

---

## Literaturverzeichnis

Zum Gebiet der Codierungsverfahren gibt es eine Fülle von Büchern und Artikeln, in denen Übersichten und Einzelheiten dargestellt sind. Da die zugrunde liegende Mathematik der Algebra endlicher Ganzzahl-Körper angehört und vielen von uns diese Welt nicht geläufig ist, müssen man sich hier erst etwas eingewöhnen (wenngleich wir manches in anderer Form bereits kennen). Tut man dieses aber, dann belohnen uns die Codierungsverfahren mit reichhaltigen, vielseitigen Erkenntnissen. Auf *Spezialaufsätze* wird im Text verwiesen.

Das vorliegende Buch unterstützt das Erreichen der im Unterkapitel 2.5 skizzierten Ziele. Zur Ergänzung kann die nachfolgend genannte Literatur hinzugezogen werden (auf jeden Fall sollte nach dem Durcharbeiten dieses Buches hier eine gute Grundlage zum tieferen Einstieg geschaffen sein, sofern dieser erforderlich ist):

**Jiri Adamek:** Foundations of Coding, 1991, John Wiley, ISBN 0-471-62187-0 (guter Überblick zur Datenfehlerbeseitigung, sehr ausführlich, mit kurzem Ausblick auf Verschlüsselungsverfahren)

**W. Wesley Peterson und E.J. Weldon:** Error correcting methods, 1971, MIT Press, Cambridge (etwas älterer, aber sehr umfassender "Klassiker" zur Datenfehlerbeseitigung)

**Steinbuch, Rupprecht:** Nachrichtentechnik Band 3, Nachrichtenverarbeitung, 1982, Springer-Verlag (zur Nachrichten- und Informationstheorie)

**Albrecht Beutelsbacher:** Kryptologie, 1991, Vieweg, ISBN 3-528-18990-8 (sehr gut und leicht zu lesender, dabei aber doch sehr fundierter Überblick auf die Verschlüsselungsverfahren)

**Albrecht Beutelsbacher, Jörg Schwenk, Klaus-Dieter Wolfenstetter:** Moderne Verfahren der Kryptographie (von RSA zu Zero-Knowledge), 1995, Vieweg, ISBN 3-528-06590-7 (eine vorzügliche Ergänzung zum vorgenannten Werk, was weitere neue Verfahren kompakt darstellt)

**Martin E. Hellmann:** Die Mathematik neuer Verschlüsselungssysteme, Spektrum der Wissenschaften, Heft 10/1979 (mit Beispielen versehener, gut verständlicher Kurzbeitrag zur Verschlüsselung; von einem der bekanntesten Wissenschaftler dieses Fachgebiets)

**DTV-Atlas Mathematik**, Band 1, ISBN 3-423-03007-0 (als Nachschlagewerk für Fragen der Mathematik), zum Einstieg in die - nicht minder - interessanten Nachbargebiete unter anderen geeignet.

**Hans Riesel**: Prime Numbers and Computer Methods for Factorization, 1985, Birkhäuser, ISBN 0-8176-3291-3 (Mathematische Grundlagen für die modernen Verschlüsselungsverfahren)

**Ian Stewart, David Hall**: Algebraic Number Theory, 1986, Chapman and Hall (Grundlagen der Zahlentheorie)

**Jörg Sauerbrey**: Langzahl-Modulo-Arithmetik für kryptographische Verfahren, 1993, Deutscher Universitäts Verlag, ISBN 3-8244-2048-1

**Ingrid Schaumüller-Bichl**: Sicherheitsmanagement, BI-Verlag, ISBN 3-411-15501-9 (Schwerpunkte sind hier zwar Fragen der Informationssicherung, das Buch enthält u.a. aber auch kurze Beschreibungen verschiedener aktueller Verschlüsselungsverfahren (z.B. DES) und gibt dazu interessante Bewertungen zur Leistungsfähigkeit)

