



---

Johannes Buchmann

# Einführung in die Kryptographie

6., überarbeitete Auflage



**Springer** Spektrum

Johannes Buchmann  
FB Informatik  
Technische Universität Darmstadt  
Darmstadt, Deutschland

ISSN 0937-7433

Springer-Lehrbuch

ISBN 978-3-642-39774-5

ISBN 978-3-642-39775-2 (eBook)

DOI 10.1007/978-3-642-39775-2

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Springer Spektrum

© Springer-Verlag Berlin Heidelberg 1999, 2000, 2003, 2007, 2010, 2016

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

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.

Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen.

*Planung:* Annika Denkert

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.

Springer-Verlag GmbH Berlin Heidelberg ist Teil der Fachverlagsgruppe Springer Science+Business Media  
([www.springer.com](http://www.springer.com))

*Für Almut, Daniel und Jan*

---

## Vorwort zur sechsten Auflage

In der sechsten Auflage meiner Einführung in die Kryptographie habe ich die Darstellung der mathematischen Modelle, die die Sicherheit kryptographischer Verfahren beschreiben, deutlich erweitert. Ich behandle jetzt die elementare Wahrscheinlichkeitstheorie im ersten Kapitel um dort schwierige Berechnungsprobleme, die Grundlage kryptographischer Sicherheit, definieren zu können. Modelle für die Sicherheit symmetrischer Verschlüsselungsverfahren finden sich in Kapitel 4. Neben der Theorie perfekter Geheimhaltung wird dort auch semantische Sicherheit und Chosen-Plaintext-Sicherheit und Ciphertext-Sicherheit vorgestellt. Auch die Kapitel 8 „Public-Key-Verschlüsselung“ und 12 „Digitale Signaturen“ wurden entsprechend erweitert. Auch die Fehler, auf die mich Leserinnen und Leser hingewiesen haben, habe ich beseitigt. Ich bedanke mich herzlich für die Aufmerksamkeit.

Darmstadt, im Dezember 2015

Johannes Buchmann

---

## Vorwort zur fünften Auflage

In der fünften Auflage meiner Einführung in die Kryptographie habe ich die Beweise für die Sicherheit des Lamport-Diffie-Einmalsignaturverfahren und des Merkle-Signaturverfahren erweitert und einen Abschnitt über algebraische Angriffe auf Blockchiffren neu aufgenommen. Es handelt sich dabei um eine Angriffstechnik, die neue Anforderungen an die Konstruktion von kryptographischen Verfahren stellt. Immer wieder erhalte ich Emails von Lesern, die mich auf Fehler hinweisen und Verbesserungsvorschläge machen. Dafür bin ich sehr dankbar und habe versucht, die Anregungen zu berücksichtigen.

Darmstadt, im Oktober 2009

Johannes Buchmann

---

## Vorwort zur vierten Auflage

In der vierten Auflage meiner Einführung in die Kryptographie habe ich auch diesmal den Stand der Forschung im Bereich Faktorisieren und Berechnung diskreter Logarithmen aktualisiert. Neu aufgenommen wurde das Merkle-Signaturverfahren. Dieses Verfahren wurde etwa zeitgleich mit dem RSA-Signaturverfahren erfunden. Nachdem Peter Shor gezeigt hat, dass Quantencomputer das Faktorisierungsproblem und die in der Kryptographie relevanten Diskrete-Logarithmen-Probleme in Polynomzeit lösen können, hat das Merkle-Verfahren neue Relevanz bekommen. Es stellt nämlich eine Alternative zu den heute verwendeten Signaturverfahren dar, die alle unsicher würden, wenn genügend große Quantencomputer gebaut werden können. Außerdem habe ich die Fehler, die mir seit Erscheinen der dritten Auflage bekannt geworden sind, korrigiert. Für die vielen Hinweise, die ich von Lesern erhalten habe, bedanke ich mich sehr.

