

# 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> Umläpprobleme .....	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

<b>Kapitel 4</b>	<b>Boole'sche Algebra</b>	<b>81</b>
4.1	Rätsel: 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

<b>Kapitel 5</b>	<b>Hardware-Komponenten eines Computers</b>	<b>91</b>
5.1	Rätsel: 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 .....	93
5.3	Die heutigen Personal Computer (PCs) .....	95
5.4	Die Zentraleinheit .....	95
5.4.1	Der Prozessor .....	97
5.4.2	Der Arbeitsspeicher .....	107
5.4.3	ROMs zur Speicherung von Programmen und konstanten Daten ..	109
5.4.4	Das BIOS .....	111
5.4.5	Busse und Schnittstellen (Anschlüsse) .....	111
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 .....	128
5.7	Alternative Rechnerarchitekturen (Neuronale Netze) .....	133

## Kapitel 6 Vom Programm zum Maschinenprogramm 135

6.1	Rätsel: 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	Rätsel: 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 .....	309
7.8.6	Ausblick .....	317
7.9	Funktionale Programmierung (Scala, F#) .....	320

<b>Kapitel 8</b>	<b>Datenstrukturen und Algorithmen</b>	<b>323</b>
8.1	Rätsel: Analytische Rätsel (5) .....	324
8.2	Grundlegende Datenstrukturen .....	325
8.2.1	Allgemeine Eigenschaften von Daten .....	325
8.2.2	Basis-Datentypen .....	325
8.2.3	Datenstruktur = Daten + Operationen .....	325
8.2.4	Verkettete Listen .....	326
8.2.5	Stack (Stapel) .....	339
8.2.6	Queue (Warteschlange) .....	347
8.3	Bäume .....	352
8.3.1	Grundlegendes zu Bäumen .....	352
8.3.2	Binäre Bäume .....	354
8.3.3	Baumrekursion bei Bäumen mit mehr als zwei Zweigen .....	369
8.4	Komplexität von Algorithmen und O-Notation .....	380
8.4.1	Zeitaufwand .....	380
8.4.2	Speicherplatzbedarf .....	383

8.4.3	Klassifikation von Algorithmen .....	384
8.4.4	Die O-Notation .....	386
8.4.5	Wahl eines Algorithmus .....	391
8.4.6	Einfache Optimierungen bei der Implementierung .....	393
8.5	Elementare Sortieralgorithmen .....	396
8.5.1	Grundsätzliches zu Sortieralgorithmen .....	396
8.5.2	Bubble-Sort .....	397
8.5.3	Insert-Sort .....	399
8.5.4	Select-Sort .....	400
8.5.5	Zeitmessungen für Bubble-, Insert- und Select-Sort .....	401
8.5.6	Distribution Count-Sort (Bucket-Sort) .....	402
8.6	Shell-Sort .....	405
8.7	Quicksort .....	407
8.8	Mergesort .....	409
8.8.1	Rekursiver Mergesort für Arrays .....	409
8.8.2	Nicht-rekursiver Mergesort für Arrays .....	411
8.8.3	Analyse des Mergesort .....	412
8.8.4	Mischen von zwei sortierten Arrays .....	412
8.9	Backtracking .....	413
8.9.1	Finden in einem Labyrinth .....	413
8.9.2	Das Achtdamen-Problem .....	415
8.9.3	Rekursives Füllen von Figuren .....	417
8.9.4	Sudoku .....	417
8.9.5	Branch-and-Bound-Verfahren .....	418
<b>9</b>	<b>Kapitel 9 Betriebssysteme</b>	<b>419</b>
9.1	Rätsel: Überquerung einer Hängebrücke .....	420
9.2	Der Begriff Betriebssystem .....	420
9.3	Die Geschichte von Betriebssystemen .....	420
9.4	Grundaufgaben von Betriebssystemen .....	423
9.5	Aufbau und Dienste von Betriebssystemen .....	424
9.5.1	Schichtenaufbau .....	425
9.5.2	Prozesse, Threads, Scheduling .....	426
9.5.3	Synchronisations-Mechanismen .....	429
9.5.4	Zeitdienste (Timer) .....	432
9.5.5	Speicherverwaltung .....	434
9.5.6	Dateiverwaltung und Dateisysteme .....	435
9.5.7	Geräteverwaltung und Treiber .....	438
9.5.8	Benutzerschnittstelle (Kommandozeile bzw. GUI) .....	440
9.5.9	Programmierschnittstelle (API) .....	442
9.6	Besonderheiten bei Embedded Systemen .....	445
<b>10</b>	<b>Kapitel 10 Rechnernetze und das Internet</b>	<b>449</b>
10.1	Rätsel: Synthetische Rätsel (1) .....	450
10.2	Grundlagen der Vernetzung von Rechnern .....	450
10.3	Das ISO/OSI-Modell und Internet-Protokolle .....	451

