Kryptographie und Kryptoanalyse
Literaturhinweise

- Begleitbuch inkl. Übungen und Musterlösungen: [1]
- Auswahl weiterer Bücher: [5, 10, 25, 30, 41, 45]
- Schlüsselaustausch: [9]
- Sicherheit kryptographischer Systeme:
  - Informationstheoretische Sicherheit: [42]
  - Weitere Sicherheitsbegriffe: [23, 33, 39, 15, 43, 3, 2, 28, 27]
- Klassische Verfahren: [22, 31, 44]
- Symmetrische Verfahren:
  - Analyse u.a. auch in [46]
  - DES: [19, 20, 11, 22, 31]
    differentielle Kryptoanalyse: [6]
    lineare Kryptoanalyse: [29]
  - AES: [18, 13]
  - Betriebsarten: [21, 34, 35, 36, 37]
- Asymmetrische Verfahren:
  - Diffie-Hellman-Schlüusselaustausch: [14]
  - RSA: [40, 7]; Padding: [4, 8]
  - Rabin: [38, 8]
  - ElGamal: [16, 17]
  - System von Cramer und Shoup: [12]
  - Elliptische Kurven: [32, 26, 24]

Literatur

[1] U. Baumann, E. Franz, and A. Pfitzmann: *Kryptographische Systeme*. Springer, 2014.

[2] M. Bellare: *Practice-Oriented Provable-Security*. In *Proceedings of the 1997 Information Security Workshop (ISW)*, pp. 221–231, Springer, 1998.

[3] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway: *Relations Among Notions of Security for Public-Key Encryption Schemes*. In H. Krawczyk (ed.), *Advances in Cryptology – Crypto '98*, vol. 1462 of *LNCS*, pp. 26 – 46, 1998.

[4] M. Bellare and P. Rogaway: *Optimal Asymmetric encryption – How to Encryt with RSA*. In A. D. Santis (ed.), *Advances in Cryptology – Eurocrypt '94*, vol. 950 of *LNCS*, pp. 92 – 111, Springer, 1995.

[5] A. Beutelspacher, H. B. Neumann, and T. Schwarzpaul: *Kryptographie in Theorie und Praxis*. Vieweg & Sohn Verlag, 2005.

[6] E. Biham and A. Shamir: *Differential Cryptanalysis of DES-like Cryptosystems*. In *Advances in Cryptology – CRYPTO '90*, pp. 2 – 21, 1990.

[7] D. Bleichenbacher: *Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1*. In *Advances in Cryptology - CRYPTO '98*, pp. 1 – 12, 1998.

[8] D. Boneh: *Simplified OAEP for the RSA and Rabin Functions*. In *Advances in Cryptology - CRYPTO '01*, no. 2139 in LNCS, pp. 275 – 291, Springer, 2001.

[9] C. Boyd and A. Mathuria: *Protocols for Authentication and Key Establishment*. Springer, 2003.

[10] J. Buchmann: *Einführung in die Krytographie*. Springer, 4., erw. Aufl., 2008.

[11] D. Coppersmith: *The Data Encryption Standard (DES) and its strength against attacks*. *IBM Journal of Research and Development*, vol. 38(3):pp. 243–250, May 1994.

[12] R. Cramer and V. Shoup: *A Practical Public Key Cryptosystem Secure against Adaptive Chosen Ciphertext Attack*. In *Advances in Cryptology – Crypto '98*, pp. 13 – 25, 1998.

[13] J. Daemen and V. Rijmen: *The Design of Rijndael*. Springer Berlin Heidelberg, 2002.

[14] W. Diffie and M. E. Hellman: *New Directions in Cryptography*. *IEEE Transactions on Information Theory*, vol. 22(6):pp. 644 – 654, 1976.

[15] D. Dolev, C. Dwork, and M. Naor: *Non-Malleable Cryptography.* In *23rd Annual ACM Symposium on Theory of Computing (STOC '91)*, pp. 542–552, 1991.

[16] T. ElGamal: *A Public Key cryptosystem and a Signature Scheme Based on Discrete Logarithms.* In *Advances in Cryptology – CRYPTO '84*, pp. 10 – 18, 1985.

