# 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 Kurzbeirag 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, Viewег-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

# 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 Internet-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 Steuerungsinstrumente - Verschlüsselung - Identitätsmangement - Zukunftsperspektiven 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 Anwendungen - Konfigurierung von Schutzzielen und Sicherheitsmechanismen - Aushandlung der Schutzinteressen - Prototyp in Java

vieweg

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 - Ausgeglichene 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

vieweg

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.