Literaturliste zur Kryptologie und ihrer Didaktik

Stand: 6. Mai 2019

(Diese Liste erhebt keinen Anspruch auf Vollständigkeit.
Für die Einführung in die Kryptologie unserer Ansicht nach besonders geeignete Bücher und Artikel sind durch $\star$ gekennzeichnet. Einige Werke sind mehrfach aufgelistet.)

Inhaltsverzeichnis

1 Unterhaltungsliteratur

A. Conan Doyle: (Tanzende Männchen)

Umberto Eco: Das Foucaultsche Pendel. Dtv. Carl Hauser Verlag, München, Wied 1989 (Il pendolo di Foucault 1988)

Umberto Eco: Der Name der Rose. Dtv. Carl Hauser Verlag

Esslinger, B. u. a. : Das CrypTool-Skript -Kryptographie, Mathematik und mehr. 2010[10]. **Anhang A3** (S. auch diese Liste Nr.4) http://www.cryptool.com/download/CrypToolScript-de.pdf

⋆ R. Harris: Enigma. Heyne Verlag, München 1995

Tom Hillenbrand: Der Kaffeedieb. Kiepenheuer& Witsch 2016. ISBN-13: 978-3462048513

Tom Hillenbrandt: Des Königs NSA: 1684 statt 1984. Kindle Edition/epubli.2016

⋆ Edgar A. Poe: Der Goldkäfer. In: Der Mord in der Rue Morgue. RoRoRo 1959

⋆ D. L. Sayers: Zur fraglichen Stunde. RoRoRo 1983

2 Schulbezogen bzw. schüler(innen)bezogen

Baumann, Rüdeger: Digitales Geld. Bestellen und Bezahlen im Internet. Log In 17/2 (1997) 30-38)

⋆ Baumann, Rüdeger: Informationssicherheit durch kryptologische Verfahren. Vorschläge für den Unterricht. LogIn **16** 5/6 (1996), p.52-61.

⋆ Baumann, Rüdeger: Authentisierung ohne Wissenspreisgabe – Kryptografische Protokolle im Informatikunterricht. LogIn **145** (2007), p.35 ff.

Batzer, P.: Materialien zur Kryptographie (nicht veröffentlicht)

Berlin, Julia & Nicole Roth-Sonnen: Von Cäsar zum Internet. Mit Max und Lisa durch die Welt der Kryptographie. E. Friedrich Verlag, Velber, Mathematik lehren/ Heft 129, April 2005, S. 15-21.

Bertherat, Marie: Geheimbotschaften, Codes, Morsezeichen, Signale. Ensslins kleine Naturführer. Arena Verlag 2004. (Übersetzung von: 'Messages secrets'. Milan 1996/2004) ISBN 9-783401-451701.

⋆ Beutelspacher, Albrecht: Geheimsprache und Geheimzeichen. Mathe-Welt in Mathematik lehren. Best. Nr. 32933; E. Friedrich Verlag, Velber 1995

H. Biernoth: Der RSA Algorithmus. Eine Einführung in die moderne Kryptographie. Staatsex. Arbeit. Univ. Giessen 1992 (nicht veröffentlicht)

Borys, Thomas: Codierung und Kryptologie. Facetten einer anwendungsorientierten Mathematik im Bildungsprozess. Vieweg+Teubner V. 2011.

⋆ Cryptoportal für Lehrer: http://www.cryptoportal.org/

Einhaus, Erik: Zahlentheoretische Grundlagen der Public-Key Kryptographie und deren Behandlung im Unterricht. http://www.idn.uni-bremen.de/pubs/Examensarbeit_Einhaus_2.pdf (Link zuletzt geprüft am 4.2.2014)

Esslinger, Bernhard u. Koy,H: Kryptologie im Unterricht mit CrypTool. LogIn 29.Jg. (2009) H.157/158, S. 75-78.

M. Fowler & Radhi Parekh: Codes and Ciphers. Educ. Development Corp., 10302 E, 55th Place. Tulsa, OK 74146-6515 USA 1995 (48 pp.)

F. Kardel: Die Falltürfunktion als mathematische Grundlage für eine Codierung und Decodierung auf dem Kleincomputer. In: LOG IN, 4 1984, Teil 1: H. 1, S. 56-62; Teil 2: H. 2, S. 61-62; Teil 3: H. 3, S. 62-64

B. Koerber, I. Peters: Von der ITG zum Informatikunterricht - Beispiel einer spiralcurricularen Planung und Durchführung größerer Unterrichtsvorhaben. In: LOG IN, 14 1994, H. 1, S. 11-15

M. Kuhn: Der Cäsar- und der Vigenère-Code. Ein Einstieg in eine Unterrichtsreihe“Kryptographie” unter Verwendung von PASCAL. Computer und Unterricht 18/1995 p. 55-57

M. Kuhn: Moderne Kryptographie. Hintergründe und Auswirkungen aktueller Chiffrierverfahren - nicht nur für den Informatikunterricht. Computer und Unterricht 18/1995 p. 41-43

C. Niederdrenk-Felgner: Algorithmen der elementaren Zahlentheorie, CM1 (mit Begleitheft) , Institut für Fernstudien, Univ. Tübingen, 1988, Nr. 01255; (s. auch Teil 6)
Programmdiskette zu CM 1 bis CM 3 Nr. 01262 (mit ausführbaren Dateien)

Sebastian Pauli: Computeralgebra in der Lehre am Beispiel der Kryptografie. (siehe auch Teil 9!)

⋆ Hermann Puhlmann: Kryptographie verstehen. Ein schülergerechter Zugang zum RSA–Verfahren. Preprint Nr.2000. Fachbereich Mathematik der Technischen Universität Darmstadt. August 1998.

Norbert Ryska: Weltgeschichte der Kryptologie. (Über 200 Powerpoint-Seiten auf Compact Disc) Heinz Nixdorf Museums Forum 2006.