10.4	Internet-Protokolle in Rechnernetzen .....	453
10.4.1	Grundbegriffe zu TCP/IP-Netzen .....	453
10.4.2	TCP/IP-Protokolle .....	456
10.5	Hubs, Switches, Router und Gateways .....	461
10.6	Grundlagen der Socket-Programmierung .....	461
10.7	Verteilte Anwendungen .....	461
10.8	Das World Wide Web (WWW) .....	463
10.8.1	Wichtige Komponenten und Konzepte des WWW .....	463
10.8.2	Kurze Einführung in HTML .....	465
10.8.3	Cascading Style Sheets (CSS) .....	478
10.8.4	Eine kurze Einführung in XML .....	480
10.8.5	XHTML – das neue, XML-basierte HTML .....	483
10.8.6	Web-Programmierung .....	483
10.9	Gefahren durch Software .....	490
10.9.1	Arten von Schadsoftware .....	490
10.9.2	Pufferüberläufe (Buffer Overflows) .....	493

## Kapitel 11 Datenbanksysteme 501

11.1	Rätsel: Synthetische Rätsel (2) .....	502
11.2	Grundlegendes zu Datenbanksystemen .....	502
11.2.1	Aufgaben einer Datenbank .....	502
11.2.2	Vorteile von Datenbanken .....	503
11.2.3	Datenunabhängigkeit .....	504
11.3	Datenmodelle .....	505
11.3.1	Das Entity-Relationship-Modell .....	505
11.3.2	Das relationale Datenmodell .....	506
11.3.3	Die relationale Algebra .....	508
11.4	Die Datenbanksprache SQL .....	509
11.4.1	Datendefinition .....	510
11.4.2	Einfügen, Ändern und Löschen von Datensätzen .....	511
11.4.3	Anfragen mit select .....	512

## Kapitel 12 Software Engineering 515

12.1	Rätsel: Synthetische Rätsel (3) .....	516
12.2	Die Software-Krise .....	516
12.3	Eine geeignete Software-Architektur .....	518
12.4	UML-Diagramme für die Modellierung .....	518
12.4.1	Statische Modellierung in UML .....	519
12.4.2	Dynamische Modellierung in UML .....	521
12.5	Modellierungsmöglichkeiten für die Software .....	523
12.6	Notwendigkeit von Prozessen .....	523
12.7	Der wichtige Prozess „Requirement Engineering“ .....	524
12.7.1	Das UML-Anwendungsfalldiagramm (Use Case Diagram) .....	525
12.7.2	Das UML-Aktivitätsdiagramm .....	526
12.7.3	Genaue Klärung der Kundenanforderungen .....	528

12.8	Prozessmodelle .....	529
12.8.1	Schwer- und leichtgewichtige Prozessmodelle .....	529
12.8.2	Das Wasserfall-Modell .....	529
12.8.3	Das V-Modell .....	531
12.8.4	Inkrementelle und iterative Prozessmodelle .....	532
12.8.5	Agiles Vorgehen mit eXtreme Programming (XP) .....	534
12.9	Qualität eines Software-Produktes aus Kundensicht .....	536

## Teil III Technische Informatik 539

### Kapitel 13 Transistoren, Chips und logische Bausteine 541

13.1	Rätsel: Synthetische Rätsel (4) .....	542
13.2	Transistoren .....	542
13.2.1	Funktionsweise und Aufbau von Transistoren .....	542
13.2.2	Realisierung boolescher Funktionen mit Transistoren .....	544
13.3	Chips .....	545
13.3.1	Geschichtliche Entwicklung .....	545
13.3.2	Herstellungsprozess .....	546
13.4	Logische Bausteine .....	547
13.4.1	Gatter .....	547
13.4.2	Decoder .....	548
13.4.3	Encoder .....	549
13.4.4	Multiplexer (Selektor) .....	549
13.4.5	Demultiplexer .....	552

### Kapitel 14 Schaltnetze 555

14.1	Rätsel: Ein dialektisches Rätsel .....	556
14.2	Normalformen von Schaltfunktionen .....	556
14.2.1	Disjunktive Normalform (DNF) .....	556
14.2.2	Konjunktive Normalform (KNF) .....	557
14.2.3	Allgemeines Verfahren beim Erstellen einer Schaltung .....	558
14.2.4	Schaltkreisrealisierung durch PLAs .....	559
14.3	Entwurf von Schaltnetzen .....	562
14.4	Minimierung logischer Ausdrücke .....	563
14.4.1	Karnaugh-Veitch-Diagramme (KV-Diagramme) .....	563
14.4.2	Don't Care Argumente .....	567
14.4.3	Quine-McCluskey-Verfahren .....	570
14.5	Addiernetze .....	576
14.5.1	Paralleladdierer .....	576
14.5.2	Paralleladdierer und -subtrahierer .....	578
14.5.3	Carry-Select-Addiernetze .....	579
14.5.4	Carry-Save-Addiernetze .....	581
14.5.5	Multiplizierer .....	582
14.6	Prinzipieller Aufbau einer ALU .....	584