Darmstadt, im Dezember 2007

Johannes Buchmann

---

## Vorwort zur dritten Auflage

In die dritte Auflage meiner Einführung in die Kryptographie habe ich Aktualisierungen und einige neue Inhalte aufgenommen. Aktualisiert wurde die Diskussion der Sicherheit von Verschlüsselungs- und Signaturverfahren und der Stand der Forschung im Bereich Faktorisieren und Berechnung diskreter Logarithmen. Neu aufgenommen wurde die Beschreibung des Advanced Encryption Standard (AES), des Secure Hash Algorithmus (SHA-1) und des Secret-Sharing-Verfahrens von Shamir. Außerdem habe ich die Fehler, die mir seit Erscheinen der zweiten Auflage bekannt geworden sind, korrigiert. Für die vielen Hinweise, die ich von Lesern erhalten habe, bedanke ich mich sehr.

Darmstadt, im Mai 2003

Johannes Buchmann



---

## 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, Tobias Straub, 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</b>	<b>Grundlagen</b>	<b>1</b>
1.1	Ganze Zahlen	1
1.1.1	Grundbegriffe und Eigenschaften	1
1.1.2	Vollständige Induktion	3
1.1.3	Konvention	4
1.1.4	Teilbarkeit	4
1.1.5	Darstellung ganzer Zahlen	5
1.1.6	Größter gemeinsamer Teiler	7
1.1.7	Zerlegung in Primzahlen	10
1.2	Wahrscheinlichkeit	12
1.2.1	Grundbegriffe	12
1.2.2	Bedingte Wahrscheinlichkeit	14
1.3	Zufallsvariablen	15
1.3.1	Geburtstagsparadox	16
1.4	Algorithmen	17
1.4.1	Grundbegriffe	17
1.4.2	Zustandsbehaftete Algorithmen	18
1.4.3	Probabilitistische Algorithmen	18
1.4.4	Asymptotische Notation	19
1.4.5	Laufzeit von deterministischen Algorithmen	20
1.4.6	Laufzeit von probabilistischen Algorithmen	22
1.4.7	Durchschnittliche Laufzeit	22
1.5	Berechnungsprobleme	22
1.6	Algorithmen für ganze Zahlen	24
1.6.1	Addition, Multiplikation und Division mit Rest	24
1.6.2	Euklidischer Algorithmus	26
1.6.3	Erweiterter euklidischer Algorithmus	29
1.6.4	Analyse des erweiterten euklidischen Algorithmus	31
1.7	Übungen	34

<b>2</b>	<b>Kongruenzen und Restklassenringe</b>	37
2.1	Kongruenzen	37
2.2	Halbgruppen	39
2.3	Gruppen	41
2.4	Restklassenringe	42
2.5	Körper	43
2.6	Division im Restklassenring	43
2.7	Rechenzeit für die Operationen im Restklassenring	44
2.8	Prime Restklassengruppen	45
2.9	Ordnung von Gruppenelementen	47
2.10	Untergruppen	48
2.11	Der kleine Satz von Fermat	50
2.12	Schnelle Exponentiation	50
2.13	Schnelle Auswertung von Potenzprodukten	52
2.14	Berechnung von Elementordnungen	53
2.15	Der Chinesische Restsatz	55
2.16	Zerlegung des Restklassenrings	57
2.17	Bestimmung der Eulerschen $\varphi$ -Funktion	58
2.18	Polynome	59
2.19	Polynome über Körpern	61
2.20	Konstruktion endlicher Körper	63
2.21	Struktur der Einheitengruppe endlicher Körper	66
2.22	Struktur der primen Restklassengruppe nach einer Primzahl	67
2.23	Quadratische Reste	68
2.24	Übungen	69
<b>3</b>	<b>Verschlüsselung</b>	73
3.1	Symmetrische Verschlüsselungsverfahren	73
3.2	Verschiebungsschiffre	75
3.3	Asymmetrische Verschlüsselungsverfahren	76
3.4	Sicherheit von Verschlüsselungsverfahren	77
3.4.1	Angriffsziele	77
3.4.2	Angriffstypen	78
3.5	Alphabete und Wörter	82
3.6	Permutationen	84
3.7	Blockchiffren	85
3.8	Permutationschiffren	85
3.9	Mehrfachverschlüsselung	86
3.10	Verschlüsselungsmodi	87
3.10.1	ECB-Mode	87
3.10.2	CBC-Mode	90
3.10.3	CFB-Mode	94
3.10.4	OFB-Mode	96