W. Schnitzspan: Schwierigkeiten mit dem Thema Militär und weitere Geheimnisse - Integration gesellschaftlicher Aspekte in den Informatikunterricht. In: Computer und Unterricht 1992, H. 8, S. 52-56

Anton Schüller, Ulrich Trottenberg, Roman Wienand, Michael Koziol & Rebekka Schneider: RSA-Primzahlen zur Verschlüsselung von Nachrichten. 19.9.2013 (Internetadresse zuletzt geprüft am 4.2.2014):

http://www.scai.fraunhofer.de/fileadmin/download/mathematik_praxis/rsa/rsa_skript_und_arbeitsblaetter.pdf

Schulz, Ralph-Hardo: Primzahlen in öffentlichen Chiffrierverfahren. Mathematik lehren 61 (1993) p. 56-64

Schulz, Ralph-Hardo & Helmut Witten: Zeitexperimente zur Faktorisierung . Ein Beitrag zur Didaktik der Kryptographie. LogIn Heft Nr. 166/167 (2010) 113-120. (S. auch Teile 6 und 9 dieser Liste!)

Schulz, Ralph-Hardo & Helmut Witten: Faktorisieren mit dem Quadratischen Sieb. Ein Beitrag zur Didaktik der Algebra und Kryptologie.FU, (FB-Preprint A/03/2011) LogIn Heft Nr.172/173 (2011/2012) 70-78. (S. auch Teile 6 und 9 dieser Liste!)

Schulz, Ralph-Hardo , Helmut Witten & Bernhard Esslinger: Rechnen mit Punkten einer Elliptischen Kurve. LogIn, Heft 181/182 (2015) 103-115 . (S. auch Teil 9 dieser Liste!)

M. Seiffert: Verschlüsselungsmethoden - Eine anwendungsorientierte Einführung mit SCHEME (Teil 2). In: LOG IN, 14 1994, H. 3, S. 33-40

K. Sennholz: Verschlüsselte Botschaften. Informatik betrifft uns. 2/1995 p. 1-23

Heike Sommer: Zahlentheorie in der Schule ? Der RSA–Algorithmus als ihre hochaktuelle Anwendung. PM 4/40 (1998) 159–162.

B. Uher: Geheimcodes und Verschlüsselungen & Die Mathematik des Zufalls. Mathe-Welt. Mathematik lehren 71/1995 p. 8(30)-23(45)

J. Wiesenbauer Public Key Kryptosysteme in Theorie und Programmierung, Schriftenreihe zur Didaktik der ÖMG, Heft 30, 1999(144-159).

Helmut Witten: Codierungstheorie. Ein Überblick. Log in 14 (1994) 5/6 p. 26-34.

⋆ Helmut Witten, Irmgard Letzner und Ralph-Hardo Schulz: RSA & Co. in der Schule. Moderne Kryptologie, alte Mathematik, raffinierte Protokolle.
Teil I: Sprache und Statistik. LogIn 18 (1998) Heft 3/4, p. 57–65.
Teil II: Von Cäsar über Vigenère zu Friedman. LogIn 18 (1998) Heft 5, p. 31–39.
Teil III: Flußchiffren, perfekte Sicherheit und Zufall per Computer. LogIn 19 (1999) Heft 2, p. 50–57.
(Siehe auch Teil 9 dieser Liste!)

⋆ Helmut Witten & Ralph-Hardo Schulz: RSA & Co. in der Schule. Moderne Kryptologie, alte Mathematik, raffinierte Protokolle. Neue Folge.
Teil 1: RSA für Einsteiger. LogIn 140 (2006) p.45–54.
Teil 2: RSA für große Zahlen. LogIn 143 (2006) p. 50-58.
Teil 3: RSA und die elementare Zahlentheorie. LogIn 152 (2008) p.60–70.
Teil 4: Gibt es genügend Primzahlen für RSA? LogIn 163/164 (2010)

p.97-103.
Teil 5: Der Miller-Rabin-Primzahltest oder Falltüren für RSA mit Primzahlen aus Monte Carlo. LogIn Heft Nr.166/167 (2010) 98-112
Teil 6: Das Faktorisierungsproblem oder: Wie sicher ist RSA? LogIn Heft Nr.172/173 (2011/2012) 59-69.
(Siehe auch Teil 9 dieser Liste!)

⋆ Helmut Witten , Ralph-Hardo Schulz & Bernhard Esslinger: RSA & Co. in der Schule. Moderne Kryptologie, alte Mathematik, raffinierte Protokolle. Neue Folge.
Teil 7: Alternativen zu RSA oder Diskreter Logarithmus statt Faktorisierung. LogIn, Heft 181/182 (2015) 85-102. (Siehe auch Teil 9 dieser Liste!)

⋆ Jochen Ziegenbalg & andere: Codierung und Kryptographie. Materialien zur gleichnamigen Vorlesung von Prof. Dr. Jochen Ziegenbalg. Siehe unter den Internet-Adressen!

⋆ Kryptographie und Sicherheit in Netzen. LogIn 16 (1996) 5/6 (u.a. mit Artikeln von P. Batzer, R. Baumann (s.o.), K.C. Becker / A. Beutelspacher, R.-H. Schulz und H. Witten)

3 Populärwissenschaftlich

J. Bamford and W. Madsen: The Puzzle Palace. Penguin Books 1995[2] (Zur Geschichte der NSA)

⋆ A. Beutelspacher: Kryptologie. Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen. Springer Spektrum, 2015[10]

⋆ A. K. Dewdney: Auf den Spuren der Enigma (Teil I)
Moderne Verschlüsselungssysteme (Teil II)
Computer Kurzweil, Spektrum der Wissenschaft 12/1988

Franke: Die geheime Nachricht. Umschau Verlag, Frankfurt 1982

Boris Gröndahl: Die Entdeckung der Pubic-Key Kryptographie. 20.1.98.
http://www.heise.de/tp/deutsch/special/krypto/1381/1.html.

Dörte Haftendorn: Mathematik sehen und verstehen: Schlüssel zur Welt.(Kap.2) Spektrum Akademischer V., 2010.

Harel, David: Das Affenpuzzle. Springer Verlag, Berlin, Heidelberg 2002 (Kap.5 und Kap.6).

⋆ Kahn, D.: The Codebrakers. Macmillan, New York 1967

⋆ Kippenhahn, R.: Verschlüsselte Botschaften – Geheimschrift, Enigma und Chipkarte. Reinbek bei Hamburg: Rowohlt, 1997, 1999[4].
ISBN: 978-3499608070

R. Kippenhahn: Streng geheim! - Wie man Botschaften verschlüsselt und Zahlencodes knackt". Rowohlt Taschenbuch Verlag, Reinbek 2002. (Jugendausgabe)

⋆ Leiberich, O.: Vom diplomatischen Code zur Falltürfunktion. Hundert Jahre Kryptographie in Deutschland. Spektrum der Wissenschaft. Juni 6/1999, p. 26–34.