**Charles P. Pfleeger**: Security in Computing, 1989, Prentice-Hall International Editions, ISBN 0-13-799016-2 (enthält im Abschnitt 3 einige kurzgefaßte Darstellungen zu Verschlüsselungstechniken, setzt sich aber hauptsächlich mit den interessanten Fragen der Informationssicherung auseinander)

**Heider, Kraus, Welschenbach**: Mathematische Methoden der Kryptoanalyse, 1985, Vieweg, ISBN 3-528-03601-X (behandelt ausführlich die mathematischen Grundlagen der Verschlüsselungsverfahren, u.a. auch diejenigen der Primzahlenerzeugung; als Ergänzung zum Buch von Beutelsbacher zu empfehlen)

**Kiyek/Schwarz**: Mathematik für Informatiker 2, 1991, Teubner, ISBN 3-519-02278-8 (als umfassendes Nachschlagewerk für Fragen der Informatik, allerdings für den Ingenieur nicht gerade leicht zu lesen; ein Schwerpunkt ist unter vielen anderen die Erzeugung großer Pseudoprimzahlen)

**W. Leonhard**: Statistische Analyse linearer Regelsysteme, 1973, Teubner, ISBN 3-519-02046-7 (sehr praxisorientierte Ergänzung speziell zu den im Kapitel 5 verwendeten Korrelationsverfahren)

---

**Rafael C. Gonzalez, Richard E. Woods:** Digital Image Processing, 1992, Addison-Wesley Publishing Company (Ein Überblick auf die Verfahren der Bildverarbeitung)

**Lüneburg:** Galoisfelder, Kreisteilungskörper und Schieberegisterfolgen, 1979, ISBN 3-411-01566-7 (mathematisch sehr interessante Ergänzung speziell zu den im Kapitel 5.1 behandelten Schieberegistern).

**Gunter Lepschies:** E-Commerce und Hackerschutz, 2.Auflage 2000, Vieweg-Verlag, DuD-Fachbeiträge, ISBN 3-528-15702-X (kompakter Überblick auf technische und organisatorische Probleme sowie deren Lösungen bei der Abwicklung von Geschäften mit elektronischen Medien, zum Beispiel über das Internet, als wesentliche Ergänzung und Erweiterung der in Kapitel 6 behandelten Themen)

## Sachwortverzeichnis

- Abtasttheorem 74
- AES (Advanced Encryption Standard) 259
- Autokorrelationsfunktion 228
- Bandbreite 61, 73, 74, 75, 77, 353, 356
  - eines Filters 355
  - um 1/R erweitert 71
- Bandbreiten-Ausnutzungsgrad 73
- binomische Formel 41
- Bitfehlerrate 63, 64, 65, 68
- Blockfehlerrate 69, 71, 72
- Charakteristik 41, 112, 113, 124, 137, 176
- chosen plaintext- Angriff 294
- Cipher-Block-Chaining 306
- Code 7, 15, 97, 132
  - (n,k)- 17
  - Alphabet 7
  - ASCII\_ 5
  - Balken- 4
  - BCH- 110, 129, 130, 161, 163, 188
  - Block- 5, 16
  - CRC 5
  - Datenkompressions- 5
    - Definition 7
  - Faltungen- 14
  - Faltungs-, Convolutional- 221
  - Farb 4
  - Geheim- 5
  - genetischer 4
  - Goppa- 163, 164, 170, 174, 287
  - IEC-Farb- 5
  - ISBN- 4
    - Länge 17
  - Morse- 3
  - nichtsystematischer 97, 98
  - Produkt- 47, 213
  - Reed-Muller- 199, 200, 204, 206
  - Reed-Solomon- 82, 132, 133, 144
  - Strich- 4
  - systematischer 16
    - Turbo-Produkt- 77, 220
    - Wiederholungscode 48
      - zyklischer 90, 97, 147, 154
- Codewort 12, 15, 16, 23, 49
- Codewortlänge 60, 77, 129, 144, 160
- CRC 152, 163, 276
- CRC-Polynom 152
- critical bands 354
- Dämpfungsfaktor 357
- Decodierung 47, 60, 67, 131, 152, 154
- DES (Data Encryption Standard) 258
- Diskrete Cosinus Transformation 19, 331, 341, 348
  - zweidimensionale 345
- diskreter Logarithmus 296
- Einwegfunktion 305
- Element
  - eines Codes 15
  - eines Codewortes 16
  - eines Erweiterungskörpers 102
  - eines Galoisfeldes 41, 118
  - eines Ganzzahlkörpers 32
  - eines p-Zahlensystems 16
  - eines Vektors 31
  - eines Zahlenkörpers 30
  - inverses 34, 36, 37
  - modulares inverses 44
  - neutrales 34
  - Null- 102
  - Ordnung eines... 40, 106, 109, 117, 119
  - primitives 40, 41, 129, 130, 131
- Empfangswort 13, 21, 111, 138, 144, 154, 155, 161, 175, 177, 202, 215, 223
- Empfangswortvektor 174
- Entschlüsselung 245, 247, 259, 263, 270, 273

