Inhaltsverzeichnis

1 Von Geheimschriften zu Kryptosystemen **9**
Geschichte und Grundbegriffe 10
Funktionen 15
Codierungen 19
Kryptosysteme 23
Zusammenfassung 33

2 Die Suche nach Sicherheit und modulares Rechnen **37**
Kryptoanalyse und der Begriff der Sicherheit 38
Modulare Addition 40
Algebraische Strukturen 46
Modulare Multiplikation 53
Monoide 54
Gruppen 58
Verallgemeinerungen vom Kryptosystem CAESAR 62
Zusammenfassung 76

3 Entwurf und Kryptoanalyse von monoalphabetischen Kryptosystemen **81**
Der Begriff der monoalphabetischen Kryptosysteme 81
Kryptoanalyse von monoalphabetischen Kryptosystemen 84
Verbesserung zu monoalphabetischen Kryptosystemen 90
Zusammenfassung 96

4 Polyalphabetische Kryptosysteme und deren Kryptoanalyse **101**
Das polyalphabetische Kryptosystem VIGENÈRE 101
Kryptoanalyse von VIGENÈRE 106
Statistische Kryptoanalyse von VIGENÈRE 112
Der Euklidische Algorithmus 130
Homophone Kryptosysteme 137
Zusammenfassung 140

5 Perfekte Sicherheit und das ONE-TIME-PAD-Kryptosytem **145**
Die Entwicklung des ONE-TIME-PAD-Kryptosystems 145
Das mathematische Konzept der perfekten Sicherheit 150

Sicherheitsgrad eines Kryptosystems 160
Zusammenfassung 166

6 Die ENIGMA und moderne Kryptosysteme 171
Die Geschichte der ENIGMA 172
Kryptographie im Zeitalter der Computer 182
Moderne Kryptosysteme 186
Zusammenfassung 189

7 Der geheime Schlüsselaustausch und das DIFFIE-HELLMAN-Protokoll 193
Schlüsselaustausch mit einer verschließbaren Truhe 194
Digitale Umsetzung des Schlüsselaustauschs 195
Modulares Potenzieren und die schnelle Exponentiation 201
Das DIFFIE-HELLMAN-Kommunikationsprotokoll 206
Zusammenfassung 211

8 Komplexitätstheoretische Konzepte und Sicherheit 215
Messung der Berechnungskomplexität von Algorithmen 218
Vergleich der Effizienz unterschiedlicher Algorithmen 221
Zeitkomplexität von algorithmischen Problemen 225
Beispiele von schweren Problemen 226
Zusammenfassung 240

9 Das Konzept der Public-Key-Kryptographie 245
Eine schwer berechenbare Grapheigenschaft als Geheimnis 251
Das Untersummen-Problem als Grundlage für ein Public-Key-Kryptosystem . 267
Ein Public-Key-Kryptosystem zum Verschicken eines Bits 284
Zusammenfassung 289

10 Zahlentheoretische Public-Key-Kryptosysteme und RSA 297
Das Public-Key-Kryptosystem RABIN 298
Korrektheit und Effizienz von RABIN 306
Sicherheit von RABIN 323
Effizienter Aufbau des Kryptosystems RABIN 325
Das Public-Key-Kryptosystem RSA 326
Korrektheit von RSA 328
Zusammenfassung 331

11 Anwendungen der Public-Key-Kryptographie und Protokolle 337
Digitale Unterschrift von Dokumenten 338
Vergessliche Übertragung oder Münzwurf über das Telefon 340
Vergleich von zwei geheimen Zahlen 345

Zero-Knowledge-Beweissysteme 348
Teilen von Geheimnissen 358
Zusammenfassung 362

A Lösungen zu ausgewählten Aufgaben 367