R. Lindner, B. Wohak, H. Zeltwanger: Planen, Entscheiden, Herrschen - Vom Rechnen zur elektronischen Datenverarbeitung. Kap. 4. Das Militär und die Entwicklung des Computers. Reihe „ Deutsches Museum - Kulturgeschichte der Naturwissenschaften und Technik", Bd. 7715. Reinbek: Rowohlt Taschenbuch Verlag 1984.

Stephen Pincock & Mark Frary: Geheime Codes: Die berühmtesten Verschüsselungstechniken und ihre Geschichte. Ehrenwirth V. 2007. ISBN: 978-3431037340. Originaltitel:Codebreaker. The History of Secret Communication.

N. F. Pötzl: Chipkarten revolutionieren das menschliche Zusammenleben.
In: DER SPIEGEL, 48 1994, H. 47, S. 62-79

Th. von Randow: Kryptologie. Die Codeknacker. Zeit-Magazin,?, p. 66-71

⋆ Schmeh, Klaus: Die Welt der geheimen Zeichen. W3L-Verlag.Herdecke, Dortmund.2004, ISBN 3-937137-90-4

Schmeh, Klaus: Versteckte Botschaften (TELEPOLIS): Die faszinierende Geschichte der Steganografie. dpunkt Verlag 2008.ISBN 978-3936931549

Schmeh, Klaus: Codeknacker gegen Codemacher: Die faszinierende Geschichte der Verschlüsselung. Verlag W3l. 2007[2]. ISBN 978-3937137896

Bruce Schneier: Secrets and Lies. IT-Sicherheit in einer vernetzten Welt. dpunkt.verlag, Heidelberg, und Wiley-VCH Verl., Weinheim, 2001

⋆ Singh, Simon (& Klaus Fritz, Übersetzer): Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet. DTV 2001.

⋆ Singh, Simon (& Klaus Fritz, Übersetzer): Codes. Die Kunst der Verschlüsselung. DTV 2004. ('Jugendversion' der 'Geheimen Boschaften'.)

W. Stallings: Datensicherheit mit PGP. Prentice Hall, München etc. 1995. ISBN 3-930436-28-0

W. Stallings: Sicherheit in Datennetzen. Prentice Hall, München etc. 1995. ISBN 3-930436-29-9

Taschner, Rudolf: Die Zahl die aus der Kälte kam. Wenn Mathematik zum Abenteuer wird. (S.111 ff.). W.Goldmann Verlag, München, 2015& Carl Hanser Verlag, München, 2013 ISBN 978-3-442-15828-7

Wrixon, Fred B.: Codes, Chiffren und andere Geheimsprachen. Könemann V., Köln, 2000.

⋆ Ph. Zimmermann: PGP ; deutsche Übersetzung von: Abel Deuring und Christopher Creutzig: Art d'Ameublement. 3.Aufl.1997 (mit CD–Rom). ISBN 3-9802182-7-9 (e-mail: foebud@bionic.zer.de)

4 Wissenschaftliche Darstellungen (1.Teil)

M. W. Baldoni, C. Ciliberto & G.M. Piacentini Cattaneo: Elementary Number Theory, Cryptography and Codes. Springer Verlag 2009.

Bauer, Craig.P.: Secret History. The Story of Cryptology. CRC Press Chapman & Hall, 2013 (s.auch 7.)

F. L. Bauer: Kryptologie. Berlin/Heidelberg/New York: Springer-Verlag 1993. Siehe nächstes Zitat!

⋆ F. L. Bauer: Entzifferte Geheimnisse - Methoden und Maximen der Kryptologie. Berlin/Heidelberg/New York 1995 (leicht überarbeitete Fassung von "Kryptologie")

Baumann, Ulrike, Elke Franz & Andreas Pfitzmann: Kryptographische Systeme. eXamen.press. Wiesbaden: Springer Vieweg 2014.

K.-Cl. Becker & A. Beutelspacher: Hinter Schloß und Riegel? Kryptologie oder: Wie schütze ich meine Daten. mc, Mai 1994 p. 88-95

G. Berendt: Elemente der Kryptologie. In: R.-H. Schulz (Hrsg.) : Mathematische Aspekte der Angewandten Informatik, BI Verlag Mannheim 1994 p. 128-146

Beutelspacher, Albrecht, Heike B. Neumann, Thomas Schwarzpaul: Kryptografie in Theorie und Praxis. Vieweg Verlag, Wiesbaden 2005, 2010^2.

Beutelspacher, A., T. Hueske, A. Pfau: Kann man mit Bits bezahlen? Informatik-Spektrum 16 (1993) 99-106.

Beutelspacher, A., J. Schwenk, K.-D. Wolfenstetter: Moderne Verfahren der Kryptographie; Vieweg 1995 , Springer Spektrum 2015^8

Beutelspacher, A.: Kryptographie - Eine Einführung in die Wissenschaft von der Geheimhaltung der Daten. In MU Beutelspacher, Schulz (Hrsg) - Der Mathematikunterricht, 33 (1987), H. 3, S. 4-14

A. Beutelspacher: Hilfreiche Dämonen - oder: Wie schützt man Daten vor Veränderung?. In: MU - Der Mathematikunterricht, 33 (1987), H. 3, S. 16-21

Biggs, Norman L.: Codes. An Introduction to Information Communication and Cryptography. Springer Verlag London 2008. ISBN 978-1-84800-272-2

Ian F. Blake, G. Seroussi, N. Smart: Elliptic Curves in Cryptography. Cambridge University Press, 1999

Brands, Gilbert: Verschlüsselungsalgorithmen. Angewandte Zahlentheorie rund um Sicherheitsprotokolle. Vieweg V., Braunschweig/Wiesbaden, 2002;(s. auch Teil 6!).

⋆ Buchmann, Johannes: Einführung in die Kryptographie. Berlin: Springer V. 1999, 2008^{4}

Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, Frederik Vercauteren (Editors): Handbook of Elliptic and Hyperelliptic Curve Cryptography, Discrete Mathematics and Its Applications, Chapman Hall/CRC, 2012^{2}

Wilfried Dankmeier: Grundkurs Codierung: Verschlüsselung, Kompression, Fehlerbeseitigung. Mit Online-Service zum Buch. Vieweg+Teubner V., 2006^{3}. ISBN: 978-3528253998.