3.11	CTR-Mode	99
3.12	Stromchiffren	100
3.13	Typen von Stromchiffren	100
3.14	Rückgekoppelte Schieberegister	101
3.15	Die affine Chiffre	103
3.16	Matrizen und lineare Abbildungen	104
3.16.1	Matrizen über Ringen	104
3.16.2	Produkt von Matrizen mit Vektoren	105
3.16.3	Summe und Produkt von Matrizen	105
3.16.4	Der Matrizenring	106
3.16.5	Determinante	106
3.16.6	Inverse von Matrizen	107
3.16.7	Affin lineare Funktionen	108
3.17	Affin lineare Blockchiffren	109
3.18	Vigenère, Hill- und Permutationschiffre	109
3.19	Kryptoanalyse affin linearer Blockchiffren	110
3.20	Sichere Blockchiffren	111
3.20.1	Konfusion und Diffusion	111
3.20.2	Time-Memory Trade-Off	112
3.20.3	Differentielle Kryptoanalyse	114
3.20.4	Algebraische Kryptoanalyse	114
3.21	Übungen	116
<b>4</b>	<b>Sicherheitsmodelle</b>	<b>119</b>
4.1	Perfekte Geheimhaltung	119
4.2	Das Vernam-One-Time-Pad	123
4.3	Semantische Sicherheit	124
4.4	Chosen-Plaintext-Sicherheit	129
4.5	Chosen-Ciphertext-Sicherheit	131
4.6	Übungen	133
<b>5</b>	<b>Der DES-Algorithmus</b>	<b>135</b>
5.1	Feistel-Chiffren	135
5.2	Der DES-Algorithmus	136
5.2.1	Klartext- und Schlüsselraum	136
5.2.2	Die initiale Permutation	137
5.2.3	Die interne Blockchiffre	137
5.2.4	Die S-Boxen	139
5.2.5	Die Rundenschlüssel	141
5.2.6	Entschlüsselung	142
5.3	Ein Beispiel für DES	142

5.4	Sicherheit des DES	143
5.5	Übungen	144
<b>6</b>	<b>Der AES-Algorithmus</b>	<b>145</b>
6.1	Bezeichnungen	145
6.2	Cipher	146
6.2.1	Identifikation der Bytes mit Elementen von $GF(2^8)$	147
6.2.2	SubBytes	147
6.2.3	ShiftRows	148
6.2.4	MixColumns	149
6.2.5	AddRoundKey	149
6.3	KeyExpansion	150
6.4	Ein Beispiel	151
6.5	InvCipher	152
6.6	Übungen	153
<b>7</b>	<b>Primzahlerzeugung</b>	<b>155</b>
7.1	Probedivision	155
7.2	Der Fermat-Test	157
7.3	Carmichael-Zahlen	157
7.4	Der Miller-Rabin-Test	159
7.5	Zufällige Wahl von Primzahlen	161
7.6	Übungen	162
<b>8</b>	<b>Public-Key Verschlüsselung</b>	<b>165</b>
8.1	Idee	165
8.2	Definition	167
8.2.1	Sicherheit	168
8.3	Das RSA-Verfahren	168
8.3.1	Schlüsselerzeugung	168
8.3.2	Verschlüsselung	169
8.3.3	Entschlüsselung	171
8.3.4	Sicherheit des privaten Schlüssels	172
8.3.5	Auswahl von $p$ und $q$	174
8.3.6	Auswahl von $e$	175
8.3.7	Auswahl von $d$	176
8.3.8	Performanz	176
8.3.9	Multiplikativität	178
8.3.10	Sichere Verwendung	178
8.3.11	Verallgemeinerung	179
8.4	Das Rabin-Verschlüsselungsverfahren	180
8.4.1	Schlüsselerzeugung	181
8.4.2	Verschlüsselung	181

