Ausklang

Bevor sich unsere Wege wieder trennen, möchte ich Ihnen, verehrte Leserin, lieber Leser, das folgende Wort des Dichter Novalis (1772 - 1801) in Erinnerung rufen.

In diesem Gedicht drückt sich die Sehnsucht nach einer Welt aus, in der Kryptologie überflüssig ist. Nach Meinung des Dichters wird diese Welt Wirklichkeit, wenn man nur ein Zauberwort weiß und es ausspricht:

Wenn nicht mehr Zahlen und Figuren
Sind Schlüssel aller Kreaturen,
wenn die, so singen oder küssen,
mehr als die Tiefgelehrten wissen,
wenn sich die Welt ins freie Leben
und in die Welt wird zurückbegeben,
wenn dann sich wieder Licht und Schatten
zu echter Klarheit werden gatten
und man in Märchen und Gedichten
erkennt die wahren Weltgeschichten,
dann fliegt von einem geheimen Wort
das ganze verkehrte Wesen fort.

Entschlüsselung der Geheimtexte

Im folgenden finden Sie Lösungshinweise zu einigen Übungsaufgaben. Die Hinweise sind so gestaltet, dass Sie noch die Chance haben, ein wenig nachzudenken.

Kapitel 1.
Übungsaufgabe **1**: Ich wusste es ja!
Übungsaufgabe **15**: Moni, Moni!
Übungsaufgabe **20**: Die Lösung finden Sie *vor* Seite 1.

Kapitel 2.
Übungsaufgabe **5**: BXMFF, LEU, ZHUM
Übungsaufgabe **7**: Lesen Sie in [Sin02] den Abschnitt über Blaise de Vigenère.
Übungsaufgabe **17**: NEIN!

Kapitel 5.
Übungsaufgabe **2**: Eine meiner amerikanischen Freunde, der diese Aufgabe lösen sollte, schrieb mir:

„You should have given a hint: The man is a second-rate mathematician! Then I would have gotten it right away. He's the French mathematician *Charles P. Tebeau*. Of course, it could also been the German *Albrecht E. Pause*, who is not so well known. My colleague, who is very clever at these things, argued that it must be *Beulah C. Streep*, the feminist author from the Bronx who ran unsuccessfully for congress; his second guess would be *Peaches Butler*, a porno star from Atlanta, Georgia, suspected of having an affair with the governor."

Literaturverzeichnis

Der Klassiker von Kahn [Kah96] und das Buch von Franke [Fra82] sind sehr lesenswerte Darstellungen der Geschichte der Kryptologie, in denen insbesondere die Entwicklungen bis 1945 detailliert geschildert sind. Zur Vertiefung der in diesem Buch dargestellten Themen können [BSW], [BP82], [DP89], [FR94], [Ruh87] und [Schn93] dienen, während die Lektüre der empfehlenswerten kryptographischen Bücher [Buc01], [Den83], [HKW85], [Hor85], [Kob87], [Koh81], [Kra86], [MM82], [SP89] zum Teil erhebliche mathematische Anforderungen an den Leser stellt.

[BDG95] J. L. Balcazar, J. Diaz, J. Gabarro: Structural Complexity I. Springer-Verlag, Heidelberg, 2. Auflage 1995.

[BRK01] A. Bartholome, J. Rung, H. Kern: Zahlentheorie für Einsteiger. Vieweg, Braunschweig und Wiesbaden, 3. Auflage 2001.

[Bau] Friedrich L. Bauer: Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie. Springer-Verlag, Berlin, Heidelberg, 2000.

[BP82] H. Beker and F. Piper: Cipher Systems. The Protection of Communication. Northwood, London 1982.

[BFS92] Th. Beth, M. Frisch, G.J. Simmons: Public-Key Cryptography: State of the Art and Future Directions. Springer, Lecture Notes in Computer Science 578 (1992).

[Beu86] A. Beutelspacher: Luftschlösser und Hirngespinste. Vieweg, Braunschweig und Wiesbaden 1986.

[Beu96] A. Beutelspacher. Geheimsprachen. C.H. Beck Verlag München, 3. Auflage 2002.

[BKP91] A. Beutelspacher, A. Kersten, A. Pfau: Chipkarten als Sicherheitswerkzeug. Springer-Verlag, Heidelberg 1991.