D. W. Davies: The Lorenz Cipher Machine SZ 42. Cryptologia, Jan. 95, XIX 1 p. 39-61

H.Delfs u. H.Knebl: Introduction to Cryptography. Principles and Applications. Springer Berlin/Heidelberg 2002, 2015^{3}.

Ertel, W.: Angewandte Kryptographie. fv.Fachverlag Leipzig. Leipzig 2001.

⋆ Esslinger, B. u. a. : Das CrypTool-Skript -Kryptographie, Mathematik und mehr. 2010^{10}. (S.auch Nr.9).
http://www.cryptool.com/download/CrypToolScript-de.pdf

⋆ Esslinger, B. u.a.: Das CrypTool-Buch: Kryptographie lernen und anwenden mit CrypTool und SageMath. 2016^{12}

Freiermuth, Karin, Juraj Hromkovic, Lucia Keller u.Björn Steffen: Einführung in die Kryptologie. Lehrbuch für Unterricht und Selbststudium. Vieweg + Teubner 2010. ISBN: 978-3-8348-1005-2

F. J. Furrer: Fehlerkorrigierende Block–Codierung für die Datenübertragung. Birkhäuser Verlag, Basel etc. 1981, Kap. 8

Helen Fouche Gaines: Cryptanalysis. Dover Pubn Inc 2000. ISBN: 978-0486200972.

Galbraith, Steven D.: Public Key Cryptography. Cambridge Univ.Press 2012

Goldreich, Oded: Foundations of Cryptography. Basic Tools. Cambridge University Press 2001/2006.

Goldreich, Oded: Foundations of Cryptography: A Primer (Foundations and Trends in Theoretical Computer Science). Now Publishers Inc. 2005

⋆ E. G. Giessmann: Sichere Verschlüsselungen - geht das überhaupt.
Teil I Alpha 6/1995 p. 10-11
Teil II Alpha 7/1995 p. 8-10

A. Guthmann: Vigenère-Verschlüsselung: Theorie und Praxis. Math. Semesterberichte **47** (2000) p. 39-49

Darrel Hankerson, Scott Vanstone, Alfred J. Menezes: Guide to Elliptic Curve Cryptography. Springer Professional Computing, 2004

E. Henze & H. H. Homuth: Einführung in die Codierungstheorie. Vieweg, Braunschweig 1974, **Kap. 3**

Th. Hermann, W. Poguntke: Fehlerkorrigierende Codes in der Kryptologie. Math. Semesterb. 42 (1995): 139-151

J. Hoffstein, J. Pipher & J. Silverman: An Introduction to Mathematical Cryptography (Undergraduate Texts in Mathematics). Springer V. 2014^2 ISBN 978-1-4939-1710-5

H. Horak: Der bunte Zoo der Kryptologie. Teil I: Mathe-plus (Feb. 1987) 3/3, p. 2-5; Teil II (oder Großwildjagd auf Primzahlriesen): Mathe-plus (April 1987) 3/4, p. 2-6; Teil 3 (oder Die Exoten der Gattung Public Key): Mathe-plus (Juli/August 1987) 3/5,6 p. 2-7.

P. Horster: Kryptologie, BI-Wissenschaftsverlag, Zürich 1985.

M. Hortmann: Datensicherheit durch Kryptographie. Mitt. Math. Ges. Hamburg 19 (2000), 21-33.

Karpfinger, Christian & Hubert Kiechle: Kryptologie: Algebraische Methoden und Algorithmen. Vieweg+Teubner 2010.

Katz, Jonathan & Yehuda Lindell: Introduction to Modern Cryptography: Principles and Protocols. Chapman & Hall/Crc Cryptography and Network Security Series. 2007.

Klein, Andreas: Visuelle Kryptographie. Springer V. 2007.

Knudsen, Lars R. & Matthew J.B.Robshaw: The Block Cipher Companion. Springer V. Berlin Heidelberg 2011.

Kraft, James S.& Lawrence C. Washington: An Introduction to Number Theory with Cryptography. Chapman and Hall/CRC 2013; (s. auch Tei 6).

Kranakis, E.: Primality and Cryptography. John Wiley & Teubner Verlag, Stuttgart 1986; (s. auch Teil 6).

Martin, Keith M.: Everyday Cryptography. Fundamental Principles and Applications. Oxford University Press 2012.

Massierer, Maike: ECC Notebook. An Interactive Introduction to Elliptic Curve Cryptography.
http://sage.mathematik.uni-siegen.de:8000/home/pub/45/
bis
http://sage.mathematik.uni-siegen.de:8000/home/pub/51
(Link zuletzt geprüft am 3.9.2013)

McAndrew, Alasdair: Introduction to Cryptography with Open-Source Software. CRC Press, 2011.

A. R. Miller: The cryptographic mathematics of Enigma. Cryptologia Jan. 1995 XIX/1, p. 66-80.

Miller, Michael: Symmetrische Verschlüsselungsverfahren. Design, Entwicklung und Krytoanalyse klassischer und moderner Chiffren. Teubner Verlag Stuttgart/Leipzig/Wiesbaden, 2003.

R.A.Mollin: Codes. The Guide to Secrecy from Ancient to Modern Times. Discrete Mathematics and its applications. Chapman & Hall. Boca Raton, FL. 2005

V.Nachev, J.Patarin, E.Volte: Feistel Ciphers, Springer V. 2017, ISBN 978-3-319-49528-6

W. Oberschelp: Algorithmen und Computer im Unterricht. Kurseinheit 1-7, Fernuniv. GSH Hagen, FB Math. u. Inform. 1986, Kurseinheit 3

Rubinstein-Salzedo, Simon. Cryptography. Springer Undergraduate Mathematics Series. Springer International Publishing. 2018

A. Salomaa: Public Key Cryptography. Springer. Verlag, 1990

Klaus Schmeh: Kryptografie: Verfahren, Protokolle, Infrastrukturen. dpunkt Verlag, 2009[4]. ISBN 978-3898646024

Jürgen Schmidt: Kryptographie in der IT – Empfehlungen zu Verschl üsselung und Verfahren, Dieser Artikel erschien ursprünglich in c't 01/2016, Seite 174. Veröffentlicht am 17.06.2016 in

http://www.heise.de/security/artikel/Kryptographie-in-der-IT-Empfeh lungen-zu-Verschluesselung-und-Verfahren-3221002.html

B. Schneier: Angewandte Kryptographie: Protokolle, Algorithmen und Sourcecode in C. Addison–Wesley, Bonn etc. 1996. ISBN 0-471-11709-9

⋆ R.-H. Schulz: Codierungstheorie - eine Einführung. Braunschweig/Wiesbaden: Vieweg 1991, 2003^2. (**Kap.IV**)

Schwenk, Jörg: Sicherheit und Kryptographie im Internet. Von sicherer E-Mail bis zu IP-Verschlüsselung. Vieweg V., Braunschweig/Wiesbaden, 2002, 2005^2.