8.4.3	Entschlüsselung	181
8.4.4	Effizienz	182
8.4.5	Sicherheit	182
8.4.6	Ein Chosen-Ciphertext-Angriff	184
8.4.7	Sichere Verwendung	184
8.5	Sicherheitsmodelle	184
8.5.1	Chosen-Plaintext-Sicherheit	184
8.5.2	Chosen-Ciphertext-Sicherheit	186
8.5.3	Sicherheitsbeweise	186
8.6	Diffie-Hellman-Schlüsselaustausch	188
8.6.1	Diskrete Logarithmen	188
8.6.2	Schlüsselaustausch	189
8.6.3	Das Diffie-Hellman-Problem	190
8.6.4	Auswahl von $p$	192
8.6.5	Man-In-The-Middle-Angriff	194
8.6.6	Andere Gruppen	194
8.7	Das ElGamal-Verschlüsselungsverfahren	195
8.7.1	Schlüsselerzeugung	195
8.7.2	Verschlüsselung	196
8.7.3	Entschlüsselung	196
8.7.4	Effizienz	197
8.7.5	ElGamal und Diffie-Hellman	197
8.7.6	Parameterwahl	198
8.7.7	Chosen-Plaintext-Sicherheit	198
8.7.8	Chosen-Ciphertext-Sicherheit	201
8.7.9	Homomorphie	201
8.7.10	Verallgemeinerung	202
8.8	Übungen	202
<b>9</b>	<b>Faktorisierung</b>	<b>205</b>
9.1	Probdivison	205
9.2	Die $p - 1$ -Methode	206
9.3	Das Quadratische Sieb	206
9.3.1	Das Prinzip	207
9.3.2	Bestimmung von $x$ und $y$	207
9.3.3	Auswahl geeigneter Kongruenzen	208
9.3.4	Das Sieb	209
9.4	Analyse des Quadratischen Siebs	211
9.5	Effizienz anderer Faktorisierungsverfahren	213
9.6	Übungen	214

<b>10</b>	<b>Diskrete Logarithmen</b>	217
10.1	Das DL-Problem	217
10.2	Enumeration	218
10.3	Shanks Babystep-Giantstep-Algorithmus	218
10.4	Der Pollard- $\rho$ -Algorithmus	220
10.5	Der Pohlig-Hellman-Algorithmus	223
10.5.1	Reduktion auf Primzahlpotenzordnung	224
10.5.2	Reduktion auf Primzahlordnung	225
10.5.3	Gesamtalgorithmus und Analyse	227
10.6	Index-Calculus	227
10.6.1	Idee	228
10.6.2	Diskrete Logarithmen der Faktorbasiselemente	228
10.6.3	Individuelle Logarithmen	230
10.6.4	Analyse	231
10.7	Andere Algorithmen	231
10.8	Verallgemeinerung des Index-Calculus-Verfahrens	231
10.9	Übungen	232
<b>11</b>	<b>Hashfunktionen und MACS</b>	233
11.1	Hashfunktionen und Kompressionsfunktionen	234
11.2	Geburtsangriff	236
11.3	Kompressionsfunktionen aus Verschlüsselungsfunktionen	237
11.4	Hashfunktionen aus Kompressionsfunktionen	237
11.5	SHA-3	239
11.6	Eine arithmetische Kompressionsfunktion	240
11.7	Message Authentication Codes	241
11.8	Übungen	243
<b>12</b>	<b>Digitale Signaturen</b>	245
12.1	Idee	245
12.2	Definition	246
12.3	Das Lamport-Diffie-Einmal-Signaturverfahren	247
12.3.1	Schlüsselerzeugung	247
12.3.2	Signatur	248
12.3.3	Verifikation	249
12.4	Sicherheit	249
12.4.1	Angriffsziele	249
12.4.2	Angriffstypen	250
12.5	RSA-Signaturen	251
12.5.1	Schlüsselerzeugung	252
12.5.2	Signatur	252
12.5.3	Verifikation	252



