

Helmut Herold • Bruno Lurz • Jürgen Wohrab

# Grundlagen der Informatik

Praktisch – Technisch – Theoretisch



---

ein Imprint von Pearson Education  
München • Boston • San Francisco • Harlow, England  
Don Mills, Ontario • Sydney • Mexico City  
Madrid • Amsterdam

# Inhaltsverzeichnis

<b>Kapitel 1</b>	<b>Einleitung</b>	<b>15</b>
1.1	Idee dieses Buches .....	16
1.2	Beispiele, Übungen und Rätsel .....	17
1.3	Begleitmaterial zu diesem Buch .....	17
1.4	Danksagung .....	18
1.5	Hinweis in eigener Sache .....	19
<b>Teil I</b>	<b>Einführung in die Informatik</b>	<b>21</b>
<b>Kapitel 2</b>	<b>Die Historie und die Teilgebiete der Informatik</b>	<b>23</b>
2.1	Rätsel: Streichholzprobleme .....	24
2.2	Der Begriff Informatik .....	24
2.3	Historische Entwicklung der Informatik .....	24
2.3.1	Der Abakus .....	24
2.3.2	Der Begriff Algorithmus und Ibn Musa Al-Chwarismi .....	27
2.3.3	Wichtige Stationen von 1500 bis 1930 .....	28
2.3.4	Konrad Zuse und der erste funktionstüchtige Computer .....	30
2.3.5	Howard H. Aiken und die Mark I .....	32
2.3.6	John von Neumann .....	32
2.3.7	Generationen der elektronischen Datenverarbeitung .....	33
2.4	Einordnung und Einteilung der Informatik .....	37
2.4.1	Verschiedene Einsatzgebiete von Computern (Informatik) .....	37
2.4.2	Die Teilgebiete der Informatik .....	38
2.4.3	Die Informatik und unsere Abhängigkeit von ihr .....	41
<b>Kapitel 3</b>	<b>Speicherung und Interpretation von Information</b>	<b>43</b>
3.1	Rätsel: Umfüllprobleme .....	44
3.2	Unterschiedliche Zahlensysteme .....	44
3.2.1	Das römische Zahlensystem .....	44
3.2.2	Positionssysteme .....	45
3.2.3	Positionssysteme bei natürlichen Zahlen .....	46
3.2.4	Positionssysteme bei gebrochenen Zahlen .....	51
3.3	Dual-, Oktal- und Hexadezimalsystem .....	52
3.3.1	Das Dualsystem und das Bit im Rechner .....	52
3.3.2	Konvertieren zwischen Dual- und Oktalsystem .....	53
3.3.3	Konvertieren zwischen Dual- und Hexadezimalsystem .....	53
3.4	Konvertierungsalgorithmen .....	55
3.4.1	Konvertieren von anderen Systemen in das Dezimalsystem .....	55
3.4.2	Konvertieren vom Dezimalsystem in andere Positionssysteme ...	55

3.4.3	Konvertieren echt gebrochener Zahlen .....	56
3.4.4	Konvertieren unecht gebrochener Zahlen .....	58
3.5	Rechenoperationen im Dualsystem .....	58
3.5.1	Addition .....	58
3.5.2	Subtraktion und Darstellung negativer Zahlen .....	59
3.5.3	Multiplikation und Division .....	63
3.5.4	Konvertieren durch sukzessive Multiplikation und Addition ....	63
3.6	Reelle Zahlen .....	64
3.6.1	Festpunktzahlen .....	64
3.6.2	Gleitpunktzahlen und das IEEE-Format .....	64
3.7	Codes zur Darstellung von Zeichen .....	67
3.7.1	ASCII-Code .....	67
3.7.2	Unicode .....	70
3.8	Weitere Codes für Zahlen und Zeichen .....	71
3.8.1	BCD-Code für Zahlen .....	71
3.8.2	Gray-Code .....	72
3.8.3	Barcode .....	72
3.9	Duale Größenangaben .....	73
3.10	Die Grunddatentypen in der Programmiersprache C/C++ .....	73

## **Kapitel 4      Boolesche Algebra** **77**

4.1	Analytische Rätsel (1) .....	78
4.2	George Boole und seine Algebra mit nur zwei Werten .....	78
4.3	Operatoren .....	79
4.4	Boolesche Schaltungen .....	81
4.5	Axiome .....	81
4.6	Funktionen .....	83