Selke, Gisbert W. : Kryptographie. Verfahren, Ziele, Einsatzmöglichkeiten. O'Reilly, 2000 (vergriffen).

A. Sgarro & M. Würmeli: Geheimschriften. Weltbild Verlag (vergriffen).

Stanoyevitch, Alexander: Introduction to Cryptography with Mathematical Foundations and Computer Implementations. CRC Press 2010.

Swoboda, Joachim, Spitz, Stephan & Pramateftakis, Michael: Kryptographie und IT-Sicherheit. Grundlagen und Anwendungen. Vieweg+ Teubner 2008. ISBN: 978-3-8348-0248-4

T. K. Thong & R. Schulz: Implementation of the RSA Public Key Cryptosystem. Math. Medley 19/2 1991 (Singapore) 53-64.

van Tilborg, Henk C.A. (Editor in Chief): Encyclopedia of Cryptography and Security. Springer Sience +Business Media, Inc., 2005. (12+684 Seiten)

Voß, H.: Praktische Kryptologie mit Java. Book on Demand.

Wätjen, Dietmar: Kryptographie. Spektrum Akad.V., Heidelberg, 2004.

Washington, L.: Elliptic Curves – Number Theory and Cryptography. Chapman and Hall/CRC, 2003

Weis, R. : Chiffrieren am laufenden Band. PC Magazin Kryptographie.

Weis, R. : Zahlen Sie bar oder digital? Protokolle für sicheres Geld. PC Magazin spezial 5.98. (Kryptographie und Netzsicherheit) 1998, p.94-97.

Werner, Annette: Elliptische Kurven in der Kryptographie. Springer Verlag, Berlin/ Heidelberg, 2002.

J. Wiesenbauer: Using DERIVE to Explore the Mathematics Behind the RSA Cryptosystem", Proceedings of the 4th Int. DERIVE & TI-89/92 Conference "Computer Algebra in Mathematics Education"(Liverpool 2000), ed. T. Etchells, C. Leinbach, D. Pountney, bk-teachware (auf CD-ROM), ISBN 3-901769-34-X

Willems, W. : Codierungstheorie und Kryptographie. Birkhäuser V. Basel, 2008.

Wobst, R. : Abenteuer Kryptologie.Addison-Wesley,München etc.,1998[2].

Young, Anne L. : Mathematical Cyphers. From Caesar to RSA. AMS, 2006. ISBN 978-0-8218-3730.

5 Quantenkryptographie

Aaronson, Scott: Die Grenzen der Quantencomputer. Spektrum der wissenschaft. Juli 2008, p. 90-97.

M. W. Baldoni, C. Ciliberto & G.M. Piacentini Cattaneo: Elementary Number Theory, Cryptography and Codes. Springer Verlag 2009 (letztes Kapitel).

Bennett, C.H. , Brassard, G. & Ekert,A: Quanten-Kryptograhie. Spektrum der Wissenschaft, Dezember 1992, p.96-104.

Bruß, Dagmar: Quanteninformation. Fischer Taschenbuch Verlag, Frankfurt am Main, 2003.

6 Zur Zahlentheorie (Faktorisierung/Primzahltests/Primzahlen)

(zum Teil auch populärwissenschaftlich)

M. W. Baldoni, C. Ciliberto & G.M. Piacentini Cattaneo: Elementary Number Theory, Cryptography and Codes. Springer Verlag 2009.

Brands, Gilbert: Verschlüsselungsalgorithmen. Angewandte Zahlentheorie rund um Sicherheitsprotokolle. Vieweg V., Braunschweig/Wiesbaden, 2002.

J. Buchmann: Faktorisierung großer Zahlen. Spektrum d. Wissenschaft, Sept. 1996 p. 80-88.

Crandall, Richard & Carl Pomerance:Prime Numbers A Computational Perspective. Springer Verlag 2005.

A.K. Dewdney: Primzahlwäsche. In: Computer Kurzweil 2. Spektrum Akadem. Verlag, Heidelberg 1992 p. 175-178

Esslinger, B. u. a. : Das CrypTool-Skript -Kryptographie, Mathematik und mehr. 2010[10]. **Kap.3 und 4** (S.auch diese Liste Nr.4)
http://www.cryptool.com/download/CrypToolScript-de.pdf

Fine, Benjamin u. Gerhard Rosenberger: Number Theory - An Introduction via the Distribution of Primes. Birkhäuser V., Boston 2007

F. Fricker: Neue Rekord-Faktorisierung. Spektrum d. Wissenschaft, Nov. 1990, p. 38-42

J. Kilian: Uses of Randomness in Algorithms and Protocols. MIT Press. Cambridge (Mass.) 1990.

Kraft, James S.& Lawrence C. Washington: An Introduction to Number Theory with Cryptography. Chapman and Hall/CRC 2013; (s. auch Teil 4).

Kranakis, E.: Primality and Cryptography. John Wiley & Teubner Verlag, Stuttgart 1986; (s. auch Teil 6).

Mazur, Barry, & William Stein: Prime Numbers and the Riemann Hypothesis . Cambridge University Press; 2016. ISBN-13: 978-1107499430

Möller, Herbert: Elementare Zahlentheorie und Problemlösen
http://wwwmath.uni-muenster.de/u/mollerh/data/ZtPP.pdf
(Link zuletzt geprüft am 8.3.2010).