[17] T. ElGamal: *A Public Key cryptosystem and a Signature Scheme Based on Discrete Logarithms. IEEE Transactions on Information Theory*, vol. 31(4):pp. 469 – 472, 1985.

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

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

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

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

[22] W. Fumy and H. P. Rieß: *Kryptographie: Entwurf, Einsatz und Analyse symmetrischer Kryptoverfahren.* R. Oldenbourg Verlag München Wien, 2., akt. und wesentl. verb. Auflage, 1994.

[23] S. Goldwasser and S. Micali: *Probabilistic Encryption. Journal of Computer and System Sciences*, vol. 28(2):pp. 270 – 299, April 1984.

[24] D. Hankerson, A. Menezes, and S. Vanstone: *Guide to Elliptic Curve Cryptography.* Springer, 2004.

[25] J. Katz and Y. Lindell: *Introduction to Modern Cryptography.* Chapman & Hall/CRC, 2008.

[26] N. Koblitz: *Elliptic Curves Cryptosystems. Mathematics of Computation*, pp. 203 – 209, 1987.

[27] N. Koblitz: *The Uneasy Relationship Between Mathematics and Cryptography. Notices of the AMS*, vol. 54:pp. 972 – 979, 2007.

[28] N. Koblitz and A. J. Menezes: *Another Look at Provable Security. Journal of Cryptology*, vol. 20:pp. 3 – 37, 2004.

[29] M. Matsui: *Linear Cryptanalysis Method for DES Cipher.* In *Advances in Cryptology – EUROCRYPT '93*, pp. 386 – 397, 1993.

[30] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone: *Handbook of Applied Cryptography.* CRC Press, 1996.

[31] M. Miller: *Symmetrische Verschlüsselungsverfahren – Design, Entwicklung und Kryptoanalyse klassischer und moderner Chiffren.* Teubner, 2003.

[32] V. S. Miller: *Use of Elliptic Curves in Cryptography.* In *Advances in Cryptology – CRYPTO '85*, pp. 417 – 426, 1986.

[33] M. Naor and M. Yung: *Public-key Cryptosystems Provably Secure against Chosen Ciphertext Attacks.* In *22nd ACM Symposium on Theory of Computing*, pp. 427 – 437, 1990.

[34] NIST Special Publication 800-38A: *Recommendation for Block Cipher Modes of Operation – Methods and Techniques.* U.S. DoC/NIST, http://csrc.nist.gov/groups/ST/toolkit/BCM/current_modes.html, December 2001.

[35] NIST Special Publication 800-38B: *Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication.* U.S. DoC/NIST, http://csrc.nist.gov/groups/ST/toolkit/BCM/current_modes.html, May 2005.

[36] NIST Special Publication 800-38C: *Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality.* U.S. DoC/NIST, http://csrc.nist.gov/groups/ST/toolkit/BCM/current_modes.html, May 2004.

[37] NIST Special Publication 800-38D: *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.* U.S. DoC/NIST, http://csrc.nist.gov/groups/ST/toolkit/BCM/current_modes.html, November 2007.

[38] M. O. Rabin: *Digitalized signatures and public-key functions as intractable as factorization.* Tech. Rep. LCS/TR-212, MIT Lab. for Computer Science, 1979.

[39] C. Rackoff and D. R. Simon: *Non-interactive Proof of Knowledge and Chosen Ciphertext Attack.* In *Advances in Cryptology - CRYPTO '91*, pp. 433–444, 1991.

[40] R. L. Rivest, A. Shamir, and L. Adleman: *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM*, vol. 21(2):pp. 120 – 126, February 1978.

[41] B. Schneier: *Applied Cryptography.* John Wiley & Sons, 1996.

[42] C. E. Shannon: *Communication Theory of Secrecy Systems. Bell Systems Technical Journal*, vol. 28:pp. 656–715, 1949.

[43] V. Shoup: *Why chosen Ciphertext Security Matters.* Tech. Rep. RZ 3076, IBM Research Division, 1998.

[44] S. Singh: *Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet.* Dtv, 2001.

[45] D. R. Stinson: *Cryptography: Theory and Practice*. Chapman & Hall/CRC, 3rd ed., 2006.

[46] C. Swenson: *Modern Cryptanalysis: Techniques for Advanced Code Breaking*. Wiley Publishing, Inc., 2008.