# Ausklang

Bevor sich unsere Wege wieder trennen, möchte ich Ihnen, verehrte Leserin, lieber Leser, das folgende Wort des Dichters Novalis (1772 bis 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**:

**Polya lphab etisc heal g**
**orith menha bendi e Eige**
**nscha ft, das sein b estim**
**mter G eheim textb uchst**
**abeme hrals einen Klart**

**extbu chsta benda rstel**
**lenka nn. Abe rmand arfni**
**cht ve rgess en, das s der G**
**eheim textd en Kla rtext**
**einde utigb estim men mu**
**ss.**

Übungsaufgabe **17**: NEIN!

*Kapitel 5.*
Übungsaufgabe **2**: Einer 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 be the German, **Albrecht E. Pause**, who is 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 [Kah67] 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 [BP82], [DP89], [FR94], [Ruh87] und [Schn93] dienen, während die Lektüre der empfehlenswerten kryptographischen Bücher [Den83], [HKW85], [Hor85], [Kob87], [Koh81], [Kra86], [MM82], [SP89] zum Teil erhebliche mathematische Anforderungen an den Leser stellt.


[BDG88] J. L. Balcázar, J. Díaz, J. Gabarró: *Structural Complexity I.* Springer-Verlag, Heidelberg, 1988.

[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: *Luftschösser und Hirngespinste.* Vieweg, Braunschweig und Wiesbaden 1986.

[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).

[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.

[Bos94] K. Bosch: *Elementare Einführung in die Wahrscheinlichkeitsrechnung*. Vieweg-Verlag, Braunschweig, Wiesbaden 51994.

[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.

[Cox63] H.S.M. Coxeter: *Unvergängliche Geometrie*. Birkäuser, Basel 1963.

[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.

[Fie89] K. Fietta: *Chipkarten: Technik, Sicherheit, Anwendungen*. Hüthig-Verlag, Heidelberg 1989.

[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.

[Fre84] G. Frey: *Elementare Zahlentheorie.* Vieweg, Braunschweig, Wiesbaden 1984.

[Fri90] F. Fricker: *Neue Rekord-Faktorisierung.* Spektrum der Wissenschaft 11/1990, 38-42.

[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 ²1994.

[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.

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

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

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

[Kah67] D. Kahn: *The Codebreakers.* Macmillan, New York 1967.

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

[Koh81] A.G. Konheim: *Cryptography. A Primer.* John Wiley & Sons, New York 1981.

[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.

[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.

[Opp92] R. Oppliger: *Computersicherheit. Eine Einführung.* Verlag Vieweg, Braunschweig, Wiesbaden 1992.

[Pad89] F. Padberg: *Elementare Zahlentheorie.* B.I.-Wissenschaftsverlag, Mannheim, Wien, Zürich 1989.

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

[Pom91] K. Pommerening: *Datenschutz und Datensicherheit.* B.I.-Wissenschaftsverlag 1991.

[QG90] J.-J., 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.

[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.

[Scha92] I. Schaumüller-Bichl: *Sicherheits-Management.* B.I.-Wissenschaftsverlag, Mannheim, Leipzig, Wien, Zürich 1992.

[Schn93] B. Schneier: *Applied Cryptography. Protocols, Algorithms, and Source Code in C.* John Wiley & Sons, New York 1993.

[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.

[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.

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

[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) und
- *Computer & Security* (Elsevier),

die beide 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.

# Namen- und Sachverzeichnis


additive Chiffre 13
affine Chiffre 28
aktiver Angriff 79
Alberti, Leon Battista 13
Alberti-Algorithmus 53
Algorithmus 14
Al-Khwarizmi, Muhamad ibn Musa 94
Alphabet 11
Anonymität 149
ASCII 129
asymmetrischer Algorithmus 113
asymmetrischer Riegel 121
asymmetrisches Kryptosystem 114
asymmetrisches Signaturschema 114, 119
asymmetrisches Verschlüsselungssystem 114
Authentizität 82
a posteriori-Wahrscheinlichkeit 59
a priori-Wahrscheinlichkeit 59

Babbage, Charles 40
Benutzerauthentikation 81, 86
beobachtete Wahrscheinlichkeit 59
Berlekamp-Massey-Algorithmus 75
Bigramm 25
Briefkastenbeispiel 116
Broadcasting 153
Buchstabenwurm 50

Caesar, C. Julius 13
Cardano, Geronimo 95
Certification Authority 147
Challenge-and-Response 91
Chaum, David 155
Chiffrieren 11
Chiffriersystem 57
Chipkarte 100
chosen plaintext attack 24
Cipher-Block-Chaining-Modus 84

Dechiffrieren 11
Della Porta, Giovanni Battista 37
DES 24, 26, 30
Dethloff, Jürgen 100
Diffie, Whitfield 113
Diffie-Hellman-Schlüsselaustausch 138
diskreter Logarithmus 139

Einweg-Hashfunktion 85
Einwegfunktion 88
electronic cash 103
elektronisches Geld 155
elektronische Unterschrift 119
ElGamal, Taher 141
ElGamal-Schema 141
ElGamal-Signaturschema 142
e-mail-Methode 135
erweiterter euklidischer Algorithmus 126
euklidischer Algorithmus 125
Euler, Leonhard 123