⋆ C. Niederdrenk-Felgner: Algorithmen der elementaren Zahlentheorie, CM1 (mit Begleitheft), Institut für Fernstudien, Univ. Tübingen, 1988

W. Oberschelp: Algorithmen und Computer im Unterricht. Kurseinheit 1-7, Fernuniv. GSH Hagen, FB Math. u. Inform. 1986, Kurseinheit 3.

Ramberger, Martin: Lernprogramm: Zahlentheorie zur asymmetrischen Verschlüsselung
http://www.uni-koblenz.de/ rambo/

Lasse Rempe & Rebecca Waldecker: Primzahltests für Einsteiger: Zahlentheorie - Algorithmik - Kryptographie. Vi Barry Mazur (Author), William Stein (Author) eweg+Teubner, 2009.
ISBN: 978-3834806796.

⋆ Ribenboim, Paulo: Die Welt der Primzahlen- Geheimnisse und Rekorde. Springer Verlag, Berlin, Heidelberg, New York 2006.

Ribenboim, Paulo: The Book of Prime Number Records. Springer Verlag, New York 1988, 1996

Ribenboim, Paulo: My Numbers, My Friends Popular Lectures on Number Theory. Springer Verlag 2000.

Riesel, H.: Prime Numbers and computer Methods for Factorization.(Progress in Mathematics). Birkhäuser Boston, 1994

⋆ du Sautoy, M.: Die Musik der Primzahlen. C.H.Beck Verl. München 2004 (populärwissenschaftlich, auch historisch).

Schulz, Ralph-Hardo & Helmut Witten: Zeitexperimente zur Faktorisierung. Ein Beitrag zur Didaktik der Kryptographie. LogIn Heft 166/167 (2010)

113-120. (S. auch Teil 2 und Teil 9 dieser Liste!)

Schulz, Ralph-Hardo & Helmut Witten: Faktorisieren mit dem Quadratischen Sieb Ein Beitrag zur Didaktik der Algebra und Kryptologie. (FB-Preprint A/03/2011) LogIn Heft Nr.172/173 (2011/2012) 70-78. (S. auch Teil 2 und Teil 9 dieser Liste!)

Stein, William: Elementary Number Theory-Primes, Congruences, and Secrets.Springer V., New York 2009.
http://modular.math.washington.edu/ent/ent.pdf

Streuding, Jörn, & Annegret Weng: Primzahltests – von Eratosthenes bis heute. Math. Semesterberichte 51, 231-252 (2004). Digital Object Indetifier (DOI): 10.1007/s00591-004-0081-6.

7 Historisch

Bauer, Craig.P.: Secret History. The Story of Cryptology. CRC Press Chapman & Hall, 2013 (siehe auch 4.).

Beckmann, Bengt: Arne Beurling und Hitlers Geheimschreiber. Schwedische Entzifferungserfolge im 2. Weltkrieg. Springer-Verlag, 2005.

Churchhouse, Robert: codes and ciphers. Julius Caesar, the Enigma, and the internet. Cambridge Univ. Press, 2002.

O. I. Franksen: Mr. Babbage's Secret. The Tale of a Cipher- and APL. Prentice Hall, Englwood Cl. 1985

R. Hochhuth: Alan Turing. Rowohlt 1987

⋆ A. Hodges: Alan Turing: Enigma. Springer Verlag 1994

⋆ D. Kahn: The Codebrakers. Macmillan, New York 1967 (siehe 3.)

⋆ R. Kippenhahn: Verschlüsselte Botschaften – Geheimschrift, Enigma und Chipkarte.(Siehe 3. !)

⋆ O. Leiberich: siehe 3.)

Levy, Steven: Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age . Penguin books. 2001.

⋆ R. Lewin: Entschied Ultra den Krieg? Verlag Wehr und Wisen, Bonn 1981

R. Lindner, B. Wohak, H. Zeltwanger: Planen, Entscheiden, Herrschen – Vom Rechnen zur elektronischen Datenverarbeitung. Kap. 4. Das Militär und die Entwicklung des Computers. Reihe, Deutsches Museum – Kulturgeschichte der Naturwissenschaften

Mollin, Richard A.: ...und Technik", Bd. 7715. Reinbek: Rowohlt Taschenbuch Verlag 1984 (siehe auch 4.)

Stephen Pincock & Mark Frary: Geheime Codes: Die berühmtesten Verschlüsselungstechniken und ihre Geschichte. Ehrenwirth V. 2007. ISBN: 978-3431037340. Originaltitel:Codebreaker. The History of Secret Communication. (siehe 3.)

Norbert Ryska: Weltgeschichte der Kryptologie. CD. HNF 2006 (siehe 2.!)

⋆ Schmeh, K.: Die Welt der geheimen Zeichen. Die faszinierende Geschichte der Verschlüsselung.W3L-Verlag, Herdecke/Dortmund 2004 (siehe 3.)

⋆ Singh, Simon (& Klaus Fritz, Übersetzer): Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet.(Siehe 3.)

A. Sgarro, M. Würmeli: Geheimschriften. Weltbild Verlag (vergriffen)

8 Einige weitere wissenschaftliche Abhandlungen

Becket, Brian: Introductin to Cryptology. Blackwell Scientific Publ. Oxford etc., 1988.

H. Beker & F. Piper: Ciphersystems. The Protection of Communications. Northwood Books, London 1982

H. Beker & F. Piper: Edts. Cryptography and Coding. Clarendon Press. Oxford 1989

Beth, Heß, Wirl: Kryptographie, Teubner Verlag, Stuttgart 1983

Biham, Eli & Orr Dunkelman: Techniques for Cryptanalysis of Block Ciphers. Springer Verlag 2012, 2013

Boyd,Colin & Anish Mathuria: Protocols for Authentication and Key Establishment. Information Security and Cryptography. Springer V., 2003.

J.Daemen & V.Rijmen: The Design of Rijndael. AES–The Advanced Encryption Standard. Springer V., 2002

D. F. R. Denning: Cryptography and Data Security. Addison-Wesley, Reading etc. 1983[2]

W. Diffie & M. E. Hellman: Privacy and Authentication: An introduction to cryptography. Proc. of the IEEE, 67/3 März 1979, p. 397-426

W. Diffie & M. E. Hellman: New directions in Cryptographie. IEEE Trans. Inform. Th. IT -22, p. 644-654

W. Fumy & P. Rieß: Kryptographie. Oldenburg Verlag, München 1988, 1994[2].

D. Gollmann: Algorithmenentwurf in der Kryptographie. BI Mannheim 1994.

Gómez Pardo, José Luis: Introduction to Cryptography with Maple. Springer-Verlag 2013.

