

Inhaltsverzeichnis

Vorwort	vii
Einleitung	1
I Codierungstheorie	3
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
II Kryptographie	65
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
Anhang	117
20 Gruppen	117
21 Zahlen	120
22 Körper	124
23 Komplexität von Algorithmen	130

Lösungen ausgewählter Aufgaben	133
Literatur	141
Namenverzeichnis	145
Symbolverzeichnis	147
Stichwortverzeichnis	149