[BR89] A. Beutelspacher, U. Rosenbaum: Sicherer Zugang zu Betriebssystemen mit der Chip-Karte. 8. GI-Fachgesprächs über Rechenzentren, Informatik-Fachberichte 207 (Hg. J. Knop), 186-193 (1989).

[BS93] A. Beutelspacher, J. Schwenk: Was ist Zero-Knowledge? Math. Semesterber. 40, 73-85 (1993).

[BSW] A. Beutelspacher, J. Schwenk, K.-D. Wolfenstetter: Moderne Verfahren der Kryptographie. Von RSA bis Zero-Knowledge. Vieweg, Braunschweig und Wiesbaden, 4. Auflage 2001.

[MBeu86] M. Beutelspacher: Kultivierung bei lebendigem Leib. Drumlin Verlag, Weingarten 1986.

[BS91] E. Biham and A. Shamir: Differential Cryptanalysis of DES-like Cryptosystems. J. Cryptology 4 (1991), 3-72.

[BS93] E. Biham and A. Shamir: Differential Cryptanalysis of the Data Encryption Standard. Springer-Verlag, Berlin, ... 1993.

[Buc01] J. Buchmann: Einführung in die Kryptographie. Springer-Verlag, Berlin, Heidelberg, 2. Auflage 2001.

[BDPW90] M.V.D. Burmester, Y. Desmedt, F. Piper, M. Walker: A General Zero-Knowledge Scheme. Advances in Cryptology ? EUROCRYPT '89. Springer Lecture Notes in Computer Science 434 (1990), 122-133.

[CCITT] CCITT Recommendation X.509: The Directory ? Authentication Framework, 1988.

[Cha81] D. Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Comm. ACM 24 (1981), 84-88.

[Cha85] D. Chaum: Security without Identification: Transaction systems to Make Big Brother Obsolete. Comm. ACM 28 (1985), 1030-1044.

[CFN90] D. Chaum, A. Fiat, M. Naor: Untraceable Electronic Cash. Advances in Cryptology – CRYPTO '88. Springer Lecture Notes in Computer Science 403, 1990, 319-327.

[CBZ99] C. Creutzig, A. Buhl, P. Zimmermann: PGP. Pretty Good Privacy. Der Briefumschlag für Ihre elektronische Post. FoeBuD e.V. Bielefeld 1999.

[DR01] J. Daemen and V. Rijmen: The Design of Rijndael. Springer, 2001.

[DP89] D.W. Davies, W.L. Price: Security for Computer Networks. John Wiley & Sons, Chichester 1984, 2nd edition 1989.

[Den83] D. Denning: Cryptography and Data Security. Addison Wesley, Reading, Mass. 1983.

[Dif88] W. Diffie: The First Ten Years of Public-Key Cryptography. Proceedings of the IEEE 76 (5) (1988), 560-577.

[DH76] W. Diffie and M.E. Hellman: New directions in cryptography. Trans. IEEE Inform. Theory, IT-22, 6 (1976), 644-654.

[ElG85] T. ElGamal: A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. on Inform. Theory, Vol. IT-31 (1985), 469-472.

[FS87] A. Fiat and A. Shamir: How To Prove Yourself: Practical Solutions to Identification and Signature Problems. Advances in Cryptology – CRYPTO '86. Springer Lecture Notes in Computer Science 263 (1987), 186-194.

[Fra82] H.W. Franke: Die geheime Nachricht. Umschau-Verlag, Frankfurt/Main 1982.

[Fra84] O.I. Franksen: Mr. Babbage's Secret. The Tale of a Cypher ? and APL. Prentice Hall, Englewood Cliffs, 1984.

[FFKK93] O. Fries. A. Fritsch, V. Kessler, B. Klein (Hrsg.): Sicherheitsmechanismen. Bausteine zur Entwicklung sicherer Systeme. Oldenbourg Verlag, München, Wien 1993.

[FP90] W. Fumy und A. Pfau: Asymmetric Authentication Schemes for Smart Cards – Dream or Reality? Proc. IFIP SEC '90. Espoo, Finnland.

[FR94] W. Fumy, H.P. Rieß: Kryptographie – Entwurf, Einsatz und Analyse symmetrischer Kryptosysteme. Oldenbourg, München ^{2}1994.