Hankerson, Hoffman, Leonard, Lindner, Phelps, Rodger, and Wall: Coding Theory and Cryptography. The Essentials. Chapman & Hall, 2001^2

Huber, Michael: Combinatorial Designs for Authentication and Secrecy Codes. Foundations and Trends in Communications and Information Theory, Now Publishers 2010. ISBN 978-1601983589.

J. Kilian: Uses of Randomness in Algorithms and Protocols. MIT Press. Cambridge (Mass.) 1990.

N. Koblitz: A course in Number Theory and Cryptography. Springer Verlag, New York, Berlin etc. 1987

N. Koblitz: Algebraic Aspects of Cryptography. Springer V., 1998, 2004^3.

A. G. Konheim: Cryptography. A Primer. John Wiley & Sons, New York etc. 1981

Koukouvinos, Christos / Simos, Dimitrios E. / Georgiou, Stelios: Combinatorial Designs. With Applications to Coding Theory and Cryptography. De Gruyter 9/2014.

Myasnikov, A., V.Shpilrain & A.Ushakov: Group-based Cryptography. Birkhäuser V. 2008. ISBN 978-3-7643-8826-3.

C. H. Meyer & St. M. Matyas: Cryptography: A New Dimension in Computer Data Security. John Wiley, New York etc. 1982

Christof Paar & Jan Pelzl: Understanding Cryptography. A Textbook for Students and Practitioners. Springer V. 2010. ISBN 978-3-642-04100-6.
"Uniquely designed for students of engineeering and applied computer science, and engineering practitioners".

R. L. Rivest, A. Shamir & L. Adleman: A method for obtaining digital signatures and public key cryptosystems, Comm. A CM **21** (1978) p. 120-126

N. Ryska & S. Herda: Kryptographische Verfahren in der Datenverarbeitung. Springer Verlag Berlin etc. 1980

B. Schneider: Applied Cryptography. Protocols, Algorithms and Source Code in C. John Wiely & Sons, New York etc. 1996^2

C. E. Shannon: Communication Theory of Secrecy Systems. Bull. Sys. Tech. J. 28 (1949) p. 656-715

Shaska, T., W.C. Huffman, D. Joyner & V. Ustimenko (edit.): Advances in Coding Theory and Cryptography. World Scientific – Imperial College Press. 2007.

G. J. Simmons (Hrsg.): Contemporary cryptology. IEEE-Press, New York 1992

Stinson, Douglas R. Cryptography. Theory and Practice. Chapman & Hall, 2006[3]

H.van Tilborg: Fundamentals of Cryptology. Kluwer, 2000

R. Tum: Privacy transformations for databank systems, in Proc. Nat. Comp. Conf. and Exp. (NCC) 42, AFIPS Press, Montwale NJ 1973

D. Welsh: Codes and Cryptography. Clarendon Press. Oxford 1988

Yan, Song Y.: Cryptanalytic Attacks on RSA. Springer V., 2008, ISBN: 978-0-387-48741-0.

Yaschenko, V.V. (Ed.): Cryptography: An Introduction, AMS, Student Mathematical Library, Vol.18, 2002.

9 Einige Internetadressen

Baier, Harald: Vorlesung Datensicherheit (Kap.3), Hochschule Darmstadt
https://www.fbi.h-da.de/fileadmin/personal/h.baier/Lectures-summer-10/SS-10-Datensicherheit/vorlesung_datensicherheit_ss10_kap3krypto2.pdf

Bernstein, Daniel J.: Curve25519: new Diffie-Hellman speed records. 2006.
http://cr.yp.to/ecdh.html#curve25519-paper.html
http://cr.yp.to/ecdh/curve25519-20060209.pdf

Bernstein, Daniel J. & Tanja Lange: ECCHacks – A gentle introduction to elliptic-curve cryptography, Dez. 2014 :
http://ecchacks.cr.yp.to/ (Gliederung und Python-Skripte)
https://www.youtube.com/watch?v=l6jTFxQaUJA (Video vom Vortrag)
(Links zuletzt geprüft am 17.4.2015)

Brandes, Torsten: Moderne Verfahren in der Kryptographie unter Anwendungsaspekten.
http://www.torsten-brandes.de/TorstensWeltV4/content/uni_content/kryptoWeb/krypto.html

BSI: http://www.bsi.bund.de/esig/basics/techbas/krypto/

BSCW (Shared Workspace Server): Materialien zur Kryptographie.
http://bscw.schule.de/pub/nj_bscw.cgi/159132/
(Link zuletzt geprüft am 18.12.2012)

Carl, Lothar F.: Kryptologie in der Schule. Themenangebot in learn:line NRW.
http://www.learn-line.nrw.de/angebote/kryptologie/

⋆ Cryptool: http://www.cryptool.de

⋆ Cryptoportal für Lehrer: http://www.cryptoportal.org/

Einhaus, Erik: Zahlentheoretische Grundlagen der Public-Key Kryptographie und deren Behandlung im Unterricht.
http://www.idn.uni-bremen.de/pubs/Examensarbeit_Einhaus_2.pdf
(Link zuletzt geprüft am 4.2.2014)

⋆ Esslinger, B. u. a. : Das CrypTool-Skript -Kryptographie, Mathematik und mehr. 2010[10]. (S.auch Nr.4)
http://www.cryptool.com/download/CrypToolScript-de.pdf

Fried, Joshua/ Pierrick Gaudry/ Nadia Heninger/Emmanuel Thomé: A kilobit hidden SNFS discrete logarithm computation.
http://caramba.inria.fr/hsnfs1024.html
Cryptanalysis of 1024-bit trapdoored primes:
http://eprint.iacr.org/2016/961
DSA und Diffie Hellman: Primzahlen können Hintertür enthalten
http://www.golem.de/news/dsa-diffie-hellman-primzahlen-koennen-hintertuer-enthalten-1610-123778.html
(Links zuletzt geprüft am 19.10.2016)

Gräbe, Hans-Gert: Primzahltestverfahren. Vortrag am St.-Augustin-Gymnasium Grimma, 1.3.2007
http://www.hg-graebe.de/MV/Grimma-07.pdf

