

# Inhaltsverzeichnis

<b>Vorwort</b>	<b>17</b>
<b>Kapitel 1 Einleitung</b>	<b>19</b>
1.1 Idee dieses Buches .....	20
1.2 Beispiele, Übungen und Rätsel .....	21
1.3 Begleitmaterial zu diesem Buch .....	22
1.4 Danksagung .....	23
1.5 Hinweis in eigener Sache .....	23
<b>Teil I Einführung in die Informatik</b>	<b>25</b>
<b>Kapitel 2 Die Historie und die Teilgebiete der Informatik</b>	<b>27</b>
2.1 <b>Rätsel:</b> Streichholzprobleme .....	28
2.2 Der Begriff Informatik .....	28
2.3 Historische Entwicklung der Informatik .....	28
2.3.1 Der Abakus .....	28
2.3.2 Der Begriff Algorithmus und Ibn Musa Al-Chwarismi .....	31
2.3.3 Wichtige Stationen von 1500 bis 1930 .....	32
2.3.4 Konrad Zuse und der erste funktionstüchtige Computer .....	34
2.3.5 Howard H. Aiken und die Mark I .....	36
2.3.6 John von Neumann .....	36
2.3.7 Generationen der elektronischen Datenverarbeitung .....	37
2.4 Einordnung und Einteilung der Informatik .....	41
2.4.1 Verschiedene Einsatzgebiete von Computern (Informatik) .....	41
2.4.2 Die Teilgebiete der Informatik .....	42
2.4.3 Die Informatik und unsere Abhängigkeit von ihr .....	45
<b>Kapitel 3 Speicherung und Interpretation von Information</b>	<b>47</b>
3.1 <b>Rätsel:</b> Umfüllprobleme .....	48
3.2 Unterschiedliche Zahlensysteme .....	48
3.2.1 Das römische Zahlensystem .....	48
3.2.2 Positionssysteme .....	49
3.2.3 Positionssysteme bei natürlichen Zahlen .....	50
3.2.4 Positionssysteme bei gebrochenen Zahlen .....	55
3.3 Dual-, Oktal- und Hexadezimalsystem .....	56
3.3.1 Das Dualsystem und das Bit im Rechner .....	56
3.3.2 Konvertieren zwischen Dual- und Oktalsystem .....	57
3.3.3 Konvertieren zwischen Dual- und Hexadezimalsystem .....	57
3.4 Konvertierungsalgorithmen .....	59

3.4.1	Konvertieren von anderen Systemen in das Dezimalsystem .....	59
3.4.2	Konvertieren vom Dezimalsystem in andere Positionssysteme ...	59
3.4.3	Konvertieren echt gebrochener Zahlen .....	60
3.4.4	Konvertieren unecht gebrochener Zahlen .....	62
3.5	Rechenoperationen im Dualsystem .....	62
3.5.1	Addition .....	62
3.5.2	Subtraktion und Darstellung negativer Zahlen .....	63
3.5.3	Multiplikation und Division .....	67
3.5.4	Konvertieren durch sukzessive Multiplikation und Addition ...	67
3.6	Reelle Zahlen .....	68
3.6.1	Festpunktzahlen .....	68
3.6.2	Gleitpunktzahlen und das IEEE-Format .....	68
3.7	Codes zur Darstellung von Zeichen .....	71
3.7.1	ASCII-Code .....	71
3.7.2	Unicode .....	74
3.8	Weitere Codes für Zahlen und Zeichen .....	75
3.8.1	BCD-Code für Zahlen .....	75
3.8.2	Gray-Code .....	76
3.8.3	Barcode .....	77
3.9	Duale Größenangaben .....	77
3.10	Die Grunddatentypen in der Programmiersprache C/C++ .....	78

## **Kapitel 4    Boole'sche Algebra** **81**

4.1	<b>Rätsel:</b> Analytische Rätsel (1) .....	82
4.2	George Boole und seine Algebra mit nur zwei Werten .....	82
4.3	Operatoren .....	83
4.4	Boole'sche Schaltungen .....	85
4.5	Boole'sche Rechenregeln .....	85
4.6	Funktionen .....	87

