Literatur

1. Advanced Encryption Standard, http://csrc.nist.gov/encryption/aes/
2. M. Agraval, N. Kayal, N. Saxena, Primes is in P, http://www.cse.iitk.ac.in/news/primality.html
3. A. Aho, J. Hopcroft, J. Ullman, *The Design and Analysis of Computer Algorithms* (Addison-Wesley, Reading, Massachusetts, 1974)
4. E. Bach, J. Shallit, *Algorithmic Number Theory* (MIT Press, Cambridge, Massachusetts and London, England, 1996)
5. F. Bauer, *Entzifferte Geheimnisse* (Springer, Berlin, 1995)
6. F. Bauer, *Decrypted Secrets* (Springer, Berlin, 2000)
7. M. Bellare, P. Rogaway, The exact security of digital signatures: How to sign with RSA and Rabin, in *Advances in Cryptology – EUROCRYPT '96* (Springer, 1996), S. 399–416
8. M. Bellare, P. Rogaway, Optimal asymmetric encryption – how to encrypt with RSA, in *Advances in Cryptology – EUROCRYPT '94* (Springer, 1996), S. 92–111
9. M. Bellare, R. Canetti, H. Krawczyk, Keying hash functions for message authentication, in *Advances in Cryptology – CRYPTO '96*, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18–22, 1996, S. 1–15
10. D.J. Bernstein, J. Buchmann, E. Dahmen (Hrsg.), *Post-Quantum Cryptography* (Springer, 2008)
11. D.J. Bernstein, D. Hopwood, A. Hülsing, T. Lange, R. Niederhagen, L. Papachristodoulou, M. Schneider, P. Schwabe, Z. Wilcox-O'Hearn, SPHINCS: practical stateless hash-based signatures, in *Advances in Cryptology – EUROCRYPT 2015*, 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26–30, 2015, Proceedings, Part I, S. 368–397
12. A. Beutelspacher, J. Schwenk, K.-D. Wolfenstetter, *Moderne Verfahren der Kryptographie* (Vieweg, 1998)
13. E. Biham, A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard* (Springer, New York, 1993)
14. I.F. Blake, G. Seroussi, N.P. Smart, *Elliptic Curves in Cryptography* (Cambridge University Press, Cambridge, England, 1999)
15. D. Bleichenbacher, Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS#1, in *Advances in Cryptology – CRYPTO '98*, 1998, S. 1–12
16. D. Boneh, The decision Diffie-Hellman problem, in *ANTS III*, *Lecture Notes in Computer Science*, Bd. 1423, (Springer, Berlin, 1998), S. 48–63

J. Buchmann, *Einführung in die Kryptographie*, Springer-Lehrbuch,
DOI 10.1007/978-3-642-39775-2

17. D. Boneh, G. Durfee, Cryptanalysis of RSA with private keys d less than $N^{0.292}$, IEEE Transact. Inf. Theory **46**(4), 1339–1349 (2000)

18. J. Buchmann, Faktorisierung großer Zahlen. Spektrum Wiss. **9**, 80–88 (1996)

19. J. Buchmann, S. Paulus, A one way function based on ideal arithmetic in number fields, in *Advances in Cryptology – CRYPTO '97*, *Lecture Notes in Computer Science*, Bd. 1294, hrsg. von B. Kaliski (Springer, Berlin, 1997), S. 385–394

20. J. Buchmann, H.C. Williams, Quadratic fields and cryptography, in *Number Theory and Cryptography*, *London Mathematical Society Lecture Note Series*, Bd. 154, hrsg. von J.H. Loxton (Cambridge University Press, Cambridge, England, 1990), S. 9–25

21. J.A. Buchmann, E.G. Karatsiolis, A. Wiesmaier, *Introduction to Public Key Infrastructures* (Springer, 2013)

22. T.H. Cormen, C.E. Leiserson, R.L. Rivest, *Introduction to Algorithms* (MIT Press, Cambridge, Massachudetts, 1990)

23. R. Cramer, V. Shoup, Signature schemes based on the strong rsa assumption. ACM Transact. Inf. Syst. Theory **3**, 161–185 (2000)

24. N.G. de Bruijn, On the number of integers $\leq x$ and free of prime factors $> y$. Indag. Math. **38**, 239–247 (1966)

25. W. Diffie, M.E. Hellman, New directions in cryptography. IEEE-IT **IT-22**, 644–654 (1976)

26. Discrete Logarithm Records, https://en.wikipedia.org/wiki/Discrete_logarithm_records#Integers_modulo_p

27. Factoring records, http://www.crypto-world.com/FactorRecords.html

28. A. Fiat, M. Naor, Rigorous time/space trade offs for inverting functions, in *23rd ACM Symp. on Theory of Computing (STOC)* (ACM Press, 1991), S. 534–541

29. A. Fiat, A. Shamir, How to prove yourself: practical solutions to identification and signature problems, in *Advances in Cryptology – CRYPTO '86*, *Lecture Notes in Computer Science*, Bd. 263, hrsg. von A.M. Odlyzko (Springer, 1986), S. 186–194

30. FIPS 186-4, Digital Signature Standard (DSS). Federal Information Processing Standards Publication 186-4, U.S. Department of Commerce/N.I.S.T., National Technical Information Service, Springfield, Virginia, 2013.

