

# Inhaltsverzeichnis

<b>Vorwort</b>	<b>vii</b>
<b>Einleitung</b>	<b>1</b>
<b>I Codierungstheorie</b>	<b>3</b>
1 Grundbegriffe und Beispiele . . . . .	3
2 Lineare Codes . . . . .	15
3 Der CD-Spieler . . . . .	27
4 LDPC-Codes . . . . .	31
5 Duale Codes . . . . .	36
6 Gewichtspolynome und Decodierfehler . . . . .	42
7 Zyklische Codes . . . . .	47
8 Schranken und Lineare Optimierung . . . . .	53
9 Decodierung von BCH-Codes . . . . .	58
<b>II Kryptographie</b>	<b>65</b>
10 Grundbegriffe und Sicherheit . . . . .	65
11 Symmetrische Verfahren – die AES-Chiffrierung . . . . .	69
12 Public-Key-Kryptographie . . . . .	74
13 Signaturen . . . . .	81
14 Hash-Funktionen . . . . .	84
15 Elliptische Kurven . . . . .	87
16 Der Diskrete Logarithmus . . . . .	92
17 Der AKS-Algorithmus . . . . .	97
18 Wahrscheinlichkeitstheoretische Primzahltests . . . . .	104
19 Faktorisierung ganzer Zahlen . . . . .	109
<b>Anhang</b>	<b>117</b>
20 Gruppen . . . . .	117
21 Zahlen . . . . .	120
22 Körper . . . . .	124
23 Komplexität von Algorithmen . . . . .	130

<b>Lösungen ausgewählter Aufgaben</b>	133
<b>Literatur</b>	141
<b>Namenverzeichnis</b>	145
<b>Symbolverzeichnis</b>	147
<b>Stichwortverzeichnis</b>	149