Contents

Chapter 1

Zero

1.1 One

blah

1.2 Two

blah

1.2.1 One

blah

Two

blah

Bibliography

[1] C. Adams. The cast-128 encryption algorithm, may 1997.

[2] Ross Anderson, Eli Biham, and Lars Knudsen. *Serpent: A Proposal for the Advanced EncryptionStandard*. NIST, England, Isarael, Norway, 1999.

[3] Werner Arnhold. Lieben Sie PYTHON? *LOG IN*, 21(2):18–24, 2001.

[4] Peter Bartke and Christian Maurer. Thesen zum Informatikunterricht in der Oberstufe. `http://www.inf.fu-berlin.de/inst/ag-lfwb/didaktik/diverses/thesen.html`, 2000.

[5] Peter Batzer. Die Enigma. *LOG IN Informatische Bildung und Computer in derSchule*, (5/6):44–51, 1996.

[6] Friedrich L. Bauer. *Entzifferte Geheimnisse - Methoden und Maximender Kryptologie*. Springer Verlag, Berlin Heidelberg New York, zweite edition, 1997.

[7] Friedrich L. Bauer and Gerhard Goos. *Informatik, eine einführende Übersicht*. Springer Verlag, Berlin Heidelberg New York, dritte edition, 1982.

[8] Rdeger Baumann. Informationssicherheit durch kryptologischeVerfahren. *LOG IN, Informatische Bildung und Computer in derSchule*, (5/6):52–61, 1996.

[9] Rdeger Baumann. Java – Stimulans fr den Informatikunterricht. *LOG IN*, 17:20–31, 1997.

[10] Klaus-Cl. Becker and Albrecht Beutelspacher. Datenverschlüsselung - Anwendung der Kryptologie. *LOG IN, Informatische Bildung und Computer in derSchule*, (5/6):16–21, 1996.

[11] Gerhard Berendt. *Mathematische Aspekte der angewandten Informatik*, chapter Elemente der Kryptologie, pages 128–146. Bibliographisches Instiut & F.A.Brockhaus AG,Mannheim, 1994.

[12] Albrecht Beutelspacher and Jg Schwenk andKlaus Dieter Wolfenstetter. *Moderne Verfahren der Kryptographie*. Friedrich Vieweg & Sohn Verlagsgesellschaft, Braunschweig Wiesbaden, dritte edition, 1999.

[13] BI-Verlag. *Meyers Hand-Lexikon des allgemeinen Wissens*. Verlag des Bibliographischen Instituts, Leipzig, dritte edition, 1883.

[14] Bibliographisches Institut. *Meyers Enzyklopisches Lexikon*. Bibliographisches Institut, Mannheim, neunte edition, 1973.

[15] Jerome Seymour Bruner. *The process of education*. Harvard University Press, CAmbridge, 1st edition, 1960.

[16] Johannes Buchmann. *Einfhrung in die Kryptographie*. Springer Verlag, Berlin, Heidelberg New York, erste edition, 1999.

[17] Bundesministerium für Wirtschaft und Technologie. Eckpunkte der deutschen Kryptopolitik. 2 June.

[18] Carolynn Burwick and other. Mars - a cansidate cipher for aes, 22 September.

[19] Herbert Voß Carole Siegfried. Mathematik im Inline-modus. 3/04:25–32, November 2004.

[20] J. Daeman, R. Govaerts, and J. Vandewalle. Weak keays for idea. *Advances in Cryptology*, Crypto '93 Proceedings:224–230, 1994.

[21] Joan Daemen and Vincent Rijmen. The rijndael block cypher, 1999.

[22] Harvey M. Deitel and Paul J. Deitel. *Java - How to program*. Prentice-Hall, Inc, Upper Saddle River, New Jersey 07458, dritte edition, 1999.

[23] Hans Dobbertin, Antoon Bosselaers, and Bart Preneel. Ripemd-160: A strngthened version of ripemd. *LNCS - Fast Software Encryption*, 1039:71–82, 1996.

[24] Walter Doberanz. *Java*. Carl & Hanser Verlag, Mnchen, erste edition, 1996.

[25] W. Duffie and M.E. Hellmann. Privacy and authentication: An introduction tocryptpgraphy. *Proc. IEEE*, 67(3)Mar:397–427, 1979.

[26] Bruce Eckel. *Java*. Prentice-Hall, Inc, Upper Saddle River, New Jersey 07458, zweite edition, 1999.

[27] Horst Feistel. Cryptography and computer privacy. *Scientific American*, 228:15–23, 1973.

[28] D.M. Geary and A.L. McClellan. *Graphic Java - das awt beherrschen*. Heinz Heise Verlag, Hannover, erste edition, 1997.

[29] Michael Gohdes. LaTeX und Chemie - ein schönes Paar? *dtk*, 2/2001(2):7–19, jul 2001.

[30] Michael Goossens, Frank Mittelbach, and AlexanderSamarin. *The LaTeX Companion*. Addison Wesley, 1994.

[31] Th. Hampel, J. Magenheim, and C. Schulte. *Informatik und Schule. Fachspezifische und fachbergreifende didaktische Konzepte*, chapter Dekonstruktion von Informatiksystemen als Unterrichtsmethode. Zugang zu objektorientierten Sichtweisen, pages 149–164. Berlin, Heidelberg, New York, 1999.

[32] Hans-Wilhelm Heibey, Andreas Pfitzmann, and UlrichSAndl. Kryptographie, Herausforderung für Staat undGesellschaft. *LOG IN, Informatische Bildung und Computer in derSchule*, (5/6):37–43, 1996.

[33] Herbert Voß. *Praktische Kryptologie mit Java*. BoD, jan 2001.