## **Kapitel 5    Hardwarekomponenten eines Computers** **91**

5.1	<b>Rätsel:</b> Analytische Rätsel (2) .....	92
5.2	Aufbau von Computersystemen .....	92
5.2.1	Zentraleinheit und Peripheriegeräte .....	92
5.2.2	EVA und das von-Neumann'sche-Rechnermodell .....	94
5.3	Die heutigen Personal Computer (PCs) .....	95
5.4	Die Zentraleinheit .....	96
5.4.1	Der Prozessor .....	97
5.4.2	Der Arbeitsspeicher .....	108
5.4.3	ROMs zur Speicherung von Programmen und konstanten Daten .	110
5.4.4	Das BIOS .....	112
5.4.5	Busse und Schnittstellen (Anschlüsse) .....	113
5.5	Die Peripherie .....	118
5.5.1	Massenspeicher .....	118

5.5.2	Eingabegeräte .....	123
5.5.3	Ausgabegeräte .....	125
5.6	Modell eines einfachen Prozessorsystems .....	129
5.7	Alternative Rechnerarchitekturen (Neuronale Netze) .....	134

## **Kapitel 6 Vom Programm zum Maschinenprogramm 135**

6.1	<b>Rätsel:</b> Analytische Rätsel (3) .....	136
6.2	Entwicklung eines Programms .....	136
6.3	Programmierwerkzeuge .....	137
6.3.1	Unterschiedliche Arten der Übersetzung .....	137
6.3.2	Der Compiler .....	138
6.3.3	Der Linker .....	139
6.3.4	Der Lader (und Locator) .....	141
6.3.5	Der Debugger .....	142

## **Teil II Praktische Informatik 145**

### **Kapitel 7 Programmiersprachen 147**

7.1	<b>Rätsel:</b> Analytische Rätsel (4) .....	148
7.2	Höhere Programmiersprachen .....	148
7.3	Grundlagen der Programmierung .....	151
7.3.1	Spezifikation einer Aufgabenstellung .....	151
7.3.2	Der Begriff Algorithmus .....	152
7.3.3	Formulierung und Darstellung eines Algorithmus .....	152
7.3.4	Programm = Daten + Algorithmus .....	154
7.4	Datentypen und Operatoren in C/C++ und Java .....	160
7.4.1	Datentypen und Konstanten .....	160
7.4.2	Bezeichner .....	162
7.4.3	Grundlegende Operatoren .....	162
7.4.4	Die logischen Operatoren &&,    und ! .....	163
7.4.5	Die Shift-Operatoren << und >> .....	163
7.4.6	Die Postfix- und Präfixoperatoren ++ und -- .....	164
7.4.7	Die Bit-Operatoren &,  , ^ und ~ .....	165
7.4.8	Prioritäten und Assoziativitäten der Operatoren .....	166
7.5	Formulierung von Algorithmen in C/C++ und Java .....	168
7.5.1	Sequenz .....	168
7.5.2	Verzweigungen mit if .....	168
7.5.3	Verzweigungen mit switch .....	174
7.5.4	for-Schleife (Schleife mit der Abfrage am Anfang) .....	175
7.5.5	while-Schleife (Schleife mit der Abfrage am Anfang) .....	182
7.5.6	do... while-Schleife (Schleife mit der Abfrage am Ende) .....	185
7.5.7	Abbruch von Schleifen mit break .....	186
7.5.8	Abbruch eines einzelnen Schleifendurchlaufs mit continue .....	188
7.5.9	Abbruch mehrerer geschachtelter Schleifen mit goto .....	188