## **Kapitel 5      Hardware-Komponenten eines Computers** **87**

5.1	Analytische Rätsel (2) .....	88
5.2	Aufbau von Computersystemen .....	88
5.2.1	Zentraleinheit und Peripheriegeräte .....	88
5.2.2	EVA und das von-Neumann'sche-Rechnermodell .....	89
5.3	Die heutigen Personal Computer (PCs) .....	91
5.4	Die Zentraleinheit .....	91
5.4.1	Der Prozessor .....	93
5.4.2	Der Arbeitsspeicher .....	103
5.4.3	ROMs zur Speicherung von Programmen und konstanten Daten .	105
5.4.4	Das BIOS .....	107
5.4.5	Busse und Schnittstellen (Anschlüsse) .....	108
5.5	Die Peripherie .....	113
5.5.1	Massenspeicher .....	113
5.5.2	Eingabegeräte .....	118
5.5.3	Ausgabegeräte .....	120

5.6	Modell eines einfachen Prozessorsystems .....	123
5.7	Alternative Rechnerarchitekturen (Neuronale Netze) .....	128
<b>Kapitel 6 Vom Programm zum Maschinenprogramm</b>		<b>129</b>
6.1	Analytische Rätsel (3) .....	130
6.2	Entwicklung eines Programms .....	130
6.3	Programmierwerkzeuge .....	131
6.3.1	Unterschiedliche Arten der Übersetzung .....	131
6.3.2	Der Compiler .....	132
6.3.3	Der Linker .....	133
6.3.4	Der Lader (und Locator) .....	135
6.3.5	Der Debugger .....	136
<b>Teil II Praktische Informatik</b>		<b>139</b>
<b>Kapitel 7 Programmiersprachen</b>		<b>141</b>
7.1	Analytische Rätsel (4) .....	142
7.2	Höhere Programmiersprachen .....	142
7.3	Grundlagen der Programmierung .....	145
7.3.1	Spezifikation einer Aufgabenstellung .....	145
7.3.2	Der Begriff Algorithmus .....	146
7.3.3	Formulierung und Darstellung eines Algorithmus .....	146
7.3.4	Programm = Daten + Algorithmus .....	148
7.4	Datentypen und Operatoren in C/C++ und Java .....	154
7.4.1	Datentypen und Konstanten .....	154
7.4.2	Bezeichner .....	156
7.4.3	Grundlegende Operatoren .....	156
7.4.4	Die logischen Operatoren &&,    und ! .....	157
7.4.5	Die Shift-Operatoren << und >> .....	157
7.4.6	Die Postfix- und Präfixoperatoren ++ und -- .....	158
7.4.7	Die Bit-Operatoren &,  , ^ und ~ .....	159
7.4.8	Prioritäten und Assoziativitäten der Operatoren .....	160
7.5	Formulierung von Algorithmen in C/C++ und Java .....	162
7.5.1	Sequenz .....	162
7.5.2	Verzweigungen mit if .....	162
7.5.3	Verzweigungen mit switch .....	168
7.5.4	for-Schleife (Schleife mit der Abfrage am Anfang) .....	169
7.5.5	while-Schleife (Schleife mit der Abfrage am Anfang) .....	176
7.5.6	do... while-Schleife (Schleife mit der Abfrage am Ende) .....	179
7.5.7	Abbruch von Schleifen mit break .....	180
7.5.8	Abbruch eines einzelnen Schleifendurchlaufs mit continue .....	182
7.5.9	Abbruch mehrerer geschachtelter Schleifen mit goto .....	182
7.5.10	Programmabbruch mit exit .....	183
7.5.11	Allgemeines zu Funktionen bzw. Methoden .....	183
7.5.12	Rekursive Funktionen bzw. rekursive Methoden .....	193