- Euklidischer Algorithmus 42, 43, 44, 107, 170, 179, 194, 272  
für Polynome 43
- Euler  
-Funktion 42, 270, 283, 285  
Satz von 274  
-zahl 271, 272
- Fehler 62  
Block- 66  
-Bündel 108, 137, 144, 145, 151, 153, 211, 276  
-Bündel bei Turbo-Codes 214  
Einzel- 48, 49  
-Erkennung 47  
-Freiheit 57  
-Funktion, Gaußsche... 66  
-Häufigkeit 62  
-Korrektur 47, 55  
-Position 48, 50, 58  
-Rate 65  
Übertragungs- 48  
-Vektor 84, 174  
-Wahrscheinlichkeit 68  
-Wort 57
- Fehlerfalle 155
- Fehlerfallen-Decodierung 158
- Fermatsches Theorem 45, 106, 150, 153, 231
- Fourier 15  
-Analyse 337  
Diskrete Fourier Transformation 19  
Fast Fourier Transformation 19, 341  
-Koeffizienten 332, 334, 340, 349  
-Reihe 330, 336  
-Summe 332  
-Transformation 19, 226, 329, 330, 358, 359  
-Transformierte 61
- Fraktale 15, 361, 363
- Fundamentalsatz der Algebra 39, 101, 104, 107
- Generator  
-Matrix 54, 55, 56, 60, 84, 168, 191  
-Matrix beim McEliece-Verfahren 289  
-Matrix beim Reed-Muller-Code 199, 200, 205  
-Matrix für Goppacode 193  
-Polynom 90, 92, 95, 96, 98, 108, 109, 110, 113, 114, 118, 119, 129, 130, 133, 137, 150, 152, 159, 276, 305  
-Zahl 91  
Zufallszahlen- 248
- Gewicht eines Codewortes 18, 148
- Größter gemeinsamer Teiler  
bei Polynomen 171
- Größter gemeinsamer Teiler (ggT) 42, 43, 272  
bei Polynomen 45
- Gruppe 34  
Abelsche 34  
Additions- 37  
Eigenschaften einer 34  
Halb- 33  
kommutative 34  
Unter- 37
- Hammingabstand 18, 21, 25, 81, 85, 115, 146  
Mindest- 22, 26, 47, 49, 166, 198, 204, 209, 216
- Hamminggewicht 158
- Hash-Funktionen 306
- Hash-Summe 306, 307, 308, 309
- Häufigkeitsverteilung 9, 14, 243, 249, 293, 316, 318, 324  
flache 248
- Ideal 37
- Informations  
-Bits 11, 14  
-Elemente 290  
-Gehalt 17, 19  
-Menge, abstrakte 7  
-Mengen 5, 14  
-Polynom 223  
-Sicherheit 10, 256  
-Sicherung 241, 256, 308  
-Stellen 17, 30, 50, 51, 289  
-Stellen beim Hammingcode 52  
-Stellen, Anzahl der 17
- Informationsrate 17, 21, 48, 59, 61, 67, 71, 75, 137, 147, 173, 204, 217
- Informationsvektor 201