7.5.10	Programmabbruch mit exit .....	189
7.5.11	Allgemeines zu Funktionen bzw. Methoden .....	189
7.5.12	Rekursive Funktionen bzw. rekursive Methoden .....	199
7.5.13	Arrays .....	208
7.5.14	Strings .....	213
7.5.15	Zufallszahlen .....	216
7.5.16	Argumente auf der Kommandozeile .....	218
7.5.17	Ausnahmen (Exceptions) in Java .....	219
7.5.18	Dateien .....	220
7.5.19	Strukturen in C/C++ .....	229
7.6	Objektorientierte Programmierung mit Java .....	231
7.6.1	Meilensteine in der Softwareentwicklung .....	231
7.6.2	Einführung in die Objektorientierung .....	239
7.6.3	Klassen und Objekte .....	246
7.6.4	Konstruktoren .....	252
7.6.5	Vererbung und Polymorphismus .....	253
7.6.6	GUI-Programmierung in Java .....	262
7.7	Portable GUI-Programmierung mit Qt .....	274
7.7.1	Allgemeines zu Qt .....	274
7.7.2	Grundlegende Konzepte und Konstrukte von Qt .....	276
7.7.3	Das Signal-Slot-Konzept von Qt .....	279
7.8	Programmierung paralleler Abläufe (Parallel-Programmierung) .....	287
7.8.1	Konzepte und HW-Architekturen für parallele Abläufe .....	288
7.8.2	SW-Konzepte und Erstellung paralleler Programme .....	290
7.8.3	Parallele Programmierung mit Threads .....	293
7.8.4	Parallele Programmierung mit openMP .....	299
7.8.5	Besondere Probleme bei paralleler Bearbeitung .....	312
7.8.6	Ausblick .....	323
7.9	Funktionale Programmierung (Scala, F#) .....	325
<b>Kapitel 8 Datenstrukturen und Algorithmen</b>		<b>329</b>
8.1	<b>Rätsel:</b> Analytische Rätsel (5) .....	330
8.2	Grundlegende Datenstrukturen .....	331
8.2.1	Allgemeine Eigenschaften von Daten .....	331
8.2.2	Basis-Datentypen .....	331
8.2.3	Datenstruktur = Daten + Operationen .....	331
8.2.4	Verkettete Listen .....	332
8.2.5	Binäre Suche in einfach verketteten Listen (Skiplisten) .....	345
8.2.6	Stack (Stapel) .....	348
8.2.7	Queue (Warteschlange) .....	356
8.3	Bäume .....	361
8.3.1	Grundlegendes zu Bäumen .....	361
8.3.2	Binäre Bäume .....	363
8.3.3	Sich selbst balancierende Binärbäume .....	378
8.3.4	Splay-Bäume .....	380
8.3.5	B-Bäume .....	380