[GMR89] S. Goldwasser, S. Micali, C. Rackoff: The Knowledge Complexity of Interactive Proof-Systems. SIAM J. Comput. 8(1) (1989), 186-208.

[Gor85] J. Gordon: Strong Primes are Easy to Find. Advances in Cryptology ? EUROCRYPT '84. Springer Lecture Notes in Computer Science 209 (1985), 216-223.

[HKW85] F.-P. Heider, D. Kraus und M. Welschenbach: Mathematische Methoden der Kryptoanalyse. Vieweg, Braunschweig, Wiesbaden 1985.

[Hen99] N. Henze: Stochastik für Einsteiger. Eine Einführung in die faszinierende Welt des Zufalls. Vieweg-Verlag, Braunschweig, Wiesbaden 1999.

[Hon73] R. Honsberger: Mathematical Gems I. MAA 1973.

[Hor85] P. Horster: Kryptologie. B.I.-Wissenschaftsverlag, Mannheim ? Wien ? Zürich 1985.

[Hor96] P. Horster (Hrsg.): Digitale Signaturen. Grundlagen, Realisierungen, Rechtliche Aspekte, Anwendungen. DuD-Fachbeiträge. Verlag Vieweg, Braunschweig / Wiesbaden 1996.

[ISO] ISO IS 7498/2: Open Systems Interconnection Reference Model ? Part 2: Security Architecture.

[Jö01] D. Jörgensen: Der Rechenmeister, Aufbau TB, Berlin 2001.

[Kah96] D. Kahn: The Codebreakers. Macmillan, New York, revised edition 1996.

[Kip] R. Kippenhahn: Verschlüsselte Botschaften. Geheimschrift, Enigma und Chipkarte. rororo-Taschenbuch, 1999.

[Kob87] N. Koblitz: A Course in Number Theory and Cryptography. Springer-Verlag, New York 1987.

[Kob98] N. Koblitz: Algebraic Aspects of Cryptography. Springer-Verlag, New York 1998.

[Kra86] E. Kranakis: Primality and Cryptography. John Wiley & Sons, Chichester 1986.

[LM90] A.K. Lenstra and M.S. Manasse: Factoring by electronic mail. Advances in Cryptology – EUROCRYPT '89. Springer Lecture Notes in Computer Science 434 (1990), 355-371.

[Mas69] J.L.Massey: Shift-register Synthesis and BCH Decoding. IEEE Inform. Theory, IT-15, 1 (1969), 122-127.

[Mas83] J.L. Massey: Logarithms in finite cyclic groups – cryptopgraphic issues. Proceedings of the 4th Benelux Symposium on Information Theory (1983), 17-25.

[Mau90] U. Maurer: Fast generation of secure RSA-moduli with almost maximal diversity. Advances in Cryptology ? EUROCRYPT '89. Springer Lecture Notes in Computer Science 434 (1990), 636-647.

[McE78] R.J. McEliece: A public-key cryptosystem based on algebraic coding theory. JPL DSN Progress Report 42-44, pp. 114-116, Jan.-Feb. 1978.

{MOV96] A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone: Handbook of Applied Cryptography, CRC Press, 1996.

[MH78] R.C. Merkle and M.E. Hellman: Hiding information and signatures in trapdoor knapsacks. IEEE Trans. Inf. Theory, IT-24 (1978), 525-530.

[MM82] C.H. Meyer, S.M. Matyas: Cryptography: A New Dimension in Computer Data Security. John Wiley & Sons, New York 1982.

[NIST91] National Institute of Standards and Technology (NIST): A Proposed Digital Signature Algorithm (4. Sept. 1991).

[Omu90] J.K. Omura: Novel Applications of Cryptography in Digital Communications. IEEE Communications Magazine, May 1990, 21-29.

[Per86] G. Perec: Anton Voyls Fortgang. Zweitausendeins, Frankfurt 1986.

[QG90] J.-J., M., M., M. Quisquater and L., M., G., A., G., S. Guillou: How to explain Zero-Knowledge Protocols to Your Children. Advances in Cryptology ? CRYPTO '89. Springer Lecture Notes in Computer Science 435 (1990), 628-631.