31. O. Goldreich, *Modern Cryptography, Probabilistic Proofs and Pseudorandomness* (Springer, New York, 1999)

32. S. Goldwasser, S. Micali, Probabilistic encryption. J. Comput. Syst. Sci. **28**, 270–299 (1984)

33. D.M. Gordon, A survey of fast exponentiation methods. J. Algorithms **27**, 129–146 (1998)

34. M. Hellman, A cryptanalytic time-memory trade-off. IEEE Transact. Inf. Theory **26**(4), 401–406 (1980)

35. P. Horster, *Kryptologie* (Bibliographisches Institut, 1987)

36. ISO/IEC 9796, Information technology – Security techniques – Digital signature scheme giving message recovery (International Organization for Standardization, Geneva, Switzerland, 1991)

37. D. Kahn, *The codebreakers* (Macmillan Publishing Company, 1967)

38. L.R. Knudsen, Contemporary block ciphers, in *Lectures on Data Security*, *LNCS*, Bd. 1561, hrsg. von I. Damgard (Springer-Verlag, New York, 1999), S. 105–126

39. D.E. Knuth, *The art of computer programming. Volume 2: Seminumerical algorithms* (Addison-Wesley, Reading, Massachusetts, 1981)
40. N. Koblitz, *A Course in Number Theory and Cryptography* (Springer, 1994)
41. L. Lamport, Constructing digital signatures from a one way function. Technical Report SRI-CSL-98, SRI International Computer Science Laboratory, 1979
42. A.K. Lenstra, H.W. Lenstra, Jr., Algorithms in number theory, in *Handbook of Theoretical Computer Science, Volume A, Algorithms and Complexity*, Kap. 12, hrsg. von J. van Leeuwen (Elsevier, Amsterdam, 1990)
43. A.K. Lenstra, H.W. Lenstra Jr., Algorithms in number theory, in *Handbook of Theoretical Computer Science. Volume A. Algorithms and Complexity*, Kap. 12, hrsg. von J. van Leeuwen (Elsevier, 1990), S. 673–715
44. A.K. Lenstra, H.W. Lenstra Jr. (Hrsg.), The Development of the Number Field Sieve, in *Lecture Notes in Math* (Springer, Berlin, 1993)
45. H.W. Lenstra, Jr., C. Pomerance, A rigorous time bound for factoring integers. J. AMS **5**, 483–516 (1992)
46. H.R. Lewis, C.H. Papadimitriou, *Elements of the Theory of Computation* (Prentice-Hall, Englewood Cliffs, NJ, 1981)
47. LiDIA, www.informatik.tu-darmstadt.de/TI/Welcome-Software.html
48. A. Menezes, *Elliptic Curve Public Key Cryptosystems* (Kluwer Academic Publishers, Dordrecht, 1993)
49. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography* (CRC Press, Boca Raton, Florida, 1997)
50. R.C. Merkle, A certified digital signature, in *CRYPTO '89: Proceedings on Advances in Cryptology*, *Lecture Notes in Computer Science*, Bd. 435 (Springer, 1989), S. 218–238
51. K. Meyberg, *Algebra Teil 1* (Carl Hanser, 1980)
52. K. Meyberg, *Algebra Teil 2* (Carl Hanser, 1980)
53. B. Möller, Improved techniques for fast exponentiation, in *Proceedings of ICISC 2002* (Springer, 2003)
54. E. Oeljeklaus, R. Remmert, *Lineare Algebra I* (Springer, Berlin, 1974)
55. J. Overbey, W. Traves, J. Wojdylo, On the keyspace of the hill cipher. Cryptologia **29**, 59–72 (2005)
56. PKCS#1, www.rsasecurity.com/rsalabs/pkcs/pkcs-1/index.html
57. D. Pointcheval, J. Stern, Security arguments for digital signatures and blind signatures. J. Cryptol. **13**, 361–396 (2000)
58. H. Riesel, *Prime Numbers and Computer Methods for Factorization* (Birkhäuser, Boston, 1994)
59. R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**, 120–126 (1978)
60. R. Rompel, One-way functions are necessary and sufficient for secure signatures, in *22nd ACM Symp. on Theory of Computing (STOC)*, 1990, S. 387–394
61. M. Rosing, *Implementing Elliptic Curve Cryptography* (Manning, 1999)
62. J. Rosser, L. Schoenfeld, Approximate formulas for some functions of prime numbers. Illinois J. Math. **6**, 64–94 (1962)

63. R.A. Rueppel, *Analysis and Design of Stream Ciphers* (Springer, Berlin, 1986)

64. O. Schirokauer, D. Weber, T. Denny, Discrete logarithms: the effectiveness of the index calculus method, in *ANTS II*, *Lecture Notes in Computer Science*, Bd. 1122, hrsg. von H. Cohen (Springer, Berlin, 1996)

65. B. Schneier, *Applied Cryptography*, 2. Aufl. (Wiley, New York, 1996)

66. C.P. Schnorr, Efficient signature generation by smart cards, in *Advances in Cryptology – CRYPTO '89*, Lecture Notes in Computer Science (Springer, 1991), S. 161–174

67. A. Shamir, How to share a secret. Commun. ACM **22**, 612–613 (1979)

68. C.E. Shannon, Communication theory of secrecy systems. Bell Sys. Tech. J. **28**, 656–715 (1949)

69. P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. **26**, 1484–1509 (1997)

70. V. Shoup, OAEP reconsidered, in *Advances in Cryptology – CRYPTO 2001* (Springer, 2001), S. 239–259

71. D. Stinson, *Cryptography* (CRC Press, Boca Raton, Florida, 1995)

72. D. Stinson, *Cryptography, Theory and Practice*, 2. Aufl. (CRC Press, Boca Raton, Florida, 2002)

73. Yearly report on algorithms and keysizes, ICT-2007-216676 ECRYPT II, 2012

Sachverzeichnis