

# Cryptography

## References

- [1] T. H. Barr. *Invitation to Cryptology*. Prentice Hall, Upper Saddle River, 2002.
- [2] A. Beutelspacher, J. Schwenk, and K. D. Wolfenstetter. *Moderne Verfahren in der Kryptographie*. Vieweg, Wiesbaden, 1995.
- [3] E. Biham and A. Shamir. *Differential Cryptanalysis of the Full 16-Round DES, Lecture Notes in Computer Science 740*. Springer, 1993.
- [4] J. Buchmann. *Einführung in die Kryptographie*. Springer, Berlin, 2nd edition, 2001.
- [5] J. Buchmann. *Introduction to Cryptography*. Springer, New York, 2nd edition, 2004.
- [6] H. Delfs and H. Knebl. *Introduction to Cryptography, Principles and Applications*. Springer, Berlin, 2002.
- [7] D. E. Denning. *Cryptography and Data Security*. Addison-Wesley, 1983.
- [8] W. Fumy and H. P. Rieß. *Kryptographie*. Oldenburg, München, 2nd edition, 1994.
- [9] D. Hankerson, A. Menezes, and S. A. Vanstone. *Guide to Elliptic Curve Cryptography*. Springer, New York, 2004.
- [10] D. R. Hankerson, D. G. Hoffman, D. A. Leonard, C. C. Lindner, K. T. Phelps, C. A. Rodger, and J. R. Well. *Coding Theory and Cryptography, the Essentials*. Marcel Dekker, New York, 2000.
- [11] N. Koblitz. *A Course in Number Theory and Cryptography*. Springer, Berlin, 2nd edition, 1994.
- [12] N. Koblitz. *Algebraic Aspects of Cryptography*. Springer, Berlin, 1998.
- [13] A. G. Kohnheim. *Cryptography, A Primer*. Wiley, New York, 1981.
- [14] E. Kranakis. *Primality and Cryptography*. Wiley-Teubner, Stuttgart, 1986.
- [15] M. Luby. *Pseudorandomness and Cryptographic Applications*. Princeton University Press, Princeton, 1996.
- [16] R. Mathar. *Informationstheorie*. Teubner, Stuttgart, 1996.
- [17] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, Boca Raton, 1996 (<http://www.cacr.math.uwaterloo.ca/hac>).
- [18] C. H. Meyer and S. Matyas. *Cryptography*. Wiley, New York, 1982.
- [19] M. Miller. *Symmetrische Verschlüsselungsverfahren*. Teubner, Stuttgart, 2003.
- [20] A. Salomaa. *Public-Key Cryptography*. Springer, Berlin, 1990.

- [21] B. Schneier. *Applied Cryptography*. Wiley, New York, 2nd edition, 1996.
- [22] B. Schneier. *Secrets and Lies*. Wiley, Indianapolis, 2000.
- [23] B. Schneier. *Angewandte Kryptographie*. Wiley, München, 2006.
- [24] J. Seberry and J. Pieprzyk. *Cryptography: An Introduction to Computer Security*. Prentice-Hall, New York, 1989.
- [25] A. Sinkov. *Elementary Cryptanalysis*. MAA Publications, 1996.
- [26] D. R. Stinson. *Cryptography, Theory and Practice*. CRC Press, Boca Raton, 1995.
- [27] D. R. Stinson. *Cryptography, Theory and Practice*. Chapman and Hall/CRC, Boca Raton, 2nd edition, 2002.
- [28] D. R. Stinson. *Cryptography, Theory and Practice, Third Edition*. Chapman and Hall/CRC, Boca Raton, 3rd edition, 2006.
- [29] W. Trappe and L. C. Washington. *Introduction to Cryptography with Coding theory*. Prentice Hall, Upper Saddle River, 2002.
- [30] H. C. A. van Tilborg. *An Introduction to Cryptology*. Kluwer Academic Publishers, Boston, 1990.
- [31] D. Welsh. *Codes and Cryptography*. Clarendon Press, Oxford, 1989.
- [32] A. Werner. *Elliptische Kurven in der Kryptographie*. Springer, Berlin, 2002.