[RE99] W. Rankl und W. Effing: Handbuch der Chipkarten. Aufbau – Funktiosnweise-Einsatz von Smart Cards. Hanser-Elektronik, 3. Auflage 1999.

[RSA78] R. Rivest, A. Shamir and L. Adleman: A method for obtaining digital signatures and public key cryptosystems. Comm. ACM 21 (1978), 120-126.

[Rue86] R. Rueppel: Analysis and design of Stream Ciphers. Springer-Verlag 1986.

[Ruh87] Ch. Ruhland: Datenschutz in Kommunikationsnetzen. Datacom-Verlag Pulheim 1987.

[Sal90] A. Salomaa: Public-Key Cryptography. Springer-Verlag, EATCS Monographs on Theoretical Computer Science Vol. 23, 1990.

[Schn00] B. Schneier: Angewandte Kryptographie. Protokolle, Algorithmen und Sourcecode in C. Addison-Wesley, München, 2000.

[SP89] J. Seberry and J. Pieprzyk: Cryptography. An Introduction to Computer Security. Prentice Hall 1989.

[Sim79] G.J. Simmons: Cryptology: The mathematics of secure communication. The Mathematical Intelligencer **1** (1979), 233-246.

[Sim92] G.J. Simmons: Contemporary Cryptology. The Science of Information Integrity. IEEE Press, New York 1992.

[Sin00] S. Singh: Geheime Botschaften. dtv 2001.

[Sin02] S: Singh: Codes. Hanser 2002.

[Sha82] A. Shamir: A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem. Proc. 23rd IEEE Symp. Found. Computer Sci. 142-152 (1982).

[Sha49] C.E. Shannon: Communication theory of secrecy systems. Bell. Sys. Tech. J. 30 (1949), 657-715.

[Smi71] L. D. Smith: Cryptography. The Science of Secret Writing. Dover Publications, New York 1971.

[Sti95] D. R. Stinson: Cryptography. Theory and Practice. CRC Press, Boca Raton London Tokyo 1995

[Str56] D.J. Struik: A concise History of Mathematics. Dover Publications, Inc. 1956.

[Wel01] M. Welschenbach: Kryptographie in C und C++. Zahlentheoretische Grundlagen, Computer-Arithmetik mit großen Zahlen, kryptographische Tools. Springer-Verlag, Berlin, Heidelberg, 2. Auflage 2001.

[WA75] H. Wußing und W. Arnold: Biographien bedeutender Mathematiker. Aulis Verlag Deubner & Co., Köln 1975.

Unter den regelmäßigen Veröffentlichungen zur Kryptologie müssen die folgenden Zeitschriften erwähnt werden:

- Journal of Cryptology (Springer Verlag),
- Designs, Codes and Cryptography (Kluwer) und
- Computer & Security (Elsevier),

die einen theoretisch-wissenschaftlichen Anspruch haben, während

- Cryptologia (Rose Hulman Institute)

sich schwerpunktmäßig mit der Geschichte der Kryptologie beschäftigt;

- KES Zeitschrift für Kommunikations- und Datensicherheit (Peter Hohl Verlag)

ist eine allgemeinverständliche Zeitschrift, in der man auch Beschreibungen von Produkten findet;

- Datenschutz und Datensicherung (Vieweg Verlag)

stellt insbesondere Zusammenhänge zwischen Technik und Recht dar.

Die Lecture Notes in Computer Science (Springer) veröffentlichen jährlich zwei Bände unter dem Titel *Advances in Cryptology*; dies sind die Proceedings der wichtigsten Tagungen über Kryptologie, nämlich der EUROCRYPT und der CRYPTO. Zusammen mit dem Journal of Cryptology sind diese Bände ein Muss für jeden, der sich einen Eindruck vom aktuellen Fortschritt der Kryptologie verschaffen will.

Ein Verzeichnis aller Listen mit frequently asked questions ist unter

http://www.faqs.org/faqs/cryptography-faq/

zu finden. Die Seite

http://www.infoserversecurity.org

ist eine sehr gute Startseite mit vielen Kryptographie-links.

In den Newsgroups: *sci.crypt*, *sci.crypt.research* wird – wie in den meisten Newsgroups – alles mögliche diskutiert, manchmal auch etwas Wichtiges.

Index