

Wilfried Dankmeier

**Codierung**

# DUD-Fachbeiträge

herausgegeben von Karl Rihaczek, Paul Schmitz, Herbert Meister

Lieferbare Titel der Reihe sind:

- |    |  |    |   |
|----|--|----|---|
| 2  | Einheitliche Höhere Kommunikationsprotokolle – Schicht 4<br>Hrsg.: Bundesministerium des Innern                  | 16 | <i>Gerhard Weck und Patrick Horster (Hrsg.)</i><br>Verlässliche Informationssysteme<br>Proceedings der GI-Fachtagung VIS'93 |
| 6  | <i>Karl Rihaczek</i><br>Datenverschlüsselung in Kommunikationssystemen   | 17 | <i>Hans-Albert Lennartz</i><br>Rechtliche Steuerung informationstechnischer Systeme   |
| 10 | <i>Hans-Albert Lennartz</i><br>Datenschutz und Wissenschaftsfreiheit   | 18 | <i>Georg Erwin Thaller</i><br>Computersicherheit  |
| 13 | <i>Ulrich Pordesch, Volker Hammer, Alexander Roßnagel</i><br>Prüfung des rechtsgemäßen Betriebs von ISDN-Anlagen | 19 | <i>Günther Cyranek, Kurt Bauknecht (Hrsg.)</i><br>Sicherheitsrisiko Informationstechnik                                     |
| 14 | <i>Hans-Jürgen Seelos</i><br>Informationssysteme und Datenschutz im Krankenhaus                                  | 20 | <i>Wilfried Dankmeier</i><br>Codierung  |
| 15 | <i>Heinzpeter Höller</i><br>Kommunikationssysteme – Normung und soziale Akzeptanz                                |    |   |

Wilfried Dankmeier

# Codierung

**Fehlerbeseitigung und  
Verschlüsselung**



Die Deutsche Bibliothek – CIP-Einheitsaufnahme

**Dankmeier, Wilfried:**

Codierung: Fehlerbeseitigung und Verschlüsselung /

Wilfried Dankmeier. – Braunschweig; Wiesbaden:

Vieweg, 1994

(DuD-Fachbeiträge; 20)

ISBN 978-3-322-92928-0

ISBN 978-3-322-92927-3 (eBook)

DOI 10.1007/978-3-322-92927-3

NE: GT

Das in diesem Buch enthaltene Programm-Material ist mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Der Autor, die Herausgeber und der Verlag übernehmen infolgedessen keine Verantwortung und werden keine daraus folgende oder sonstige Haftung übernehmen, die auf irgendeine Art aus der Benutzung dieses Programm-Materials oder Teilen davon entsteht.

Alle Rechte vorbehalten

© Springer Fachmedien Wiesbaden GmbH 1994

Ursprünglich erschienen bei Friedr. Vieweg & Sohn Verlagsgesellschaft mbH,

Braunschweig/Wiesbaden, 1994

Softcover reprint of the hardcover 1st edition 1994



Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

---

# Inhalt

<b>1 Einleitung</b>	1
<b>2 Aufgabenstellung und Ziel</b>	2
2.1 Beispiele für Codes	2
2.2 Einige Begriffe aus der Nachrichtentheorie	6
2.3 Aufgabenstellung	9
2.4 Ziel	16
<b>3 Hilfsmittel der Mathematik</b>	18
3.1 Grundlagen aus der allgemeinen Ingenieurmathematik	18
3.2 Weitere mathematische Hilfsmittel	22
<b>4 Datenfehlerbeseitigung</b>	37
4.1 Unmittelbare Ausnutzung des Hammingabstands	37
4.2 Hammingcode	39
4.2.1 Aufbau	39
4.2.2 Generatormatrix $G$	44
4.2.3 Paritätsprüfmatrix $H$	45
4.2.4 Syndrom	47
4.2.5 Technischer Gebrauch des Hammingcodes	49
4.3 Verallgemeinerung des Codierungsverfahrens von Hamming	50
4.3.1 Mehrfachfehler-Korrektur	51
4.3.2 Andere Ganzzahl-Basen	53
4.3.3 Erweiterung um zusätzliche Fehlererkennung	56
4.4 Zyklische Codes	61
4.4.1 Vorüberlegungen	61
4.4.2 Bildung der Codewörter	62
4.4.3 Das Generatorpolynom	70
4.4.3.1 Einige nützliche Eigenschaften von Polynomen	71
4.4.3.2 Kriterien für die Wahl des Generatorpolynoms	81
4.4.4 BCH-Code	83
4.4.5 Reed-Solomon-Code	106
4.4.6 Erkennung von Fehlerbündeln	118
4.4.7 Syndrompolynom, Meggitt-Decodierung, Fehlerfallen-Decodierung	128
4.4.8 Technische Verwirklichung von Verfahren mit zyklischen Codes	134

---

4.5 Goppacode . . . . .	138
4.5.1 Erzeugung der Codewörter . . . . .	138
4.5.2 Zwei Lösungswege für die Decodierung . . . . .	149
4.5.3 Der BCH-Code als Sonderfall des Goppa-Codes und ein schnelles Decodierverfahren . . . . .	163
4.6 Reed-Muller-Code . . . . .	174
4.7 Übersicht zu den verschiedenen Codes . . . . .	186
<b>5 Rückgekoppelte Schieberegister . . . . .</b>	<b>194</b>
5.1 Eigenschaften . . . . .	194
5.2 Fehlerbeseitigung bei verrauschten Nutzsignalen durch Kreuzkorrelation . . . . .	207
5.3 Zufallserzeugung von Schlüsselwörtern . . . . .	212
<b>6 Datenverschlüsselung . . . . .</b>	<b>225</b>
6.1 Datenverschlüsselung als Teilgebiet der Informationssicherung . . . . .	226
6.2 Verschlüsselung nach dem Data-Encryption- Standard (DES) . . . . .	228
6.3 Verschlüsselung mit dem RSA-Algorithmus . . . . .	240
6.4 Das Rechnen mit großen Ganzzahlen . . . . .	249
6.5 Erzeugung großer Pseudoprimzahlen . . . . .	252
6.6 Verschlüsselung mithilfe des Goppa-Codes (McEliece-Verfahren) . . . . .	257
6.7 Ansätze zur Suche nach Schwachstellen . . . . .	263
6.8 Verfahren zum Austausch von Schlüsseln (Diffie-Hellmann-Schlüsseltausch) . . . . .	265
6.9 Nachweis der Berechtigung (Benutzer-Authentikation) . . . . .	267
6.10 Nachweis der Unversehrtheit einer Nachricht (Nachrichtenintegrität, Hash-Summen) . . . . .	273
6.11 Nachweis der Absenderidentität (Nachrichten-Authentikation, digitale Unterschrift, DSA) . . .	279
<b>7 Literaturverzeichnis . . . . .</b>	<b>283</b>
<b>8 Sachwortverzeichnis . . . . .</b>	<b>285</b>