Fermat-Zahl 128
Fiat, Amos 97
Fiat-Shamir-Protokoll 98
Friedman, William Frederick 39
Friedman-Test 43

Galois, Evariste 141
Gartenzaun-Algorithmus 28

geheimer Schlüssel 114
Geheimtext 11
ggT 125
Goldwasser, Shafi 97
Gröttrup, Helmut 100
Guillou, Louis 109

Hellman, Martin 113
Helmlé, Eugen 29
homophone Chiffre 35
Hybridsystem 136

Indikator 53
Integrität 82
interaktiv 97

Kappa-Test 44
Kasiski, Friedrich Wilhelm 39
Kasiski-Test 40
Kerckhoffs von Nieuwenhof, . . . Auguste 23
Klartext 11
Knapsack-Algorithmus 145
known ciphertext attack 24
known plaintext attack 24
Kofferbeispiel 145
Koinzidenzindex 44
kollisionsfrei 85
Kryptoanalyse 10
Kryptogramm 11
Kryptographie 10
kryptographischer Fingerabdruck 83
kryptographische Prüfsumme 83
Kryptologie 10

Lenstra, Arjen K. 135
lineare Komplexität 75
linear rückgekoppeltes Schieberegister 68
lipogrammatisch 28

Magische Tür 109
MAC 83
Manasse, Mark S. 135
Massey, Jim 141
Massey-Omura-Schema 142
McEliece-Schema 145
Message-Authentication-Code 83
Micali, Silvio 97
MIX 159
modulare Inverse 126
modulo 2 68
Moreno, Roland 100
Mr. X 16
monoalphabtisch 20
Münzgeld 151

Nachrichtenauthentikation 81
Nachrichtenintegrität 80
natürliche Sprache 26
nichtlineares Schieberegister 74
Notdurftanbieter 152
Novalis 167

öffentlicher Schlüssel 114
Omura, Jim 141
one-time pad 64

passiver Angriff 10
Paßwort 87
Perec, George 29
Periode eines Schieberegisters 70
perfekte Sicherheit 51, 60
polyalphabetisch 35
POS-Banking 103
praktisch unmöglich 85
Prinzip von Kerckhoffs 23
privater Schlüssel 114
Pseudonym 153
Pseudoprimzahl 129
pseudozufällige Folge 66
public-key-Algorithmus 113

Quadratwurzelspiel 95
Quisquater, Jean-Jaques 109

Rackoff, Charles 97
RSA-Algorithmus 122
Rauschen 154
Rückkopplung 68

Schieberegister 67
Schlaube, Peter A. 121
Schlüssel 14
Schlüsselwort 22
Shakespeare, William 109
Shannon, Claude 57
Shamir, Adi 97
Shamirs no-key-Algorithmus 142
Skytale 11
Square-and-Multiply-Algorithmus 146
Substitutionsalgorithmus 12
symmetrischer Algorithmus 10, 113

Tartaglia, Niccolò 94
Tauschchiffre 22
teilerfremd 127
theoretische Wahrscheinlichkeit 59
Transformation 57
Transpositionsalgorithmus 12
Trithemius, Johannes 37
triviale Chiffrierung 13
Turing, Alan 2

umkehrbare Transformation 57
Verschiebechiffren 13
Vernam, Gilbert 64
Vielfachsummendarstellung 126
Vigenère, Blaise de 37
Vigenère-Algorithmus 38
Vigenère-Quadrat 38

XOR 68

Zero Knowledge 93
Zertifikat 106, 147
Zustand eines Schieberegisters 67

# Bücher aus dem Umfeld

## Projektive Geometrie

Von den Grundlagen bis zur Anwendung

von Albrecht Beutelspacher und Ute Rosenbaum

1992. VI, 229 Seiten.
(vieweg studium; Aufbaukurs Mathematik, Bd. 41;
hrsg. von Aigner, Martin/ Fischer, Gerd/ Grüter, Michael/
Knebusch, Manfred/ Wüstholz, Gisbert) Paperback.
ISBN 3-528-07241-5

Dieses Lehrbuch präsentiert projektive Geometrie, ein wichtiges klassisches Gebiet der Mathematik, in neuem Gewand: Ein Akzent liegt auf überraschenden und wichtigen Anwendungen von Geometrie in Codierungstheorie und Kryptographie. Dazu werden alle benötigten Teile der klassischen projektiven Geometrie (synthetische und analytische Geometrie, Quadriken) bereitgestellt. Das Buch ist in moderner mathematischer Sprache geschrieben. Zahlreiche Abbildungen und weit über hundert meist einfache Übungsaufgaben unterstützen das Verständnis des Stoffes. Es eignet sich vorzüglich zum Selbststudium.

*Über den Autor:* Prof. Dr. Albrecht Beutelspacher lehrt im Schwerpunkt Geometrie und Diskrete Mathematik des Fachbereichs Mathematik an der Justus-Liebig-Universität in Gießen.

Verlag Vieweg · Postfach 1547 · 65005 Wiesbaden · Fax (0611) 78 78 420

vieweg