



Springer-Verlag Berlin Heidelberg GmbH

Johannes Buchmann

---

# Einführung in die Kryptographie

Zweite, erweiterte Auflage



Springer

**Professor Dr. Johannes Buchmann**  
Technische Universität Darmstadt  
Fachbereich Informatik  
Alexanderstraße 10  
64283 Darmstadt  
Deutschland  
e-mail: buchmann@cdc.informatik.tu-darmstadt.de

---

Mathematics Subject Classification (2000): 94A60, 68P25, 11Y16

---

Die Deutsche Bibliothek – CIP-Einheitsaufnahme

*Buchmann, Johannes:*

Einführung in die Kryptographie / Johannes Buchmann. - 2., erw. Aufl. - Berlin; Heidelberg; New York; Barcelona; Hongkong; London; Mailand; Paris; Singapur; Tokio; Springer, 2001  
(Springer-Lehrbuch)

ISBN 978-3-540-41283-0      ISBN 978-3-662-06856-4 (eBook)  
DOI 10.1007/978-3-662-06856-4

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Eine Vervielfältigung dieses Werkes oder von Teilen dieses Werkes ist auch im Einzelfall nur in den Grenzen der gesetzlichen Bestimmungen des Urheberrechtsgesetzes der Bundesrepublik Deutschland vom 9. September 1965 in der jeweils geltenden Fassung zulässig. Sie ist grundsätzlich vergütungspflichtig. Zuwiderhandlungen unterliegen den Strafbestimmungen des Urheberrechtsgesetzes.

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 1999, 2001  
Ursprünglich erschienen bei Springer-Verlag Berlin Heidelberg New York 2001.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, daß solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Satz: Datenerstellung durch den Autor unter Verwendung eines Springer  $\text{\LaTeX}$ -Makropaketes  
Einbandgestaltung: *design & production* GmbH, Heidelberg

Bindearbeiten: Fa. Schäffer, Grünstadt

Satz: Datenerstellung durch den Autor unter Verwendung eines Springer  $\text{\TeX}$ -Makropaketes  
Einbandgestaltung: *design & production* GmbH, Heidelberg

Gedruckt auf säurefreiem Papier      SPIN: 10785432      44/3142ck - 5 4 3 2 1 0

**Für Almut, Daniel und Jan**

# Vorwort zur zweiten Auflage

In die zweite Auflage meiner Einführung in die Kryptographie habe ich eine Reihe neuer Übungsaufgaben aufgenommen. Außerdem habe ich die Fehler, die mir seit Erscheinen der ersten Auflage bekannt geworden sind, korrigiert und einige Stellen aktualisiert. Für die vielen Hinweise, die ich von Lesern erhalten habe, bedanke ich mich sehr.

Darmstadt, im Dezember 2000

*Johannes Buchmann*

# Vorwort

Kryptographie ist als Schlüsseltechnik für die Absicherung weltweiter Computernetze von zentraler Bedeutung. Moderne kryptographische Techniken werden dazu benutzt, Daten geheimzuhalten, Nachrichten elektronisch zu signieren, den Zugang zu Rechnernetzen zu kontrollieren, elektronische Geldgeschäfte abzusichern, Urheberrechte zu schützen usw. Angesichts dieser vielen zentralen Anwendungen ist es nötig, daß die Anwender einschätzen können, ob die benutzten kryptographischen Methoden effizient und sicher genug sind. Dazu müssen sie nicht nur wissen, wie die kryptographischen Verfahren funktionieren, sondern sie müssen auch deren mathematische Grundlagen verstehen.

Ich wende mich in diesem Buch an Leser, die moderne kryptographische Techniken und ihre mathematischen Fundamente kennenlernen wollen, aber nicht über die entsprechenden mathematischen Spezialkenntnisse verfügen. Mein Ziel ist es, in die Basistechniken der modernen Kryptographie einzuführen. Ich setze dabei zwar mathematische Vorbildung voraus, führe aber in die Grundlagen von linearer Algebra, Algebra, Zahlentheorie und Wahrscheinlichkeitstheorie ein, soweit diese Gebiete für die behandelten kryptographischen Verfahren relevant sind.