7.5.13	Arrays .....	202
7.5.14	Strings .....	207
7.5.15	Zufallszahlen .....	210
7.5.16	Argumente auf der Kommandozeile .....	212
7.5.17	Ausnahmen (Exceptions) in Java .....	213
7.5.18	Dateien .....	214
7.5.19	Strukturen in C/C++ .....	223
7.6	Objektorientierte Programmierung mit Java .....	225
7.6.1	Meilensteine in der Softwareentwicklung .....	225
7.6.2	Einführung in die Objektorientierung .....	233
7.6.3	Klassen und Objekte .....	240
7.6.4	Konstruktoren .....	246
7.6.5	Vererbung und Polymorphismus .....	247
7.6.6	GUI-Programmierung in Java .....	256
<b>Kapitel 8 Datenstrukturen und Algorithmen</b>		<b>269</b>
8.1	Analytische Rätsel (5) .....	270
8.2	Grundlegende Datenstrukturen .....	271
8.2.1	Allgemeine Eigenschaften von Daten .....	271
8.2.2	Basis-Datentypen .....	271
8.2.3	Datenstruktur = Daten + Operationen .....	271
8.2.4	Verkettete Listen .....	272
8.2.5	Stack (Stapel) .....	285
8.2.6	Queue (Warteschlange) .....	293
8.3	Bäume .....	298
8.3.1	Grundlegendes zu Bäumen .....	298
8.3.2	Binäre Bäume .....	300
8.3.3	Baumrekursion bei Bäumen mit mehr als zwei Zweigen .....	315
8.4	Komplexität von Algorithmen und O-Notation .....	326
8.4.1	Zeitaufwand .....	326
8.4.2	Speicherplatzbedarf .....	329
8.4.3	Klassifikation von Algorithmen .....	330
8.4.4	Die O-Notation .....	332
8.4.5	Wahl eines Algorithmus .....	338
8.4.6	Einfache Optimierungen bei der Implementierung .....	339
8.5	Elementare Sortieralgorithmen .....	342
8.5.1	Grundsätzliches zu Sortieralgorithmen .....	342
8.5.2	Bubble-Sort .....	343
8.5.3	Insert-Sort .....	345
8.5.4	Select-Sort .....	346
8.5.5	Zeitmessungen für Bubble-, Insert- und Select-Sort .....	347
8.5.6	Distribution Count-Sort (Bucket-Sort) .....	348
8.6	Shell-Sort .....	351
8.7	Quicksort .....	353
8.8	Mergesort .....	355
8.8.1	Rekursiver Mergesort für Arrays .....	355

8.8.2	Nicht-rekursiver Mergesort für Arrays .....	357
8.8.3	Analyse des Mergesort .....	358
8.8.4	Mischen von zwei sortierten Arrays .....	358
8.9	Backtracking .....	359
8.9.1	Finden in einem Labyrinth .....	359
8.9.2	Das Achtdamen-Problem .....	361
8.9.3	Rekursives Füllen von Figuren .....	363
8.9.4	Sudoku .....	363
8.9.5	Branch-and-Bound-Verfahren .....	364

## **Kapitel 9 Betriebssysteme 365**

9.1	Rätsel: Überquerung einer Hängebrücke .....	366
9.2	Der Begriff Betriebssystem .....	366
9.3	Die Geschichte von Betriebssystemen .....	366
9.4	Grundaufgaben von Betriebssystemen .....	369
9.5	Aufbau und Dienste von Betriebssystemen .....	370
9.5.1	Schichtenaufbau .....	371
9.5.2	Prozesse, Threads, Scheduling .....	372
9.5.3	Synchronisations-Mechanismen .....	375
9.5.4	Zeitdienste (Timer) .....	378
9.5.5	Speicherverwaltung .....	380
9.5.6	Dateiverwaltung und Dateisysteme .....	381
9.5.7	Geräteverwaltung und Treiber .....	384
9.5.8	Benutzerschnittstelle (Kommandozeile bzw. GUI) .....	386
9.5.9	Programmierschnittstelle (API) .....	388
9.6	Besonderheiten bei Embedded Systemen .....	391

## **Kapitel 10 Rechnernetze und das Internet 395**

10.1	Synthetische Rätsel (1) .....	396
10.2	Grundlagen der Vernetzung von Rechnern .....	396
10.3	Das ISO/OSI-Modell und Internet-Protokolle .....	397
10.4	Internet-Protokolle in Rechnernetzen .....	399
10.4.1	Grundbegriffe zu TCP/IP-Netzen .....	399
10.4.2	TCP/IP-Protokolle .....	402
10.5	Hubs, Switches, Router und Gateways .....	407
10.6	Grundlagen der Socket-Programmierung .....	407
10.7	Verteilte Anwendungen .....	407
10.8	Das World Wide Web (WWW) .....	409
10.8.1	Wichtige Komponenten und Konzepte des WWW .....	409
10.8.2	Kurze Einführung in HTML .....	411
10.8.3	Cascading Style Sheets (CSS) .....	424
10.8.4	Eine kurze Einführung in XML .....	426
10.8.5	XHTML – das neue, XML-basierte HTML .....	429
10.8.6	Web-Programmierung .....	429