Halderman, J.Alex and Nadia Heninger: Logjam: Diffie-Hellman, discrete logs, the NSA, and you. 2015.
https://media.ccc.de/v/32c3-7288-logjam_diffie-hellman_discrete_logs_the_nsa_and_you
(Link zuletzt geprüft am 18.10.2016)

Henne, H.W.: Forum für InformationssiA kilobit hidden SNFS discrete logarithm computationcherheit
http://www.gocs.de
(Link zuletzt geprüft am 3.6.2011)

Kluge, Albert: Java-Applet Mathematik : Miller-Rabin-Test
http://www.jjam.de/Java/Applets/Primzahlen/Miller_Rabin.html
(Link zuletzt geprüft am 13.5.2008)

Kuehn, M.: http://mksoftware.mk.funpic.de/krypto.php

Lenstra, Arjen K. & Eric R. Verheul: Selecting Cryptographic Key Sizes 1999
http://infoscience.epfl.ch/record/164526/files/NPDF-22.pdf
(Link zuletzt geprüft am 17.4.2015)

Lipmaa, Helger: Übersicht über Publikationen zur Kryptographie über Zopfgruppen.

http://www.adastral.ucl.ac.uk/ helger/crypto/link/public/braid/
(Link zuletzt geprüft am 13.5.2008)

Möller, Ulf: http://www.thur.de/ulf/krypto/index.html

Minh Van Nguyen: Number Theory and the RSA Public Key Cryptosystem. (Tutorial using SAGE)
http://bitbucket.org/mvngu/numtheory-crypto/downloads/numtheory-crypto.pdf
(Link zuletzt geprüft am 29.9.2010)

Pauli, Sebastian: Computeralgebra in der Lehre am Beispiel Kryptografie.
http://www.math.tu-berlin.de/∼pauli/tdm.pdf

RSA: http://www.rsasecurity.com/rsalabs/faq/index.html

Schneppe, U.: Digitales Bargeld
http://ulrich.schneppe.bei.t-online.de/s1916/tei63.htm

Sage: http://www.sagemath.org/

Anton Schüller, Ulrich Trottenberg, Roman Wienand, Michael Koziol & Rebekka Schneider: RSA-Primzahlen zur Verschlüsselung von Nachrichten. 19.9.2013
http://www.scai.fraunhofer.de/fileadmin/download/mathematik_praxis/rsa/rsa_skript_und_arbeitsblaetter.pdf
(Link zuletzt geprüft am 4.2.2014):

Schulz, R.-H., & H.Witten: Zeitexperimente zur Faktorisierung.
http://bscw.schule.de/pub/nj_bscw.cgi/159132/
(Link zuletzt geprüft am 15.3.2016)

Schulz, R.-H., & H.Witten: Faktorisieren mit dem Quadratischen Sieb.
http://bscw.schule.de/pub/nj_bscw.cgi/159132/
(Link zuletzt geprüft am 15.3.2016)

Schulz, R.-H., H. Witten & Bernhard Esslinger: Rechnen mit Punkten einer Elliptischen Kurve.
http://bscw.schule.de/pub/bscw.cgi/159132/
(Link zuletzt geprüft am 15.3.2016)

Spannagel, Christian: (verschiedene You-Tube Videos über Verschlüsselungen: Caesar, Vigenère, RSA)
https://www.youtube.com/playlist?list=PL6_AeYXBHF0OWS1GxV6lfivdReSyKhv3l
(Link zuletzt geprüft am 2.8.2017):

Wikipedia: RSA-Kryptosystem
http:/de.wikipedia.org/wiki/RSA-Kryptosystem

Wikipedia: Enigma (Maschine)
http:/en.wikipedia.org/wiki/Enigma_machine

Witten, Helmut, I.Letzner (nur Folgen 1-3) & B.Esslinger (nur Neue Folge 7) & R.-H.Schulz: RSA& Co. in der Schule. Folgen 1-3, Neue Folgen 1-7.
http://bscw.schule.de/pub/nj_bscw.cgi/159132/
(Link zuletzt geprüft am 15.3.2016)

Ziegenbalg, J.: Materialien und interaktive Simulationen zur Codierung und Kryptographie
http://www.ph-karlsruhe.de/wp/ziegenbalg/materialien-homepage-jzbg/cc-interaktiv/
(Link zuletzt kontrolliert am 29.9.2010)

Spiegel.online: 'Quantenkryptographie' (Meldung vom 8.10.2008)
http://www.spiegel.de/netzwelt/tech/0,1518,582951,00.html
(Link zuletzt geprüft am 8.3.2010)

Alle Internetquellen, auf die hier verwiesen wurden, sind zwar sorgfältig geprüft worden, es kann jedoch keine Gewähr für die Vollständigkeit und Richtigkeit von Informationen übernommen werden, die über die weiterführenden Links erreicht werden.

In: Schriften zur Didaktik der Mathematik und Informatik an der UniversitÃ¤t Salzburg. (Fuchs K. J. (Hrsg.)). Band 3. Shaker Verlag: Aachen.Â Codierung und Kryptologie. Facetten einer anwendungsorientierten Mathematik im Bildungsprozess. Vieweg + Teubner: Wiesbaden. [WLS99] Witten, Helmut, Irmgard Letzner, and Ralph Hardo Schulz: RSA & Co. in der Schule: Moderne Kryptologie, alte Mathematik, ranierte Protokolle. Teil 3: Flusschiren, perfekte Sicherheit und Zufall per Computer. LOG IN, 1999(2):50â€“57, 1999. http://bscw.schule.de/pub/nj_bscw.cgi/d637156/RSA_u_Co_T3.pdf . Download Citation | On Jan 1, 2010, Ralph-Hardo Schulz and others published Zeit-Experimente zur Faktorisierung - Ein Beitrag zur Didaktik der Kryptologie. | Find, read and cite all the research you need on ResearchGate.Â Dem von Kerckhoffs formulierten [Show full abstract] â€šGrundgesetz der Kryptologieâ€™: Â«Il faut quâ€™il puisse sans inconvÃ©nient tomber entre les mains de lâ€™ennemiÂ» gab Shannon die Fassung â€œThe enemy knows the system being usedâ€. Read more. Conference Paper.