  - Struktur von $(\mathbb{Z}/N)^\times$
  - schnelles Exponentieren
- Primzahlsatz
- quadratische Reste

- endliche Körper

III Kryptosysteme mit öffentlichem Schlüssel

- Einwegfunktionen
- RSA-Verschlüsselung
- Faktorisieren:
  - Pollardsche ρ-Methode
  - $(p-1)$- und $(p+1)$-Methode
  - das quadratische Sieb
- Diffie-Hellman-Schlüsselaustausch, El-Gamal-Verschlüsselung
- Der diskrete Logarithmus:
  - Babystep-Giantstep-Alg.
  - Pollardsche ρ-Methode
  - Pohlig-Hellman-Reduktion
  - Index-Kalkül
  - Zahlkörpersieb
- Elliptische Kurven:
  - affine und projektive ebene Kurven
  - Additionsgesetz auf elliptischen Kurven
  - diskreter Logarithmus auf elliptischen Kurven
  - Schoof-Algorithmus
  - die Höhenfunktion verhindert Index-Kalkül
  - MOV-Attacke
  - anormale Attacke