<b>Kapitel 15 Schaltwerke</b>	<b>587</b>
15.1 Rätsel: Waldlauf, Schnapsgläser und mehr .....	588
15.2 Synchrone und asynchrone Schaltwerke .....	589
15.3 Schaltungen mit Delays .....	590
15.3.1 4-Bit-Ringzähler als synchrones Schaltwerk .....	590
15.3.2 Delays .....	591
15.3.3 Realisierung von Delays mit Flipflops .....	593
15.4 Zähler und Frequenzteiler .....	601
15.4.1 Synchroner 4-Bit-Ringzähler mit JK-Flipflops .....	601
15.4.2 Asynchroner 4-Bit-Ringzähler mit T-Flipflops .....	603
15.4.3 Synchroner BCD-Zähler (Mod-10) mit T-Flipflops .....	604
15.4.4 Asynchroner BCD-Zähler (Mod-10) mit JK-Flipflops .....	604
15.5 Schieberegister .....	605
15.6 Entwurf synchroner Schaltwerke mittels Automaten .....	607
15.6.1 Kurze Einführung in die Automatentheorie .....	607
15.6.2 Entwurf von Schaltwerken mit Moore- und Mealy-Automaten ...	610
<b>Kapitel 16 Prozessorarchitekturen, Speicher und Caches</b>	<b>621</b>
16.1 Rätsel: Schachbrett-Quadrate, Flickenmuster, Kreuzformfirma .....	622
16.2 CISC und RISC .....	623
16.3 Pipelining (Fließbandverarbeitung) .....	625
16.3.1 Unterschiedliche Phasen beim Pipelining .....	625
16.3.2 Geschwindigkeitsgewinn beim Pipelining .....	627
16.3.3 Hazards beim Pipelining .....	629
16.4 Speicher für Prozessoren .....	632
16.5 Caches .....	635
16.5.1 Das Lokalitätsprinzip und der Cache-Controller .....	636
16.5.2 Der Lesezugriff .....	637
16.5.3 Vollassoziative und direktabgebildete Caches .....	639
16.5.4 Der Schreibzugriff .....	642
16.6 Virtueller Speicher .....	644
16.6.1 Paging .....	645
16.6.2 Segmentierung .....	647
<b>Teil IV Theoretische Informatik</b>	<b>649</b>
<b>Kapitel 17 Automatentheorie und formale Sprachen</b>	<b>651</b>
17.1 Rätsel: Weg durch ein Labyrinth und um die Ecke gedacht .....	652
17.2 Lexikalische und syntaktische Analyse .....	652
17.3 Reguläre Sprachen und endliche Automaten .....	654
17.3.1 Alphabet, Wort und Sprache .....	654
17.3.2 Reguläre Ausdrücke .....	655
17.3.3 Endliche Automaten und reguläre Sprachen .....	657

