Literaturempfehlungen zur Vorlesung Datensicherheit

Einige Beispiele für weiterführende Literatur, alphabetisch geordnet.

Kapitel 1 – 4:

[Ayco_06] John Aycock: Computer Viruses and Malware. Springer, 2006.

[KeKl_05] Heinrich Kersten, Gerhard Klett: Der IT-Security Manager. Vieweg Verlag, 2005.

[KöNi_05] Hans-Peter Königs: IT-Risiko-Management mit System. Vieweg Verlag, 2003.

[Pfit_00] Andreas Pfitzmann: Sicherheit in Rechnernetzen: Mehrseitige Sicherheit in verteilten und durch verteilte Systeme. Vorlesungsskript, TU Dresden, 2000.

[Weck_84] Gerhard Weck: Datensicherheit: Methoden, Maßnahmen und Auswirkungen des Schutzes von Informationen. Teubner Stuttgart, 1984.

Kapitel 5:

[ScKP_12] Dagmar Schönfeld, Herbert Klimant, Rudi Piotraschke: Informations- und Kodierungstheorie. 4. Aufl., Springer Vieweg, 2012.

Kapitel 6-7:

[BaFP_14] Ulrike Baumann, Elke Franz, Andreas Pfitzmann: Kryptographische Systeme. Springer, 2014..

[BeNS_05] Albrecht Beutelspacher, Heike B. Neumann, Thomas Schwarzpaul: Kryptographie in Theorie und Praxis. Vieweg & Sohn Verlag, 2005.

[Buch_03] Johannes Buchmann: Einführung in die Kryptographie. 3., erw. Aufl., Springer, 2003.

[DiHe_76] Whitfield Diffie, Martin E. Hellman: New Directions in Cryptography. IEEE Transaction on Information Theory, vol. IT-22, no. 6, November 1976, 644-654.

[ElGa_84] Taher ElGamal: A Public Key cryptosystem and a Signature Scheme Based on Discrete Logarithms. CRYPTO ’84, Springer-Verlag, 10-18 / IEEE Transaction on Information Theory, vol. IT-31, no. 4, July 1985, 469-472.

[FIPS_77] Federal Information Processing Standard Publication (FIPS PUB 46): Data Encryption Standard (DES). 1977.

[FIPS_81] Federal Information Processing Standard Publication (FIPS PUB 81): Data Modes of Operation. 1980.

[FIPS_99] Federal Information Processing Standard Publication (FIPS PUB 46-3): Data Encryption Standard (DES). 1999.

[FIPS_01] Federal Information Processing Standard Publication (FIPS PUB 197): Specification for the Advanced Encryption standard (AES). 2001.

[Frid_10] Jessica Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press, 2010.

[FuRi_94] Walter Fumy, Hans Peter Rieß: Kryptographie – Entwurf, Einsatz und Analyse symmetrischer Kryptoverfahren. 2., akt. und wesentl. erw. Auflage, R. Oldenbourg Verlag, 1994.

[MeOV_96] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone: Handbook of Applied Cryptography. CRC Press, 1996.

[Mill_03] Michael Miller: Symmetrische Verschlüsselungsverfahren – Design, Entwicklung und Kryptoanalyse klassischer und moderner Chiffren. Teubner, 2003.

[Pfit_00] Andreas Pfitzmann: Sicherheit in Rechnernetzen: Mehrseitige Sicherheit in verteilten und durch verteilte Systeme. Vorlesungsskript, TU Dresden, 2000.

[RiSA_78] Ronald L. Rivest, Adi Shamir, Leonhard M. Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, vol. 21, no. 2, 1978, 120-126.

[Schn_96] Bruce Schneier: Applied Cryptography. John Wiley & Sons. 1996.