8.3.6	Baumrekursion bei Bäumen mit mehr als zwei Zweigen .....	382
8.4	Komplexität von Algorithmen und O-Notation .....	393
8.4.1	Zeitaufwand .....	393
8.4.2	Speicherplatzbedarf .....	396
8.4.3	Klassifikation von Algorithmen .....	397
8.4.4	Die O-Notation .....	399
8.4.5	Wahl eines Algorithmus .....	404
8.4.6	Einfache Optimierungen bei der Implementierung .....	406
8.5	Elementare Sortieralgorithmen .....	409
8.5.1	Grundsätzliches zu Sortieralgorithmen .....	409
8.5.2	Bubble-Sort .....	410
8.5.3	Insert-Sort .....	412
8.5.4	Select-Sort .....	413
8.5.5	Zeitmessungen für Bubble-, Insert- und Select-Sort .....	414
8.5.6	Distribution Count-Sort (Bucket-Sort) .....	415
8.6	Shell-Sort .....	418
8.7	Quicksort .....	420
8.8	Mergesort .....	422
8.8.1	Rekursiver Mergesort für Arrays .....	422
8.8.2	Nicht-rekursiver Mergesort für Arrays .....	424
8.8.3	Analyse des Mergesort .....	425
8.8.4	Mischen von zwei sortierten Arrays .....	425
8.9	Backtracking .....	426
8.9.1	Finden in einem Labyrinth .....	426
8.9.2	Das Achtdamen-Problem .....	428
8.9.3	Rekursives Füllen von Figuren .....	430
8.9.4	Sudoku .....	430
8.9.5	Branch-and-Bound-Verfahren .....	431
<b>Kapitel 9 Betriebssysteme</b>		<b>433</b>
9.1	<b>Rätsel:</b> Überquerung einer Hängebrücke .....	434
9.2	Der Begriff Betriebssystem .....	434
9.3	Die Geschichte von Betriebssystemen .....	434
9.4	Grundaufgaben von Betriebssystemen .....	437
9.5	Aufbau und Dienste von Betriebssystemen .....	438
9.5.1	Schichtenaufbau .....	439
9.5.2	Prozesse, Threads, Scheduling .....	440
9.5.3	Synchronisationsmechanismen .....	443
9.5.4	Zeitdienste (Timer) .....	446
9.5.5	Speicherverwaltung .....	448
9.5.6	Dateiverwaltung und Dateisysteme .....	449
9.5.7	Geräteverwaltung und Treiber .....	452
9.5.8	Benutzerschnittstelle (Kommandozeile bzw. GUI) .....	454
9.5.9	Programmierschnittstelle (API) .....	456
9.6	Besonderheiten bei Embedded Systems .....	459

<b>Kapitel 10</b>	<b>Rechnernetze und das Internet</b>	<b>463</b>
10.1	<b>Rätsel:</b> Synthetische Rätsel (1) .....	464
10.2	Grundlagen der Vernetzung von Rechnern .....	464
10.3	Das ISO/OSI-Modell und Internet-Protokolle .....	465
10.4	Internet-Protokolle in Rechnernetzen .....	467
	10.4.1 Grundbegriffe zu TCP/IP-Netzen .....	467
	10.4.2 TCP/IP-Protokolle .....	470
10.5	Hubs, Switches, Router und Gateways .....	475
10.6	Grundlagen der Socket-Programmierung .....	475
10.7	Verteilte Anwendungen .....	475
10.8	Das World Wide Web (WWW) .....	477
	10.8.1 Wichtige Komponenten und Konzepte des WWW .....	477
	10.8.2 Kurze Einführung in HTML .....	480
	10.8.3 Kurze Einführung in CSS .....	491
	10.8.4 Eine kurze Einführung in XML .....	496
	10.8.5 Client-seitige Web-Programmierung .....	500
	10.8.6 Server-seitige Web-Programmierung .....	506
10.9	Gefahren durch Software .....	507
	10.9.1 Arten von Schadsoftware .....	508
	10.9.2 Pufferüberläufe (Buffer Overflows) .....	511
<b>Kapitel 11</b>	<b>Datenbanksysteme</b>	<b>519</b>
11.1	<b>Rätsel:</b> Synthetische Rätsel (2) .....	520
11.2	Grundlegendes zu Datenbanksystemen .....	520
	11.2.1 Aufgaben einer Datenbank .....	520
	11.2.2 Vorteile von Datenbanken .....	521
	11.2.3 Datenunabhängigkeit .....	522
11.3	Datenmodelle .....	523
	11.3.1 Das Entity-Relationship-Modell .....	523
	11.3.2 Das relationale Datenmodell .....	524
	11.3.3 Die relationale Algebra .....	526
11.4	Die Datenbanksprache SQL .....	527
	11.4.1 Datendefinition .....	528
	11.4.2 Einfügen, Ändern und Löschen von Datensätzen .....	529
	11.4.3 Anfragen mit select .....	530
<b>Kapitel 12</b>	<b>Software Engineering</b>	<b>533</b>
12.1	<b>Rätsel:</b> Synthetische Rätsel (3) .....	534
12.2	Die Software-Krise .....	534
12.3	Eine geeignete Software-Architektur .....	536
12.4	UML-Diagramme für die Modellierung .....	536
	12.4.1 Statische Modellierung in UML .....	537
	12.4.2 Dynamische Modellierung in UML .....	539
12.5	Modellierungsmöglichkeiten für die Software .....	541
12.6	Notwendigkeit von Prozessen .....	541

