30. Januar 2002. U. Schoenwaelder; *http://www.math.rwth-aachen.de/∼Ulrich.Schoenwaelder*
HB = Hochschulbibl. RWTH, HBZ = *http://www.hbz-nrw.de/* (HBZ-CD-ROM Online), MB = Mathematikbibl., DB = Didaktikbibl. (Winter), FH = Bibl. Fachhochschule Aachen, FL = Fernleihe, IB Nr. Institutsbibliothek Nr., LB = HB–Lehrbuchsammlung, LS = HB–Lesesaal

Literatur zur Kryptographie

[1] Designs, Codes and Cryptography. Zeitschrift des Kluwer-Verlages, ab 1991. RWTH, Informatikbibliothek: 2.1992 - 15.1998. ISSN 0925-1022.

[2] F. L. Bauer. *Kryptologie: Methoden und Maximen*. Springer-Lehrbuch. Springer–Verlag, 1993, ^{2}1994. HB: Bf9446, +2. ISBN 3-540-56356-3, 3-540-57771-8. Allgemein, nur elementare mathematische Kenntnisse erforderlich.

[3] F. L. Bauer. *Entzifferte Geheimnisse: Methoden und Maximen der Kryptologie*. Springer–Verlag, 1994, ^{2}1997. HB: Bf9554, +2. ISBN 3-540-58118-9, 3-540-62632-8.

[4] A. Beutelspacher. *Kryptologie. Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen*. Vieweg, 1987, ^{2}1991, ^{4}1994, ^{5}1998. MB: 16074; HB: Bb1874+3, +4, +5. ISBN .., 3-528-48990-1.

[5] A. Beutelspacher, J. Schwenk, and K.-D. Wolfenstetter. *Moderne Verfahren der Kryptographie: von RSA zu Zero-Knowledge*. Vieweg: Mathematik. Vieweg, ^{2}1998. HB: Bf9692+2. ISBN 3-528-16590-1.

[6] C. Boyd, editor. *Cryptography and Coding (Fifth IMA Conference, Cirencester, 1995)*, LNCS 1025. Springer-Verlag, 1995. HB: Za6315-1025. ISBN 3-540-60693-9.

[7] Johannes Buchmann. *Einführung in die Kryptographie*. Springer-Lehrbuch. Springer–Verlag, 1999. ISBN 3-540-66059-3.

[8] Peter Bundschuh. *Einführung in die Zahlentheorie*. Hochschultext. Springer–Verlag, 1988, ^{3}1996. MB: Bf9021, Bf9021+3. ISBN 0-387-15305-5, 3-540-60920-2. RSA: S. 101-102.

[9] Dorothy E. R. Denning. *Cryptography and Data Security*. Addison Wesley, 1983, Reprinted with corrections. RWTH, Med. Inst. 710. ISBN 0-201-10150-5.

[10] A. K. Dewdney. Die Geschichte der legendären ENIGMA: Teil I der Abhandlung über das Erzeugen und Knacken von Chiffrier-Codes zur Übermittlung geheimer Nachrichten. *Spektrum der Wissenschaft (Scientific American)*, Dezember:8–11, 1988. ISSN 0170-2971. Fortsetzung: [11].

[11] A. K. Dewdney. Über moderne Computer-Verschlüsselungsmethoden berichtet Teil II der Abhandlung über das Erzeugen und Knacken von Chiffrier-Codes zur Übermittlung geheimer Nachrichten. *Spektrum der Wissenschaft (Scientific American)*, Januar:6–10, 1989. ISSN 0170-2971. Teil I: [10].

[12] Ole Immanuel Franksen. *Mr. Babbage's Secret: the Tale of a Cypher – and APL*. Prentice-Hall, 1985. HBZ. ISBN 0-13-604729-7. History of cryptology.

[13] S. Goldwasser and C. Pomerance, editors. *Cryptology and Computational Number Theory (AMS Short Course, Boulder, 1989)*, Proceedings of symposia in applied mathematics 42: AMS short course lecture notes. AMS, 1990. HBZ. ISBN 0-8218-0155-4. Enthält [25].

[14] Dieter Gollmann. *Algorithmenentwurf in der Kryptographie*. Aspekte komplexer Systeme 1. BI, Wiss.-Verlag, 1994. HB: Bf9494-1+1. ISBN 3-411-16671-1. Habil.-Schrift Karlsruhe 1990.

[15] A. Hermans. Verschlüsselung und Entschlüsselung von Nachrichten. *Praxis der Mathematik*, 31(5):262–270, 1989. MB: Z 101; HB: Z 1757.

[16] Andrew Hodges. *Alan Turing: the Enigma*. Computerkultur 1. Springer-Verlag, 1994. HB: Bm9503-1+2. ISBN 3-211-82627-0. 1. Aufl. im Verlag Kammerer & Unverzagt, Berlin.