<b>Kapitel 11</b>	<b>Datenbanksysteme</b>	<b>437</b>
11.1	Synthetische Rätsel (2) .....	438
11.2	Grundlegendes zu Datenbanksystemen .....	438
11.2.1	Aufgaben einer Datenbank .....	438
11.2.2	Vorteile von Datenbanken .....	439
11.2.3	Datenunabhängigkeit .....	440
11.3	Datenmodelle .....	441
11.3.1	Das Entity-Relationship-Modell .....	441
11.3.2	Das relationale Datenmodell .....	442
11.3.3	Die relationale Algebra .....	444
11.4	Die Datenbanksprache SQL .....	445
11.4.1	Datendefinition .....	446
11.4.2	Einfügen, Ändern und Löschen von Datensätzen .....	447
11.4.3	Anfragen mit select .....	448
<b>Kapitel 12</b>	<b>Software Engineering</b>	<b>451</b>
12.1	Synthetische Rätsel (3) .....	452
12.2	Die Software-Krise .....	452
12.3	Eine geeignete Software-Architektur .....	454
12.4	UML-Diagramme für die Modellierung .....	454
12.4.1	Statische Modellierung in UML .....	455
12.4.2	Dynamische Modellierung in UML .....	457
12.5	Modellierungsmöglichkeiten für die Software .....	459
12.6	Notwendigkeit von Prozessen .....	459
12.7	Der wichtige Prozess „Requirement Engineering“ .....	460
12.7.1	Das UML-Anwendungsfalldiagramm (Use Case Diagram) .....	461
12.7.2	Das UML-Aktivitätsdiagramm .....	462
12.7.3	Genaue Klärung der Kundenanforderungen .....	464
12.8	Prozessmodelle .....	465
12.8.1	Schwer- und leichtgewichtige Prozessmodelle .....	465
12.8.2	Das Wasserfall-Modell .....	465
12.8.3	Das V-Modell .....	467
12.8.4	Inkrementelle und iterative Prozessmodelle .....	468
12.8.5	Agiles Vorgehen mit eXtreme Programming (XP) .....	470
12.9	Qualität eines Software-Produktes aus Kundensicht .....	472
<b>Teil III</b>	<b>Technische Informatik</b>	<b>475</b>
<b>Kapitel 13</b>	<b>Transistoren, Chips und logische Bausteine</b>	<b>477</b>
13.1	Synthetische Rätsel (4) .....	478
13.2	Transistoren .....	478
13.2.1	Funktionsweise und Aufbau von Transistoren .....	478
13.2.2	Realisierung boolescher Funktionen mit Transistoren .....	480

13.3	Chips .....	481
13.3.1	Geschichtliche Entwicklung .....	481
13.3.2	Herstellungsprozess .....	482
13.4	Logische Bausteine .....	483
13.4.1	Gatter .....	483
13.4.2	Decoder .....	484
13.4.3	Encoder .....	485
13.4.4	Multiplexer (Selektor) .....	485
13.4.5	Demultiplexer .....	488
<b>Kapitel 14  Schaltnetze</b>		<b>491</b>
14.1	Ein dialektisches Rätsel .....	492
14.2	Normalformen von Schaltfunktionen .....	492
14.2.1	Disjunktive Normalform (DNF) .....	492
14.2.2	Konjunktive Normalform (KNF) .....	493
14.2.3	Allgemeines Verfahren beim Erstellen einer Schaltung .....	494
14.2.4	Schaltkreisrealisierung durch PLAs .....	495
14.3	Entwurf von Schaltnetzen .....	498
14.4	Minimierung logischer Ausdrücke .....	499
14.4.1	Karnaugh-Veitch-Diagramme (KV-Diagramme) .....	499
14.4.2	Don't Care Argumente .....	503
14.4.3	Quine-McCluskey-Verfahren .....	506
14.5	Addiernetze .....	512
14.5.1	Paralleladdierer .....	512
14.5.2	Paralleladdierer und -subtrahierer .....	514
14.5.3	Carry-Select-Addiernetze .....	515
14.5.4	Carry-Save-Addiernetze .....	517
14.5.5	Multiplizierer .....	518
14.6	Prinzipieller Aufbau einer ALU .....	520
<b>Kapitel 15  Schaltwerke</b>		<b>523</b>
15.1	Rätsel: Waldlauf, Schnapsgläser und mehr .....	524
15.2	Synchrone und asynchrone Schaltwerke .....	525
15.3	Schaltungen mit Delays .....	526
15.3.1	4-Bit-Ringzähler als synchrones Schaltwerk .....	526
15.3.2	Delays .....	527
15.3.3	Realisierung von Delays mit Flipflops .....	529
15.4	Zähler und Frequenzteiler .....	537
15.4.1	Synchrone 4-Bit-Ringzähler mit JK-Flipflops .....	537
15.4.2	Asynchrone 4-Bit-Ringzähler mit T-Flipflops .....	539
15.4.3	Synchrone BCD-Zähler (Mod-10) mit T-Flipflops .....	540
15.4.4	Asynchrone BCD-Zähler (Mod-10) mit JK-Flipflops .....	540
15.5	Schieberegister .....	541
15.6	Entwurf synchroner Schaltwerke mittels Automaten .....	543
15.6.1	Kurze Einführung in die Automatentheorie .....	543
15.6.2	Entwurf von Schaltwerken mit Moore- und Mealy-Automaten ...	546