Das Buch ist aus einer Vorlesung entstanden, die ich seit 1996 in jedem Sommersemester an der Technischen Universität Darmstadt für Studenten der Informatik und Mathematik gehalten habe. Ich danke den Hörern dieser Vorlesung und den Mitarbeitern, die die Übungen betreut haben, für ihr Interesse und Engagement. Ich danke allen, die das Manuskript kritisch gelesen und verbessert haben. Besonders bedanke ich mich bei Harald Baier, Gabi Barking, Manuel Breuning, Safuat Hamdy, Birgit Henhagl, Andreas Kottig, Markus Maurer, Andreas Meyer, Stefan Neis, Sachar Paulus, Thomas Pfahler, Marita Skrobic, Edlyn Teske, Patrick Theobald und Ralf-Philipp Weinmann. Ich danke auch dem Springer-Verlag, besonders Martin Peters, Agnes Herrmann und Claudia Kehl, für die Unterstützung bei der Abfassung und Veröffentlichung dieses Buches.

Darmstadt, im Juli 1999

*Johannes Buchmann*

# Inhaltsverzeichnis

<b>1. Ganze Zahlen</b> .....	1
1.1 Grundlagen .....	1
1.2 Teilbarkeit .....	2
1.3 Darstellung ganzer Zahlen .....	3
1.4 $O$ - und $\Omega$ -Notation .....	5
1.5 Aufwand von Addition, Multiplikation und Division mit Rest .....	5
1.6 Polynomzeit .....	7
1.7 Größter gemeinsamer Teiler .....	7
1.8 Euklidischer Algorithmus .....	10
1.9 Erweiterter euklidischer Algorithmus .....	13
1.10 Analyse des erweiterten euklidischen Algorithmus .....	15
1.11 Zerlegung in Primzahlen .....	18
1.12 Übungen .....	20
<b>2. Kongruenzen und Restklassenringe</b> .....	23
2.1 Kongruenzen .....	23
2.2 Halbgruppen .....	25
2.3 Gruppen .....	27
2.4 Restklassenringe .....	27
2.5 Körper .....	28
2.6 Division im Restklassenring .....	29
2.7 Rechenzeit für die Operationen im Restklassenring .....	30
2.8 Prime Restklassengruppen .....	31
2.9 Ordnung von Gruppenelementen .....	32
2.10 Untergruppen .....	34
2.11 Der kleine Satz von Fermat .....	35
2.12 Schnelle Exponentiation .....	36
2.13 Schnelle Auswertung von Potenzprodukten .....	38
2.14 Berechnung von Elementordnungen .....	39
2.15 Der Chinesische Restsatz .....	41
2.16 Zerlegung des Restklassenrings .....	43
2.17 Bestimmung der Eulerschen $\varphi$ -Funktion .....	45
2.18 Polynome .....	46
2.19 Polynome über Körpern .....	47



2.20	Struktur der Einheitengruppe endlicher Körper	50
2.21	Struktur der primen Restklassengruppe nach einer Primzahl	51
2.22	Übungen	52
<b>3.</b>	<b>Verschlüsselung</b>	<b>55</b>
3.1	Verschlüsselungsverfahren	55
3.2	Symmetrische und asymmetrische Kryptosysteme	56
3.3	Kryptoanalyse	57
3.4	Alphabete und Wörter	58
3.5	Permutationen	61
3.6	Blockchiffren	62
3.7	Mehrfachverschlüsselung	63
3.8	Verwendung von Blockchiffren	63
3.8.1	ECB-Mode	64
3.8.2	CBC-Mode	65
3.8.3	CFB-Mode	68
3.8.4	OFB-Mode	70
3.9	Stromchiffren	72
3.10	Die affine Chiffre	73
3.11	Matrizen und lineare Abbildungen	74
3.11.1	Matrizen über Ringen	74
3.11.2	Produkt von Matrizen mit Vektoren	75
3.11.3	Summe und Produkt von Matrizen	75
3.11.4	Der Matrizenring	76
3.11.5	Determinante	76
3.11.6	Inverse von Matrizen	76
3.11.7	Affin lineare Funktionen	78
3.12	Affin lineare Blockchiffren	79
3.13	Vigenère-, Hill- und Permutationschiffre	79
3.14	Kryptoanalyse affin linearer Blockchiffren	80
3.15	Übungen	81
<b>4.</b>	<b>Wahrscheinlichkeit und perfekte Sicherheit</b>	<b>85</b>
4.1	Wahrscheinlichkeit	85
4.2	Bedingte Wahrscheinlichkeit	86
4.3	Geburtstagsparadox	87
4.4	Perfekte Sicherheit	89
4.5	Das Vernam-One-Time-Pad	91
4.6	Zufallszahlen	92
4.7	Pseudozufallszahlen	92
4.8	Übungen	93