12.7	Der wichtige Prozess „Requirement Engineering“ .....	542
12.7.1	Das UML-Anwendungsfalldiagramm (Use Case Diagram) .....	543
12.7.2	Das UML-Aktivitätsdiagramm .....	544
12.7.3	Genauere Klärung der Kundenanforderungen .....	546
12.8	Prozessmodelle .....	547
12.8.1	Schwer- und leichtgewichtige Prozessmodelle .....	547
12.8.2	Das Wasserfall-Modell .....	547
12.8.3	Das V-Modell .....	549
12.8.4	Inkrementelle und iterative Prozessmodelle .....	550
12.8.5	Agiles Vorgehen mit eXtreme Programming (XP) .....	552
12.9	Qualität eines Software-Produktes aus Kundensicht .....	554

## **Teil III Technische Informatik 557**

### **Kapitel 13 Transistoren, Chips und logische Bausteine 559**

13.1	<b>Rätsel:</b> Synthetische Rätsel (4) .....	560
13.2	Transistoren .....	560
13.2.1	Funktionsweise und Aufbau von Transistoren .....	560
13.2.2	Realisierung boolescher Funktionen mit Transistoren .....	562
13.3	Chips .....	563
13.3.1	Geschichtliche Entwicklung .....	563
13.3.2	Herstellungsprozess .....	564
13.4	Logische Bausteine .....	565
13.4.1	Gatter .....	565
13.4.2	Decoder .....	566
13.4.3	Encoder .....	567
13.4.4	Multiplexer (Selektor) .....	567
13.4.5	Demultiplexer .....	570

### **Kapitel 14 Schaltnetze 573**

14.1	<b>Rätsel:</b> Ein dialektisches Rätsel .....	574
14.2	Normalformen von Schaltfunktionen .....	574
14.2.1	Disjunktive Normalform (DNF) .....	574
14.2.2	Konjunktive Normalform (KNF) .....	575
14.2.3	Allgemeines Verfahren beim Erstellen einer Schaltung .....	576
14.2.4	Schaltkreisrealisierung durch PLAs .....	577
14.3	Entwurf von Schaltnetzen .....	580
14.4	Minimierung logischer Ausdrücke .....	581
14.4.1	Karnaugh-Veitch-Diagramme (KV-Diagramme) .....	581
14.4.2	Don't Care Argumente .....	585
14.4.3	Quine-McCluskey-Verfahren .....	588
14.5	Addiernetze .....	594
14.5.1	Paralleladdierer .....	594
14.5.2	Paralleladdierer und -subtrahierer .....	596

14.5.3	Carry-Select-Addiernetze .....	597
14.5.4	Carry-Save-Addiernetze .....	599
14.5.5	Multiplizierer .....	600
14.6	Prinzipieller Aufbau einer ALU .....	602

## **Kapitel 15 Schaltwerke 605**

15.1	<b>Rätsel:</b> Waldlauf, Schnapsgläser und mehr .....	606
15.2	Synchrone und asynchrone Schaltwerke .....	607
15.3	Schaltungen mit Delays .....	608
15.3.1	4-Bit-Ringzähler als synchrones Schaltwerk .....	608
15.3.2	Delays .....	609
15.3.3	Realisierung von Delays mit Flipflops .....	611
15.4	Zähler und Frequenzteiler .....	619
15.4.1	Synchroner 4-Bit-Ringzähler mit JK-Flipflops .....	619
15.4.2	Asynchroner 4-Bit-Ringzähler mit T-Flipflops .....	621
15.4.3	Synchroner BCD-Zähler (Mod-10) mit T-Flipflops .....	622
15.4.4	Asynchroner BCD-Zähler (Mod-10) mit JK-Flipflops .....	622
15.5	Schieberegister .....	623
15.6	Entwurf synchroner Schaltwerke mittels Automaten .....	625
15.6.1	Kurze Einführung in die Automatentheorie .....	625
15.6.2	Entwurf von Schaltwerken mit Moore- und Mealy-Automaten ...	628