<b>Kapitel 16</b>	<b>Prozessorarchitekturen, Speicher und Caches</b>	<b>557</b>
16.1	Rätsel: Schachbrett-Quadrate, Flickmuster, Kreuzformfirma .....	558
16.2	CISC und RISC .....	559
16.3	Pipelining (Fließbandverarbeitung) .....	561
16.3.1	Unterschiedliche Phasen beim Pipelining .....	561
16.3.2	Geschwindigkeitsgewinn beim Pipelining .....	563
16.3.3	Hazards beim Pipelining .....	565
16.4	Speicher für Prozessoren .....	568
16.5	Caches .....	571
16.5.1	Das Lokalitätsprinzip und der Cache-Controller .....	572
16.5.2	Der Lesezugriff .....	573
16.5.3	Vollasoziative und direktabgebildete Caches .....	575
16.5.4	Der Schreibzugriff .....	578
16.6	Virtueller Speicher .....	580
16.6.1	Paging .....	581
16.6.2	Segmentierung .....	583

## **Teil IV      Theoretische Informatik      585**

<b>Kapitel 17</b>	<b>Automatentheorie und formale Sprachen</b>	<b>587</b>
17.1	Rätsel: Weg durch ein Labyrinth und um die Ecke gedacht .....	588
17.2	Lexikalische und syntaktische Analyse .....	588
17.3	Reguläre Sprachen und endliche Automaten .....	590
17.3.1	Alphabet, Wort und Sprache .....	590
17.3.2	Reguläre Ausdrücke .....	591
17.3.3	Endliche Automaten und reguläre Sprachen .....	593
17.3.4	Realisierung endlicher Automaten .....	595
17.3.5	lex – Ein Werkzeug für die lexikalische Analyse .....	596
17.4	Kontextfreie Sprachen und Kellerautomaten .....	600
17.4.1	Kontextfreie Grammatiken .....	600
17.4.2	Kellerautomaten .....	603
17.4.3	yacc – Ein Werkzeug für die Syntaxanalyse .....	606
17.4.4	lex und yacc im Zusammenspiel .....	610
17.4.5	Rekursion bei der Syntaxanalyse .....	611
17.5	Die unterschiedlichen Phasen eines Compilers .....	611
<b>Kapitel 18</b>	<b>Berechenbarkeitstheorie</b>	<b>615</b>
18.1	Rätsel: Kneipen, Ei, stehen gebliebene Uhr und Alter .....	616
18.2	Berechenbare Funktionen .....	617
18.3	Nicht berechenbare Funktionen .....	618
18.3.1	Das Diagonalverfahren von Cantor .....	618
18.3.2	Nicht durch einen Algorithmus berechenbare Funktionen .....	619
18.3.3	Die Church'sche Algorithmus-Definition .....	619

18.4	Berechenbarkeitskonzepte .....	620
18.4.1	Turingmaschinen .....	620
18.4.2	Turing-berechenbare Funktionen .....	623
18.4.3	Registermaschinen .....	623
18.4.4	GOTO- und WHILE-Programme .....	624
18.4.5	LOOP-Programme (FOR-Programme) .....	626
18.4.6	Primitive Rekursion .....	627
18.4.7	$\mu$ -Rekursion .....	630
18.4.8	Die Ackermann-Funktion .....	631
18.4.9	Die Church'sche These und die Chomsky-Hierarchie .....	633
18.5	Prinzipiell unlösbare Probleme .....	634
18.5.1	Entscheidbare Mengen .....	634
18.5.2	Semi-entscheidbare Mengen (Game of Life und Halteproblem) ..	635
18.5.3	Unberechenbarkeit (Fleißiger Biber) .....	639