- Kanalkapazität 73, 74, 75, 78, 217  
 Kerckhoff, Gesetz von 268  
 known ciphertext-Angriff 293  
 known plaintext- Angriff 294  
 Körper 36, 325  
   -Charakteristik 41  
   der komplexen Zahlen 39  
   der reellen Zahlen 39  
   -Element 40, 41  
   endliche Ganzzahlkörper 30  
   endlicher 38  
   -Erweiterungen, algebraische 38  
   Erweiterungs- 34, 38, 40  
   Erweiterungskörper, endlicher 39  
   Galois- 41  
   Ganzzahl- 31  
 Korrelationsfunktion 228, 229  
 Kreisteilungspolynom 46, 106, 115, 151  
 Kreuzkorrelationsfunktion 231  
 Kryptoanalyse  
   differentielle 265  
 Maximalfolgenlänge 239, 240  
 McEliece-Verschlüsselung 287  
 Meggitt-Decodierung 157  
 Message-Authentication-Code (MAC) 306  
 Modulare  
   Inverse 45  
   inverse Polynome 44, 45, 170, 173, 182, 189  
   inverse Zahl 44, 272, 300, 310  
   Quadratzahl 297, 298  
   Wurzel 301  
 Modulo-Division 130, 152  
 Modulo-Funktion 30, 103, 280, 299  
 Nullstelle  
   des Fehlerpositionspolynoms 199  
 Nullstellen 39  
   Anzahl der 289  
   -Bestimmung 186  
   des Generatorpolynoms 110  
   eines irreduziblen Polynoms 40, 105  
   eines Kreisteilungspolynoms 107  
   eines Polynoms 39, 45, 100  
   im Erweiterungskörper 129  
   konjugiert komplexe 39  
   Mehrfach- 108  
   reziproke 234  
   unabhängige 113, 115, 133  
   und Fundamentalsatz 39  
   von irreduziblen Polynomen 38  
   zur Fehlerpositionsbestimmung 113  
 nullteilerfrei 35, 36  
 Nutzsinal 61, 62, 73  
   -Erkennung 238  
   KKF 240  
 Nutzsinalimpuls 240  
 one-time-pad 248, 249  
 Ordnung  
   einer Maximalfolgenfolge 249  
   einer Menge 35  
   eines Bandfilters 356  
   eines Galoisfeldes 290  
   eines Gleichungssystems 125  
   eines Körperelementes 40, 104, 106  
   eines Polynoms 101  
   eines primitiven Elements 129, 150  
   eines Schieberegisters 230, 294  
   eines Vektors beim Reed-Muller-Code 206  
   und Codelänge 119  
 Parität  
   gerade 50, 153  
   ungerade 153  
 Paritäts  
   -Block 214  
   -Bits 67, 213, 214, 328  
   -Gleichung 83, 84, 165, 189, 190  
   -Prüfbeziehung 83  
   -Prüfbit 5  
   -Prüfmatrix 56, 58, 60, 83, 154  
   -Prüfstellen 56  
 Paritätsprüfgleichung 83  
 Paßwort 241, 306  
   -Geschützter Zugang 241  
   -Verfahren 242, 258, 296  
 perfekte Verschlüsselung 10, 248  
 perfekter Code 57  
 Polynom  
   Anzahl irreduzibler 289  
   Binär- 165, 190, 247