[34] month = may year = 2001 howpublished = `http://www.perce.de/lyx/with/a/very/long/winded/url/for/demonstartion/equations.pdf` Herbert Vo, title = and Mathmode.

[35] W.H. Kilpatrick. The project method. *Teachers College Record*, 19:319–335, 1918.

[36] W.H. Kilpatrick. *Foundations of method: Informal talks on teaching*. Macmillan, New York, 1925.

[37] Ingo Klöckl. *LaTeX2e: Tips und Tricks*. Heidelberg. dpunkt Verlag, 2000.

[38] Helmut Kopka. *LaTeX Band 1 - Einführung*. Addison-Wesley, München, 3. edition, 2000.

[39] Markus G. Kuhn. Probability Theory for Pickpockets - ec-PINGuessing, 30 July.

[40] RSA Laboratories. Faq - frequently asked questions about todayscryptography. Technical report, USA, 1998.

[41] Leslie Lamport. *Das LaTeX Handbuch*. Addison-Wesley, München, 1995.

[42] L. D. Landau and E. M. Lifshitz. *Mechanics*, volume 1 of *Course of theoretical physics*. Butterworth Heinemann, 3. edition, 1981. Translated by J. B. Sykes and J. S. Bell.

[43] Laura Lemay and Charles L. Perkins. *Java in 21 Tagen*. Markt+Technik Buch- und Software-Verlag GmbH, Haar bei Mnchen, erste edition, 1997.

[44] Ingo Linkweiler and Ludger Humbert. Ergebnisse der Untersuchung zur Eignung einer Programmiersprache fr die schnelle Softwareentwicklung – kann der Informatikunterricht davonprofitieren? `http://www.ham.nw.schule.de/pub/bscw.cgi/d23460/24_September_2002_Linkweiler.pdf`, sep 2002.

[45] Ralph Matzky. Das Signaturgesetz. *LogIn - Informatische Bildung und Computer in derSchule*, 5/99:27ff, 1999.

[46] Jagdish Mehra and Helmut Rechenberg. *The historical development og quantum theory*, volume 1. Springer-Verlag, New York, 1982.

[47] Inc. Microsoft Corporation. *bla bla*. 1 edition, 1999.

[48] Robert Morris and Ken Thompson. Password security: A case history, 1978.

[49] National Bureau of Standards. Data encryption standard (des). Technical Report FIPS PUB 46-2, U.S. Department of Commerce, 1993.

[50] J. Nielsen. *How to Conduct a Heuristic Evaluation*. s.a. Retrieved March 23, 2001 from the World Widehttp://www.useit.com/papers/test_u.html.

[51] Dag Arne Osvik. Speeding up serpent. Technical report, N-5020 Bergen, Norwegen, Mz 2000.

[52] Ronald L. Rivest and other. The rc6 block cipher, September 1999.

[53] R.L.Rivest, A.Shamir, and L.M.Adleman. A method for obtaining digital signatures andpublic-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[54] Hans-Joachim Schneider. *Lexikon der Informatik und Datenverarbeitung*. R. Oldenbourg, Mnchen Wien, zweite edition, 1986.

[55] Bruce Schneier. *Angewandte Kryptographie*. Addison-Wesley, Bonn, erste edition, 1996.

[56] Bruce Schneier and other. *Twofish: A 128-Bit Block Cipher*. Counterpane Systems, Minneapolis USA, 1998.

[57] Andreas Schwill. Fundamentale Ideen der Informatik. *Zentralblatt fr Didaktik der Mathematik*, 1:20–31, 1993.

[58] Andreas Schwill. Programmiersprachen im Unterricht. `http://www.informatikdidaktik.de/Forschung/Schriften/PSimUnterrMatNatTag.pdf`, 1998.

[59] Robert Sedgewick. *Algorithms*. Addison-Wesley Publishing Company, Reading, Massachusetts, second edition, 1889.

[60] SuSE GmbH. *Installation, Konfiguration und erste Schritte mitSuSe Linux 6.3*. SuSE GmbH, Nrnberg, sechzehnte edition, 1999.

[61] S. Vaudenay. On the need for multipermutations: Cryptoanalysis ofmd4 and safer. *Fast Software Encryption*, Second International Workshop Proceedings:286–297, 1995.

[62] Herbert Voß. APL-Font SAXPSA (als pdf-Datei). http://www.perce.de/lyx/apl2.pdf, 2001.

[63] Herbert Voß. Farbige Mathematik. 2/04:81–87, March 2004.

[64] Herbert Voss. *PSTricks: Grafik mit PostScript für TEX und LATEX*. DANTE/Lehmanns, Heidelberg/Hamburg, 2. edition, 2005.

[65] Aaron E. Walsh. *Java für Dummies: gegen den täglichen Frustmit Java*. International Thomson Publishing GmbH, Bonn, erste edition, 1997.

[66] Helmut Witten, Irmgard Letzner, and Ralph-HardoSchulz. RSA & co in der Schule - Moderne Kryptologie,raffinierte Protokolle. *LOG IN, Informatische Bildung und Computer in derSchule*, (3/4,5):57–64 and 31–39, 1998.

[67] Reinhard Wobst. *Abenteuer Kryptologie*. Addison-Wesley, Bonn, zweite edition, 1998.

[68] Dietmar Wjen. *Kryptologie*. Technische Universit, Braunschweig, erste edition, 1999.

[69] Ursula Meyer zu Natrup and Hanns-Wilhelm Heibey. Datenschutz und informationstechnische Sicherheit imInternet. *LogIn - Informatische Bildung und Computer in derSchule*, 5/99:8ff, 1999.