## **Kapitel 19 Komplexitätstheorie 643**

19.1	Rätsel: Falsche Uhrzeit, Kalenderrechnen und mehr .....	644
19.2	Die Klasse P für praktisch lösbare Probleme .....	644
19.3	Nichtdeterminismus und die Klasse NP .....	645
19.3.1	Das SAT-Problem als erstes NP-Problem .....	645
19.3.2	Reduzierung auf ja/nein-Probleme mit zugehörigen Sprachen ...	646
19.3.3	Nichtdeterminismus .....	646
19.3.4	Die Klasse NP .....	647
19.4	Der Satz von Cook und NP-Vollständigkeit .....	649
19.4.1	Das Dreifarbenproblem als Spezialfall des SAT-Problems .....	649
19.4.2	NP-Vollständigkeit .....	650
19.4.3	$P = NP?$ .....	651
19.4.4	Das 3SAT-Problem .....	651
19.4.5	Das Cliquesproblem .....	652
19.4.6	Das Rucksack- und Teilsummen-Problem .....	654
19.4.7	Das Hamilton-Problem .....	659
19.4.8	Das Problem des Handlungsreisenden .....	659
19.4.9	Hierarchie der NP-vollständigen Probleme .....	662
19.5	Approximationsalgorithmen .....	662

## **Teil V Codes, Kompression, Kryptografie 667**

### **Kapitel 20 Fehlertolerante Codes 669**

20.1	Rätsel: Auf der Demo mit Bruder und Schwester .....	670
20.2	Motivation für fehlertolerante Codes .....	670
20.3	„k aus n“-Codes .....	670
20.4	Der Hammingabstand eines Codes .....	671
20.5	Eindimensionale Parity-Prüfung .....	673

20.6	Zweidimensionale Parity-Prüfung .....	674
20.7	Hamming-Code .....	679
20.8	CRC-Kodierung .....	681
<b>Kapitel 21 Datenkompression</b>		<b>685</b>
21.1	Rätsel: Tierseuche .....	686
21.2	Verlustbehaftete und verlustlose Kompression .....	686
21.3	Codes mit variabel langen Codewörtern .....	686
21.4	Fano-Bedingung für Dekodierbarkeit eines Codes .....	687
21.5	Laufängenkodierung („run-length encoding“) .....	688
21.6	Shannon-Fano-Kodierung .....	689
21.7	Huffman-Kodierung .....	689
21.8	Arithmetische Kodierung .....	693
21.9	Lempel-Ziv-Kodierungen .....	696
21.9.1	Der LZ77-Algorithmus .....	698
21.9.2	Der LZSS-Algorithmus .....	699
21.9.3	Der LZ78-Algorithmus .....	700
21.9.4	Der LZW-Algorithmus .....	701
21.9.5	Varianten der Lempel-Ziv-Kodierung .....	705
<b>Kapitel 22 Kryptografie</b>		<b>707</b>
22.1	Rätsel: Weinflasche und Erben von Weinfässern .....	708
22.2	Allgemeines zu Kryptosystemen .....	708
22.3	Einfache Verschlüsselungsmethoden .....	708
22.3.1	Cäsar-Chiffre .....	708
22.3.2	Chiffre mit eigener Zuordnungstabelle .....	709
22.4	Vigenère-Verschlüsselungsmethoden .....	709
22.5	Verschlüsselung mittels Zufallsfolgen .....	710
22.6	Kryptosysteme mit öffentlichen Schlüsseln .....	712
22.6.1	Eigenschaften von Public-Key-Systemen .....	712
22.6.2	Der Satz von Euler .....	713
22.6.3	Schlüsselerzeugung beim RSA-Algorithmus .....	714
22.6.4	Ver- und Entschlüsselung mit dem RSA-Algorithmus .....	716
22.7	Quantenkryptografie .....	718
<b>Weiterführende Literatur</b>		<b>721</b>
<b>Sachregister</b>		<b>727</b>
<b>Demonstrationsprogramme und HTML-/XML-Dateien</b>		<b>739</b>
<b>Simulationsprogramme</b>		<b>743</b>