- Codewort- 134, 151
- definierendes 103
- Division 92, 176
- Empfangswort- 112
- erzeugendes 188
- Fehler- 109, 110, 124, 138, 143
- Fehlerpositions- 140, 175, 179
- Generator- 92, 94, 98, 133, 151
- Grad 99
- Informations- 92, 110, 119, 134
- irreduzibles 100, 106, 116, 132, 135
- irreduzibles über  $\mathbb{R}$  102
- Koeffizienten 90, 92, 107
- Kreisteilungs- 106, 151
- lineares 170
- Merkmale 99
- Minimal- 41
- modulares inverses 170, 172, 173, 190
- Multiplikation 93
- Nullstelle 100, 103, 113
- Paar 182
- Produkt- 235
- Quadrat 181
- Rest- 92, 94, 95, 134, 182
- reziprokes 234
- Ring 101, 135
- Rückkopplungs- 226, 227, 251
- Rückkopplungs-, irreduzibles 231, 236
- Summe 190
- Syndrom- 109, 111, 154, 175, 185
- Teil- 100, 153, 180
- Teiler- 171
- über endlichen Zahlkörpern 101
- Zerlegbarkeit 99
- Primzahl** 36, 37, 41, 42, 100, 235, 255, 270, 287, 295
  - Größe einer 270
  - Pseudo- 271, 282, 283
  - Theorie 283
- Primzahlen**
  - Anzahl aller 282
  - Produkt zweier 42
- Primzahlensatz** 287
- Protokoll** 296, 312
  - Fiat-Shamir- 298
  - HDLC- 163
  - Zero-Knowledge- 297
- Redundanz** 5, 16, 152, 221, 313
- Restklassenmengen** 35, 36
- Restklassenringe** 36
- Ring**
  - Integritäts- 35
  - kommutativer 37
  - Restklassen- 36
  - von Polynomen 38
- RSA-Verschlüsselung** 270
- Rückkopplungspolynom** 250
- Schieberegister** 152, 195
  - als binärer Würfel 299
  - als MOD  $g(x)$ -Dividierer 96, 131
  - bei Faltungscodes 221
  - Folgen 41, 240
  - lineares 233
  - nichtlineare 252
  - rückgekoppelte 96, 223
  - und AKF der Maximallängenfolge 230
  - und irreduzible
    - Rückkopplungspolynome 232
    - zur Berechnung des Syndrompolynoms 161
    - zur Fehlerfallen-Decodierung 159
    - zur Schlüsselerzeugung 250
- Schlüssel**
  - asymmetrische 270
  - Erzeugung mit Schieberegistern 223, 241
  - geheimer 259, 270, 277, 292
  - Geheimhaltung 241
  - komplementäre .... beim DES 269
  - öffentlicher 270, 277, 292
  - schwache ... beim DES 268
  - Symmetrischer 259
  - Übergabe 250
  - Übertragung und -Übergabe 258
  - zufällig gewählter 248
- Schlüsselbestimmung mit**
  - Friedmann- und Kasiski-Tests 293
- Schlüsseltausch nach Diffie-Hellmann** 294
- Shannon** 11, 17
- Shannon-Grenze** 76, 77
- Shannon-Theorem** 73, 74, 75, 213
- SNR** 61, 65, 67

- Störabstand 61, 63, 65, 66, 67, 72, 76, 78
- Syndrom 58, 59, 83, 87, 111, 121, 123, 126, 129, 139, 161, 216
- Bestimmung 218
  - Polynom 111, 113, 148, 155, 156, 182
  - Spalten- 215
  - Stelle 86
  - Vektor 57, 59, 83, 84, 85, 194
  - Vektor und -Polynom 154
  - Zeilen- 215
- teilerfremd 42, 44, 171, 180, 270, 272, 284, 295, 302
- teilerfremde Polynome 43
- Teilschlüssel beim DES 260
- Vektor
- Element 202
- Verschlüsselung 1, 5, 9, 243, 247
- als Teil der Informationssicherung 10
  - mit festem Schlüssel 248
  - mit zufällig gewählten Schlüsseln 248
  - perfekte 10
  - XOR- 248
- Wavelet 20, 351, 361
- Baby- 362
  - Familien 361
  - Funktion 361
  - Koeffizienten 362
  - Mother- 362
  - Transformation 359
- Wiederholungscode 14, 48, 68
- Zerlegbarkeit
- eines Polynoms 99



# Weitere Titel aus dem Programm

Gunter Lepschies

## **E-Commerce und Hackerschutz**

Leitfaden für die Sicherheit elektronischer Zahlungssysteme

2., überarb. Aufl. 2000. VI, 242 S. mit 43 Abb. (DuD-Fachbeiträge) Br.