17.3.4	Realisierung endlicher Automaten .....	659
17.3.5	lex – Ein Werkzeug für die lexikalische Analyse .....	660
17.4	Kontextfreie Sprachen und Kellerautomaten .....	664
17.4.1	Kontextfreie Grammatiken .....	664
17.4.2	Kellerautomaten .....	667
17.4.3	yacc – Ein Werkzeug für die Syntaxanalyse .....	670
17.4.4	lex und yacc im Zusammenspiel .....	674
17.4.5	Rekursion bei der Syntaxanalyse .....	675
17.5	Die unterschiedlichen Phasen eines Compilers .....	675
<b>Kapitel 18 Berechenbarkeitstheorie</b>		<b>679</b>
18.1	Rätsel: Kneipen, Ei, stehen gebliebene Uhr und Alter .....	680
18.2	Berechenbare Funktionen .....	681
18.3	Nicht berechenbare Funktionen .....	682
18.3.1	Das Diagonalverfahren von Cantor .....	682
18.3.2	Nicht durch einen Algorithmus berechenbare Funktionen .....	683
18.3.3	Die Church'sche Algorithmus-Definition .....	683
18.4	Berechenbarkeitskonzepte .....	684
18.4.1	Turingmaschinen .....	684
18.4.2	Turing-berechenbare Funktionen .....	687
18.4.3	Registermaschinen .....	687
18.4.4	GOTO- und WHILE-Programme .....	688
18.4.5	LOOP-Programme (FOR-Programme) .....	690
18.4.6	Primitive Rekursion .....	691
18.4.7	$\mu$ -Rekursion .....	694
18.4.8	Die Ackermann-Funktion .....	695
18.4.9	Die Church'sche Thése und die Chomsky-Hierarchie .....	697
18.5	Prinzipiell unlösbare Probleme .....	698
18.5.1	Entscheidbare Mengen .....	698
18.5.2	Semi-entscheidbare Mengen (Game of Life und Halteproblem) ..	699
18.5.3	Unberechenbarkeit (Fleißiger Biber) .....	703
<b>Kapitel 19 Komplexitätstheorie</b>		<b>707</b>
19.1	Rätsel: Falsche Uhrzeit, Kalenderrechnen und mehr .....	708
19.2	Die Klasse P für praktisch lösbarer Probleme .....	708
19.3	Nichtdeterminismus und die Klasse NP .....	709
19.3.1	Das SAT-Problem als erstes NP-Problem .....	709
19.3.2	Reduzierung auf ja/nein-Probleme mit zugehörigen Sprachen ..	710
19.3.3	Nichtdeterminismus .....	710
19.3.4	Die Klasse NP .....	711
19.4	Der Satz von Cook und NP-Vollständigkeit .....	713
19.4.1	Das Dreifarbenproblem als Spezialfall des SAT-Problems .....	713
19.4.2	NP-Vollständigkeit .....	714
19.4.3	P = NP? .....	715
19.4.4	Das 3SAT-Problem .....	715

19.4.5	Das Cliquenproblem . . . . .	716
19.4.6	Das Rucksack- und Teilsummen-Problem . . . . .	718
19.4.7	Das Hamilton-Problem . . . . .	723
19.4.8	Das Problem des Handlungsreisenden . . . . .	723
19.4.9	Hierarchie der NP-vollständigen Probleme . . . . .	726
19.5	Approximationsalgorithmen . . . . .	726

**Teil V Codes, Kompression, Kryptografie** 731

Kapitel 20 Fehlertolerante Codes 733

20.1	Rätsel: Auf der Demo mit Bruder und Schwester .....	734
20.2	Motivation für fehlertolerante Codes .....	734
20.3	„k aus n“-Codes .....	734
20.4	Der Hammingabstand eines Codes .....	735
20.5	Eindimensionale Parity-Prüfung .....	737
20.6	Zweidimensionale Parity-Prüfung .....	738
20.7	Hamming-Codes .....	743
20.8	CRC-Kodierung .....	745

Kapitel 21 Datenkompression 749

21.1	Rätsel: Tierseuche .....	750
21.2	Verlustbehaftete und verlustlose Kompression .....	750
21.3	Codes mit variabel langen Codewörtern .....	750
21.4	Fano-Bedingung für Dekodierbarkeit eines Codes .....	751
21.5	Lauflängenkodierung („run-length encoding“) .....	752
21.6	Shannon-Fano-Kodierung .....	753
21.7	Huffman-Kodierung .....	753
21.8	Arithmetische Kodierung .....	757
21.9	Lempel-Ziv-Kodierungen .....	760
21.9.1	Der LZ77-Algorithmus .....	762
21.9.2	Der LZSS-Algorithmus .....	763
21.9.3	Der LZ78-Algorithmus .....	764
21.9.4	Der LZW-Algorithmus .....	765
21.9.5	Varianten der Lempel-Ziv-Kodierung .....	769

Kapitel 22 Kryptografie 771

22.1	Rätsel: Weinflasche und Erben von Weinfässern . . . . .	772
22.2	Allgemeines zu Kryptosystemen . . . . .	772
22.3	Einfache Verschlüsselungsmethoden . . . . .	772
	22.3.1 Cäsar-Chiffre . . . . .	772
	22.3.2 Chiffre mit eigener Zuordnungstabelle . . . . .	773
22.4	Vigenère-Verschlüsselungsmethoden . . . . .	773

22.5	Verschlüsselung mittels Zufallsfolgen .....	774
22.6	Kryptosysteme mit öffentlichen Schlüsseln .....	776
22.6.1	Eigenschaften von Public-Key-Systemen .....	776
22.6.2	Der Satz von Euler .....	777
22.6.3	Schlüsselerzeugung beim RSA-Algorithmus .....	778
22.6.4	Ver- und Entschlüsselung mit dem RSA-Algorithmus .....	780
<b>Weiterführende Literatur</b>		<b>783</b>
<b>Sachregister</b>		<b>789</b>