## **Kapitel 16 Prozessorarchitekturen, Speicher und Caches 639**

16.1	<b>Rätsel:</b> Schachbrett-Quadrate, Flickermuster, Kreuzformfirma .....	640
16.2	CISC und RISC .....	641
16.3	Pipelining (Fließbandverarbeitung) .....	643
16.3.1	Unterschiedliche Phasen beim Pipelining .....	643
16.3.2	Geschwindigkeitsgewinn beim Pipelining .....	645
16.3.3	Hazards beim Pipelining .....	647
16.4	Speicher für Prozessoren .....	650
16.5	Caches .....	653
16.5.1	Das Lokalitätsprinzip und der Cache-Controller .....	654
16.5.2	Der Lesezugriff .....	655
16.5.3	Vollasoziative und direktabgebildete Caches .....	657
16.5.4	Der Schreibzugriff .....	660
16.6	Virtueller Speicher .....	662
16.6.1	Paging .....	663
16.6.2	Segmentierung .....	665



<b>Kapitel 17</b>	<b>Automatentheorie und formale Sprachen</b>	<b>669</b>
17.1	<b>Rätsel:</b> Weg durch ein Labyrinth und um die Ecke gedacht .....	670
17.2	Lexikalische und syntaktische Analyse .....	670
17.3	Reguläre Sprachen und endliche Automaten .....	672
17.3.1	Alphabet, Wort und Sprache .....	672
17.3.2	Reguläre Ausdrücke .....	673
17.3.3	Endliche Automaten und reguläre Sprachen .....	675
17.3.4	Realisierung endlicher Automaten .....	677
17.3.5	lex – Ein Werkzeug für die lexikalische Analyse .....	678
17.4	Kontextfreie Sprachen und Kellerautomaten .....	682
17.4.1	Kontextfreie Grammatiken .....	682
17.4.2	Kellerautomaten .....	685
17.4.3	yacc – Ein Werkzeug für die Syntaxanalyse .....	688
17.4.4	lex und yacc im Zusammenspiel .....	692
17.4.5	Rekursion bei der Syntaxanalyse .....	693
17.5	Die unterschiedlichen Phasen eines Compilers .....	693
<b>Kapitel 18</b>	<b>Berechenbarkeitstheorie</b>	<b>697</b>
18.1	<b>Rätsel:</b> Kneipen, Ei, stehen gebliebene Uhr und Alter .....	698
18.2	Berechenbare Funktionen .....	699
18.3	Nicht berechenbare Funktionen .....	700
18.3.1	Das Diagonalverfahren von Cantor .....	700
18.3.2	Nicht durch einen Algorithmus berechenbare Funktionen .....	701
18.3.3	Die Church'sche Algorithmus-Definition .....	701
18.4	Berechenbarkeitskonzepte .....	702
18.4.1	Turingmaschinen .....	702
18.4.2	Turing-berechenbare Funktionen .....	705
18.4.3	Registermaschinen .....	705
18.4.4	GOTO- und WHILE-Programme .....	706
18.4.5	LOOP-Programme (FOR-Programme) .....	708
18.4.6	Primitive Rekursion .....	709
18.4.7	$\mu$ -Rekursion .....	712
18.4.8	Die Ackermann-Funktion .....	713
18.4.9	Die Church'sche These und die Chomsky-Hierarchie .....	715
18.5	Prinzipiell unlösbare Probleme .....	716
18.5.1	Entscheidbare Mengen .....	716
18.5.2	semi-entscheidbare Mengen (Game of Life und Halteproblem) ...	717
18.5.3	Unberechenbarkeit (Fleißiger Biber) .....	721
<b>Kapitel 19</b>	<b>Komplexitätstheorie</b>	<b>725</b>
19.1	<b>Rätsel:</b> Falsche Uhrzeit, Kalenderrechnen und mehr .....	726
19.2	Die Klasse P für praktisch lösbare Probleme .....	726

