

Block-Seminar

Kryptographie

Raum: GBIV-318, Zeit: 13. – 15.3.2000, 9:00 – 17:00
Paul Fischer, Lehrstuhl 2, GBVI-332, Tel:4684

Die Grundlage bildet das Buch *Cryptography* von D.R. Stinson, CRC-Press,1995.

Vorträge:

- 1 Kap. 1.1.1 – 1.1.4 und 1.2.1 – 1.2.3: Substitutions- und Vigenère-Chiffren und ihre Analyse.
- 2 Kap. 1.1.5 – 1.1.7 und 1.2.4 – 1.2.5: Hill-, Permutations- und Stream-Chiffren und ihre Analyse.
- 3 Kap. 2: Shannons Theorie der Kryptosysteme.
- 4 Kap. 3.1 – 3.5: Arbeitsweise und Anwendungen des Data Encryption Standards (DES).
- 5 Kap. 3.6 – 3.7: Kryptanalytische Angriffe auf den Data Encryption Standard.
- 6 Kap. 4.1 – 4.5: Arbeitsweise und Anwendungen RSA-Kryptosystems.
- 7 Kap. 4.6 – 4.9: Kryptanalytische Angriffe auf das RSA-Kryptosystem und das Rabin-Kryptosystem.
- 8 Kap. 5.1: Das ElGamal Kryptosystem.
- 9 Kap. 6.1 – 6.5: Digitale Signaturen.
- 10 Kap. 9: Identifikations-Schemata.
- 11 Kap. 10: Authentifikations-Schemata.
- 12 Kap. 11.1 – 11.6: Verteilte Geheimnisse

Weitere Literatur:

- C.H. Meyer, S.M. Matyas, *Cryptography*, Wiley-Interscience, 1982.
- A. Salomaa, *Public-Key Cryptography*, Springer-Verlag, 1989.
- F.L. Bauer, *Entzifferte Geheimnisse*, Springer-Verlag, 1997.