[17] R. Honsberger. Ch. 10: Four clever schemes in cryptography. In R. Honsberger, editor, *Mathematical Gems III*, Dolciani Mathematical Expositions 9, pages 151–173. MAA, 1985. MB: 13398.

[18] T. H. Jackson. *From Number Theory to Secret Codes: a Computer Illustrated Text*. Hilger, 1987. HBZ 361. ISBN 0-85274-077-8. Mit Diskette.

[19] H. Kleiner. Das RSA–Verfahren. *Praxis der Mathematik*, 26(5):133–140, 1984. MB: Z 101; HB: Z 1757.

[20] Neal Koblitz. *A Course in Number Theory and Cryptography*. GTM 114. Springer–Verlag, 1987, ^{2}1994. MB: 13939; HB: Bb1244-114+2. ISBN 0-387-94293-9, 3-540-94293-9. Ch. I: Some topics in elementary number theory; §1: Time estimates for doing arithmetic, §2: Divisibility and the Euclidean algorithm, §3: Congruences (Fermat's Little Theorem, Chinese Remainder Theorem), §4: Some applications to factoring. Ch. II: Finite fields and quadratic residues. Ch. III: Cryptography. Ch. IV: Public Key. Ch. V: Primality and Factoring. Ch. VI: Elliptic Curves (cryptosystems, factorization).

[21] Neal Koblitz, editor. *Advances in Cryptology (CRYPTO '96, Santa Barbara, 1996)*, LNCS 1109. Springer-Verlag, 1996. HB: Za6315-1109. ISBN 3-540-61512-1.

[22] Neal Koblitz. *Algebraic Aspects of Cryptography*. Algorithms and computation in mathematics 3. Springer–Verlag, 1998. HB: Bb532-3. ISBN 3-540-63446-0.

[23] E. Kranakis. *Primality and Cryptography*. Wiley, 1986. HB: Bm5232.

[24] Rudolf Mathar. Von Geheimschriften über perfekte Sicherheit zu Public-Key-Kryptosystemen. Vortragsangebot für Schüler der Sekundarstufe II: www.math1.rwth-aachen.de/schule.html, 1999.

[25] K. S. McCurley. Odds and ends from cryptology and computational number theory. In S. Goldwasser and C. Pomerance, editors, *Cryptology and Computational Number Theory*, Proc. Symp. Appl. Math. 42, pages 145–166. AMS, 1990. Artikel aus [13]. Attacks on RSA.

[26] A. J. Menezes, editor. *Advances in Cryptology (CRYPTO '90, Santa Barbara, 1990)*, LNCS 537. Springer–Verlag, 1991. HB: Za6315-537. ISBN 3-540-54508-5.

[27] A. J. Menezes. *Elliptic Curve Public Key Cryptosystems*. The Kluwer Intern. Ser. in Engineering and Computer Science 234. Kluwer, 1993.

[28] G. L. Mullen and P. J.-S. Shue, editors. *Finite Fields, Coding Theory, and Advances in Communications and Computing (Conf. .., Las Vegas, 1991)*, LNPAM 141. Dekker, 1992. HBZ. ISBN 0-8247-8805-2. Enthält [29].

[29] H. Niederreiter. Finite fields and cryptology. In G. L. Mullen and P. J.-S. Shue, editors, *Finite Fields, Coding Theory, and Advances in Communications and Computing (Conf. .., Las Vegas, 1991)*, LNPAM 141. Dekker, 1992. In [28].

[30] R. Remmert and P. Ullrich. *Elementare Zahlentheorie*. Birkhäuser, ^{2}1995. HB: Bf915+2 LB, B01303 Aufsicht LS. ISBN 3-7643-5197-7. Primfaktorzerlegung, ggT, Dezimalsystem, Kongruenzen, primitive Wurzeln, Reziprozitätsgesetz für quadratische Reste. Satz von Fermat-Euler in der Kryptographie.

[31] R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public key cryptosystems. *Communications ACM*, 21:120–126, 1978.

[32] Arto Salomaa. *Public Key Cryptography*. EATCS monographs on theoretical computer science 23; Texts in theoretical computer science. Springer–Verlag, 1990; ^{2}1996. HB: Bm5806-23+1; Bn6024+2. ISBN 3-540-52831-8, 0-387-52831-8; ISBN 3-540-61356-0.

[33] B. Schröder. Schnüffeln am Ende; Datenverschlüsselung – Bonn muß die Fakten erkennen. *DIE ZEIT*, 37:76, 8. Sept. 1995.

[34] I. Shparlinski. *Number Theoretic Methods in Cryptography: Complexity Lower Bounds*. PCS 17. Birkhäuser, 1999. ISBN 3-7643-5888-2.