12.5.4	Angriffe	253
12.5.5	Signatur von Nachrichten mit Redundanz	254
12.5.6	Signatur mit Hashwert	255
12.5.7	Wahl von $p$ und $q$	256
12.5.8	Sichere Verwendung	256
12.6	Signaturen aus Public-Key-Verfahren	256
12.7	ElGamal-Signatur	257
12.7.1	Schlüsselerzeugung	257
12.7.2	Signatur	257
12.7.3	Verifikation	258
12.7.4	Die Wahl von $p$	258
12.7.5	Die Wahl von $k$	259
12.7.6	Existentielle Fälschungen	259
12.7.7	Performanz	260
12.7.8	Sichere Verwendung	261
12.7.9	Verallgemeinerung	261
12.8	Der Digital Signature Algorithm (DSA)	261
12.8.1	Schlüsselerzeugung	262
12.8.2	Signatur	262
12.8.3	Verifikation	263
12.8.4	Performanz	263
12.8.5	Sicherheit	263
12.9	Das Merkle-Signaturverfahren	264
12.9.1	Initialisierung	265
12.9.2	Schlüsselerzeugung	265
12.9.3	Signatur	266
12.9.4	Verifikation	267
12.9.5	Verbesserungen	268
12.10	Sicherheitsmodelle	269
12.10.1	Grundlagen	269
12.10.2	RSA	272
12.10.3	ElGamal	273
12.10.4	Lamport-Diffie-Einmal-Signatur	273
12.10.5	Merkle-Verfahren	275
12.11	Übungen	277
<b>13</b>	<b>Andere Gruppen</b>	<b>279</b>
13.1	Endliche Körper	279
13.2	Elliptische Kurven	280
13.2.1	Definition	280
13.2.2	Gruppenstruktur	281

13.2.3	Kryptographisch sichere Kurven	282
13.2.4	Vorteile von EC-Kryptographie	282
13.3	Quadratische Formen	283
13.4	Übungen	284
<b>14</b>	<b>Identifikation</b>	<b>285</b>
14.1	Anwendungen	285
14.2	Passwörter	286
14.3	Einmal-Passwörter	287
14.4	Challenge-Response-Identifikation	287
14.4.1	Verwendung von Public-Key-Kryptographie	287
14.4.2	Zero-Knowledge-Beweise	288
14.5	Übungen	290
<b>15</b>	<b>Secret Sharing</b>	<b>293</b>
15.1	Prinzip	293
15.2	Das Shamir-Secret-Sharing-Protokoll	293
15.2.1	Initialisierung	295
15.2.2	Verteilung der Geheimnisteile	295
15.2.3	Rekonstruktion des Geheimnisses	295
15.2.4	Sicherheit	296
15.3	Übungen	296
<b>16</b>	<b>Public-Key-Infrastrukturen</b>	<b>297</b>
16.1	Persönliche Sicherheitsumgebung	297
16.1.1	Bedeutung	297
16.1.2	Implementierung	298
16.1.3	Darstellungsproblem	298
16.2	Zertifizierungsstellen	299
16.2.1	Registrierung	299
16.2.2	Schlüsselerzeugung	299
16.2.3	Zertifizierung	300
16.2.4	Archivierung	300
16.2.5	Personalisierung der PSE	300
16.2.6	Verzeichnisdienst	301
16.2.7	Schlüssel-Update	301
16.2.8	Widerruf von Zertifikaten	302
16.2.9	Zugriff auf ungültige Schlüssel	302
16.3	Zertifikatsketten	302
<b>17</b>	<b>Lösungen der Übungsaufgaben</b>	<b>305</b>
	<b>Literatur</b>	<b>321</b>
	<b>Sachverzeichnis</b>	<b>325</b>