<b>5. Der DES-Algorithmus</b> .....	95
5.1 Feistel-Chiffren .....	95
5.2 Der DES-Algorithmus .....	96
5.2.1 Klartext- und Schlüsselraum .....	96
5.2.2 Die initiale Permutation .....	97
5.2.3 Die interne Blockchiffre .....	98
5.2.4 Die S-Boxen .....	99
5.2.5 Die Rundenschlüssel .....	99
5.2.6 Entschlüsselung .....	101
5.3 Ein Beispiel für DES .....	102
5.4 Sicherheit des DES .....	103
5.5 Übungen .....	104
<b>6. Primzahlerzeugung</b> .....	105
6.1 Probedivision .....	105
6.2 Der Fermat-Test .....	106
6.3 Carmichael-Zahlen .....	107
6.4 Der Miller-Rabin-Test .....	108
6.5 Zufällige Wahl von Primzahlen .....	111
6.6 Übungen .....	112
<b>7. Public-Key Verschlüsselung</b> .....	113
7.1 Idee .....	113
7.2 Sicherheit .....	114
7.3 Das RSA-Verfahren .....	115
7.3.1 Schlüsselerzeugung .....	115
7.3.2 Verschlüsselung .....	116
7.3.3 Entschlüsselung .....	118
7.3.4 Sicherheit des geheimen Schlüssels .....	119
7.3.5 RSA und Faktorisierung .....	121
7.3.6 Wahl von $p$ und $q$ .....	121
7.3.7 Auswahl von $e$ und $d$ .....	122
7.3.8 Effizienz .....	123
7.3.9 Multiplikativität .....	124
7.3.10 Verallgemeinerung .....	125
7.4 Das Rabin-Verschlüsselungsverfahren .....	125
7.4.1 Schlüsselerzeugung .....	126
7.4.2 Verschlüsselung .....	126
7.4.3 Entschlüsselung .....	126
7.4.4 Effizienz .....	128
7.4.5 Sicherheit .....	128
7.4.6 Eine Chosen Ciphertext-Attacke .....	129
7.5 Diffie-Hellman-Schlüsselaustausch .....	129
7.5.1 Diskrete Logarithmen .....	130

## XIV Inhaltsverzeichnis

7.5.2	Schlüsselaustausch	131
7.5.3	Sicherheit	132
7.5.4	Andere Gruppen	132
7.6	Das ElGamal-Verschlüsselungsverfahren	133
7.6.1	Schlüsselerzeugung	133
7.6.2	Verschlüsselung	133
7.6.3	Entschlüsselung	134
7.6.4	Effizienz	134
7.6.5	ElGamal und Diffie-Hellman	135
7.6.6	Parameterwahl	135
7.6.7	ElGamal als randomisiertes Verschlüsselungsverfahren	136
7.6.8	Verallgemeinerung	136
7.7	Übungen	137
<b>8.</b>	<b>Faktorisierung</b>	<b>139</b>
8.1	Probedivision	139
8.2	Die $p - 1$ -Methode	140
8.3	Das Quadratische Sieb	140
8.3.1	Das Prinzip	141
8.3.2	Bestimmung von $x$ und $y$	141
8.3.3	Auswahl geeigneter Kongruenzen	142
8.3.4	Das Sieb	143
8.4	Analyse des Quadratischen Siebs	145
8.5	Effizienz anderer Faktorisierungsverfahren	147
8.6	Übungen	148
<b>9.</b>	<b>Diskrete Logarithmen</b>	<b>151</b>
9.1	Das DL-Problem	151
9.2	Enumeration	152
9.3	Shanks Babystep-Giantstep-Algorithmus	152
9.4	Der Pollard- $\rho$ -Algorithmus	154
9.5	Der Pohlig-Hellman-Algorithmus	157
9.5.1	Reduktion auf Primzahlpotenzordnung	158
9.5.2	Reduktion auf Primzahlordnung	159
9.5.3	Gesamtalgorithmus und Analyse	161
9.6	Index-Calculus	161
9.6.1	Idee	162
9.6.2	Diskrete Logarithmen der Faktorbasiselemente	162
9.6.3	Individuelle Logarithmen	164
9.6.4	Analyse	164
9.7	Andere Algorithmen	165
9.8	Verallgemeinerung des Index-Calculus-Verfahrens	165
9.9	Übungen	165