DM 98,00

ISBN 3-528-15702-X

E-Handel - Bedrohungen - Verschlüsselungsverfahren - digitale  
Signatur - Internetbanking - elektronische Kreditkartensysteme -  
Verrechnungssysteme - Scheckbasierte Systeme - Chipkartensysteme  
*„Wer Näheres zur Sicherheit von Cybercash, Chipkarten oder Inter-  
net-Banking wissen will, ist hier richtig.“ e-commerce magazin 3/99*

Helmut Bäumler (Hrsg.)

## **E-Privacy**

Datenschutz im Internet

2000. X, 331 S. (DuD-Fachbeiträge) Br. DM 69,00 ISBN 3-528-03921-3

Schutz der Privatsphäre - Internet-Governance - Neue Steuerungs-  
instrumente - Verschlüsselung - Identitätsmanagement - Zukunftsp-  
rospektiven für Demokratie und Grundrechte im Internet

Andreas Pfitzmann, Alexander Schill, Andreas Westfeld, Gritta Wolf

## **Mehrseitige Sicherheit in offenen Netzen**

Grundlagen, praktische Umsetzung

und in Java implementierte Demonstrations-Software

2000. X, 250 S. mit CD-ROM. (DuD-Fachbeiträge) Geb. DM 68,00

ISBN 3-528-05735-1

Mehrseitige Sicherheit - Sicherheitsarchitektur für verteilte Anwen-  
dungen - Konfigurierung von Schutzzielen und Sicherheitsmechanis-  
men - Aushandlung der Schutzinteressen - Prototyp in Java



Abraham-Lincoln-Straße 46  
65189 Wiesbaden  
Fax 0611.7878-400  
www.vieweg.de

Stand 1.10.2000  
Änderungen vorbehalten.  
Erhältlich im Buchhandel oder im Verlag.

# Weitere Titel aus dem Programm

Rainer Egewardt

## **Das PC-Wissen für IT-Berufe:**

### **Hardware, Betriebssysteme, Netzwerktechnik**

Kompaktes Praxiswissen für alle IT-Berufe in der Aus- und Weiterbildung, von der Hardware-Installation bis zum Netzwerkbetrieb inklusive Windows NT, Novell-Netware und Unix (Linux)  
2000. XVIII, 592 S. mit 285 Abb. Br. DM 69,80 ISBN 3-528-05739-4  
Micro-Prozessor-Technik - Funktion von PC-Komponenten - Installation von PC-Komponenten - Netzwerk-Technik - DOS - Windows NT4 - Novell Netware - Unix/Linux - Anhang: PIN-Belegungen aller Anschlüsse

Andreas Solymosi, Ulrich Grude

## **Grundkurs Algorithmen und Datenstrukturen**

Eine Einführung in die praktische Informatik mit Java  
2000. XII, 194 S. mit 83 Abb. u. Br. DM 39,80 ISBN 3-528-05743-2  
Begriffsbildung - Komplexität - Rekursion - Suchen - Sortierverfahren - Baumstrukturen - Ausgegliche Bäume - Algorithmenklassen

Hartmut Ernst

## **Grundlagen und Konzepte der Informatik**

Eine Einführung in die Informatik ausgehend von den fundamentalen Grundlagen  
2000. XIV, 822 S. mit 262 Abb. Br. DM 49,80 ISBN 3-528-05717-3  
Nachricht, Information und Codierung - Schaltalgebra, Schaltnetze und Elemente der Computer-Hardware - Rechnerarchitekturen und Betriebssysteme - Automatentheorie und Formale Sprachen - Programmiersprachen und Methodik der Programmierung - Berechenbarkeit und Komplexität - Algorithmen und Datenstrukturen



Abraham-Lincoln-Straße 46  
65189 Wiesbaden  
Fax 0611.7878-400  
www.vieweg.de

Stand 1.10.2000  
Änderungen vorbehalten.  
Erhältlich im Buchhandel oder im Verlag.