

Vorlesung über "Kryptographische Algorithmen"

Kryptographie untersucht Verfahren zur Verschlüsselung von Daten und Texten, deren Übertragung sowie im Rahmen der Kryptoanalyse auch deren Angreifbarkeit und Sicherheit, also Möglichkeiten an Schlüssel zu gelangen oder Verschlüsselungen ohne Schlüssel zu knacken.

Im Rahmen der Vorlesung sollen folgende Themen behandelt werden:

- Grundanliegen von Kryptographie und Kryptoanalyse
- Verschlüsselung und Grundfragen der Kodierungstheorie
- Data Encryption Standard
- Grundlagen aus der Theorie endlicher Gruppen
- Primzahlerzeugung und Testung, Faktorisierungsalgorithmen, Diskreter Logarithmus
- Public-Key Kryptographie insbesondere RSA-Algorithmus
- elliptische Kurven
- Komplexitätstheoretische Aspekte der Kryptographie
- Digitale Signaturen, Zero-Knowledgeprotokolle, Authentifizierung
- (evtl. Quantenkryptographie)

In loser Folge werden Übungsaufgaben ausgegeben, die im Rahmen der Vorlesung besprochen werden.

Termine

Die Vorlesung findet dienstags, von 12.00-13.30 Uhr, im Seminarraum 616, 6. Stock, Pohligstr. 1, statt.

Die Vorlesung beginnt am 24.10.2006.

Einordnung und Scheinvergabe

Einordnung: B/D. Vergabe eines Leistungsnachweises durch eine mündliche Prüfung am Ende des Vorlesungszeitraumes.

Literatur

- A. Salomaa, Public-Key Cryptography, Springer-Verlag, 1996.
- J. Buchmann, Introduction to Cryptographie, Springer-Verlag, 2000.
- I. Blake, G. Seroussi, N. Smart, Elliptic Curves in Cryptographie, London Mathematical Society, Vol. 265, Cambridge, 1999.
- Cormen, Leiserson, Rivest, Stein Introduction to Algorithms, MIT Press 2001
- J. Hromkovich Theoretische Informatik, Springer-Verlag, 2004.
- W. Lütkebohmert, Codierungstheorie, Vieweg-Verlag, 2002.
- H. Kurzweil, B. Stellmacher, Theorie der endlichen Gruppen, Springer-Verlag, 1998.
- D. Husemöller, Elliptic Curves, Springer-Verlag, 1987.
- S. Lang, Algebra, Springer-Verlag, 2002.