<b>10. Kryptographische Hashfunktionen</b> .....	167
10.1 Hashfunktionen und Kompressionsfunktionen .....	167
10.2 Geburtstagsattacke .....	169
10.3 Kompressionsfunktionen aus Verschlüsselungsfunktionen .....	170
10.4 Hashfunktionen aus Kompressionsfunktionen .....	171
10.5 Effiziente Hashfunktionen .....	173
10.6 Eine arithmetische Kompressionsfunktion .....	173
10.7 Message Authentication Codes .....	175
10.8 Übungen .....	176
<b>11. Digitale Signaturen</b> .....	177
11.1 Idee .....	177
11.2 RSA-Signaturen .....	178
11.2.1 Schlüsselerzeugung .....	178
11.2.2 Erzeugung der Signatur .....	178
11.2.3 Verifikation .....	179
11.2.4 Angriffe .....	179
11.2.5 Signatur von Texten mit Redundanz .....	180
11.2.6 Signatur mit Hashwert .....	181
11.2.7 Wahl von $p$ und $q$ .....	182
11.3 Signaturen aus Public-Key-Verfahren .....	182
11.4 ElGamal-Signatur .....	182
11.4.1 Schlüsselerzeugung .....	183
11.4.2 Erzeugung der Signatur .....	183
11.4.3 Verifikation .....	183
11.4.4 Die Wahl von $p$ .....	184
11.4.5 Die Wahl von $k$ .....	185
11.4.6 Existentielle Fälschung .....	185
11.4.7 Effizienz .....	186
11.4.8 Verallgemeinerung .....	187
11.5 Der Digital Signature Algorithm (DSA) .....	187
11.5.1 Schlüsselerzeugung .....	187
11.5.2 Erzeugung der Signatur .....	188
11.5.3 Verifikation .....	188
11.5.4 Effizienz .....	188
11.5.5 Sicherheit .....	189
11.6 Übungen .....	190
<b>12. Andere Gruppen</b> .....	191
12.1 Endliche Körper .....	191
12.1.1 Konstruktion .....	191
12.1.2 DL-Problem .....	192
12.2 Elliptische Kurven .....	193
12.2.1 Definition .....	193

- 12.2.2 Gruppenstruktur ..... 194
- 12.2.3 Kryptographisch sichere Kurven ..... 195
- 12.2.4 Vorteile von EC-Kryptographie ..... 196
- 12.3 Quadratische Formen ..... 196
- 12.4 Übungen ..... 197
  
- 13. Identifikation ..... 199**
  - 13.1 Anwendungen ..... 199
  - 13.2 Paßwörter ..... 200
  - 13.3 Einmal-Paßwörter ..... 201
  - 13.4 Challenge-Response-Identifikation ..... 201
    - 13.4.1 Verwendung von symmetrischer Kryptographie ..... 201
    - 13.4.2 Verwendung von Public-Key-Kryptographie ..... 202
    - 13.4.3 Zero-Knowledge-Beweise ..... 202
  - 13.5 Übungen ..... 204
  
- 14. Public-Key-Infrastrukturen ..... 207**
  - 14.1 Persönliche Sicherheitsumgebung ..... 207
    - 14.1.1 Bedeutung ..... 207
    - 14.1.2 Implementierung ..... 208
    - 14.1.3 Darstellungsproblem ..... 208
  - 14.2 Zertifizierungsstellen ..... 209
    - 14.2.1 Registrierung ..... 209
    - 14.2.2 Schlüsselerzeugung ..... 209
    - 14.2.3 Zertifizierung ..... 210
    - 14.2.4 Archivierung ..... 210
    - 14.2.5 Personalisierung des PSE ..... 211
    - 14.2.6 Verzeichnisdienst ..... 211
    - 14.2.7 Schlüssel-Update ..... 212
    - 14.2.8 Rückruf von Zertifikaten ..... 212
    - 14.2.9 Zugriff auf ungültige Schlüssel ..... 212
  - 14.3 Zertifikatsketten ..... 213
  
- Lösungen der Übungsaufgaben ..... 215**
  
- Literaturverzeichnis ..... 227**
  
- Sachverzeichnis ..... 229**