19.3	Nichtdeterminismus und die Klasse NP .....	727
19.3.1	Das SAT-Problem als erstes NP-Problem .....	727
19.3.2	Reduzierung auf ja/nein-Probleme mit zugehörigen Sprachen ...	728
19.3.3	Nichtdeterminismus .....	728
19.3.4	Die Klasse NP .....	729
19.4	Der Satz von Cook und NP-Vollständigkeit .....	731
19.4.1	Das Dreifarbenproblem als Spezialfall des SAT-Problems .....	731
19.4.2	NP-Vollständigkeit .....	732
19.4.3	$P = NP?$ .....	733
19.4.4	Das 3SAT-Problem .....	733
19.4.5	Das Cliquesproblem .....	734
19.4.6	Das Rucksack- und Teilsummen-Problem .....	736
19.4.7	Das Hamilton-Problem .....	741
19.4.8	Das Problem des Handlungsreisenden .....	741
19.4.9	Hierarchie der NP-vollständigen Probleme .....	744
19.5	Approximationsalgorithmen .....	744

## Teil V      Codes, Kompression, Kryptografie      749

### Kapitel 20    Fehlertolerante Codes      751

20.1	<b>Rätsel:</b> Auf der Demo mit Bruder und Schwester .....	752
20.2	Motivation für fehlertolerante Codes .....	752
20.3	„k aus n“-Codes .....	752
20.4	Der Hammingabstand eines Codes .....	753
20.5	Eindimensionale Parity-Prüfung .....	755
20.6	Zweidimensionale Parity-Prüfung .....	756
20.7	Hamming-Codes .....	761
20.8	CRC-Kodierung .....	763

### Kapitel 21    Datenkompression      767

21.1	<b>Rätsel:</b> Tierseuche .....	768
21.2	Verlustbehaftete und verlustlose Kompression .....	768
21.3	Codes mit variabel langen Codewörtern .....	768
21.4	Fano-Bedingung für Dekodierbarkeit eines Codes .....	769
21.5	Laufänglenkodierung („run-length encoding“) .....	770
21.6	Shannon-Fano-Kodierung .....	771
21.7	Huffman-Kodierung .....	771
21.8	Arithmetische Kodierung .....	775
21.9	Lempel-Ziv-Kodierungen .....	778
21.9.1	Der LZ77-Algorithmus .....	780
21.9.2	Der LZSS-Algorithmus .....	781
21.9.3	Der LZ78-Algorithmus .....	782
21.9.4	Der LZW-Algorithmus .....	783

21.9.5	Varianten der Lempel-Ziv-Kodierung .....	787
<b>Kapitel 22</b>	<b>Kryptografie</b>	<b>789</b>
22.1	<b>Rätsel:</b> Weinflasche und Erben von Weinfässern .....	790
22.2	Allgemeines zu Kryptosystemen .....	790
22.3	Einfache Verschlüsselungsmethoden .....	790
22.3.1	Cäsar-Chiffre .....	790
22.3.2	Chiffre mit eigener Zuordnungstabelle .....	791
22.4	Vigenère-Verschlüsselungsmethoden .....	791
22.5	Verschlüsselung mittels Zufallsfolgen .....	792
22.6	Kryptosysteme mit öffentlichen Schlüsseln .....	794
22.6.1	Eigenschaften von Public-Key-Systemen .....	794
22.6.2	Der Satz von Euler .....	795
22.6.3	Schlüsselerzeugung beim RSA-Algorithmus .....	796
22.6.4	Ver- und Entschlüsselung mit dem RSA-Algorithmus .....	798
	<b>Weiterführende Literatur</b>	<b>801</b>
	<b>Sachregister</b>	<b>807</b>