

Bruce Schneier

# Angewandte Kryptographie

Protokolle, Algorithmen und Sourcecode in C

**PEARSON**

**Studium**

ein Imprint von Pearson Education

München • Boston • San Francisco • Harlow, England • Don Mills, Ontario  
Sydney • Mexico City • Madrid • Amsterdam

# Inhaltsverzeichnis

<b>vorwort von wnmieia uime</b>	<b>xiii</b>
Vorwort	xvii
Über den Autor	xxii
Grundlagen	1
1.1 Terminologie	1
1.2 Steganographie	10
1.3 Chiffrierung durch Substitution und Transposition	11
1.4 Einfaches XOR	15
1.5 One-Time-Pads	17
1.6 Computer-Algorithmen	20
1.7 Größenordnungen	20
<b>Teil I Kryptographische Protokolle</b>	<b>23</b>
<b>2 Protokollelemente</b>	<b>25</b>
2.1 Einführung in Protokolle	25
2.2 Kommunikation mit symmetrischer Kryptographie	32
2.3 Einwegfunktionen	34
2.4 Einweg-Hashfunktionen	35
2.5 Kommunikation mit Public-Key-Kryptographie	37
2.6 Digitale Signaturen	41
2.7 Digitale Signaturen mit Verschlüsselung	49
2.8 Generieren von Zufalls- und Pseudozufallsfolgen	52
<b>3 Grundlegende Protokolle</b>	<b>57</b>
3.1 Schlüsselaustausch	57
3.2 Authentifizierung	62
3.3 Authentifizierung und Schlüsselaustausch	67
3.4 Formale Analyse von Protokollen für Authentifizierung und Schlüsselaustausch	77
3.5 Public-Key-Kryptographie mit mehreren Schlüsseln	81
3.6 Secret Splitting	83
3.7 Secret Sharing	84
3.8 Datenbankschutz durch Verschlüsselung	88
<b>4 Weiterführende Protokolle</b>	<b>91</b>
4.1 Zeitstempel	91

4.2	Verdeckter Kanal	95
4.3	Verbindliche digitale Signaturen	97
4.4	Signaturen mit designierter Bestätigung	99
4.5	Signaturen für Stellvertreter	100
4.6	Signaturen für Gruppen	101
4.7	Fail-stop-Signaturen	102
4.8	Berechnungen mit verschlüsselten Daten	103
4.9	Bit Commitment	104
4.10	Faires Münzenwerfen	107
4.11	Mentales Pokern	110
4.12	Einweg-Akkumulatoren	114
4.13	Alles-oder-Nichts-Geheimnisenthüllung	115
4.14	Schlüssel hinterlegung	116
	<b>Anspruchsvolle Protokolle</b>	<b>121</b>
5.1	Zero-Knowledge-Beweise	121
5.2	Zero-Knowledge-Identitätsbeweise	129
5.3	Blinde Signaturen	133
5.4	Auf Identität basierende Public-Key-Kryptographie	137
5.5	Oblivious Transfer	138
5.6	Nicht eindeutige Signaturen	140
5.7	Geichzeitige Vertragsunterzeichnung	140
5.8	Bestätigung elektronischer Post	145
5.9	Gleichzeitiger Geheimnisaustausch	147
<b>6</b>	<b>Ausgefallene Protokolle</b>	<b>149</b>
6.1	Sichere Wahlen	149
6.2	Sichere Berechnungen mit mehreren Parteien	159
6.3	Anonyme Nachrichtenverbreitung	163
6.4	Digitales Geld	165
	<b>Teil II Kryptographische Techniken</b>	<b>175</b>
<b>7</b>	<b>Schlüssellänge</b>	<b>177</b>
7.1	Symmetrische Schlüssellänge	177
7.2	Länge öffentlicher Schlüssel	185
7.3	Längenvergleich von öffentlichen und symmetrischen Schlüsseln	194
7.4	Geburtsangriffe gegen Einweg-Hashfunktionen	194
7.5	Wie lang sollte ein Schlüssel sein?	195
7.6	Wichtiger Hinweis	197
<b>8</b>	<b>Schlüsselverwaltung</b>	<b>199</b>
8.1	Schlüsselerzeugung	200

8.2	Nichtlineare Schlüsselräume	206
8.3	Übermittlung von Schlüsseln	207
8.4	Verifizierung von Schlüsseln	209
8.5	Verwendung von Schlüsseln	211
8.6	Aktualisierung von Schlüsseln	212
8.7	Speicherung von Schlüsseln	213
8.8	Sicherungskopien von Schlüsseln	214
8.9	Kompromittierte Schlüssel	215
8.10	Geltungsdauer von Schlüsseln	216
8.11	Vernichtung von Schlüsseln	218
8.12	Schlüsselverwaltung bei Public-Key-Kryptographie	219
<b>9</b>	<b>Algorithmenarten und Betriebsmodi</b>	<b>223</b>
9.1	Electronic-Codebook-Modus	223
9.2	Block Replay	225
9.3	Cipher Block Chaining	227
9.4	Stromchiffrierungen	232
9.5	Selbstsynchronisierende Stromchiffrierungen	234
9.6	Cipher-Feedback-Modus	235
9.7	Synchrone Stromchiffrierungen	238
9.8	Output-Feedback-Modus	240
9.9	Counter-Modus	243
9.10	Weitere Modi für Blockchiffrierungen	244
9.11	Wahl eines Chiffriermodus	246
9.12	Verschränkung	248
9.13	Block- und Stromchiffrierungen	249
<b>10</b>	<b>Einsatz der Algorithmen</b>	<b>251</b>
10.1	Auswahl eines Algorithmus	252
10.2	Public-Key- und symmetrische Kryptographie	254
10.3	Verschlüsselung von Kommunikationskanälen	255
10.4	Verschlüsselung gespeicherter Daten	260
10.5	Hardware- und Software-Verschlüsselung	263
10.6	Kompression, Kodierung und Verschlüsselung	266
10.7	Erkennen von Verschlüsselung	267
10.8	Verbergen von Chiffretext in Chiffretext	268
10.9	Zerstören von Informationen	269
<b>Teil III</b>	<b>Kryptographische Algorithmen</b>	<b>271</b>
<b>11</b>	<b>Mathematische Grundlagen</b>	<b>273</b>
11.1	Informationstheorie	273
11.2	Komplexitätstheorie	278
11.3	Zahlentheorie	283

11.4	Primfaktorzerlegung	299
11.5	Erzeugung von Primzahlen	302
11.6	Diskrete Logarithmen in endlichen Körpern	306
<b>12</b>	<b>Data Encryption Standard (DES)</b>	<b>309</b>
12.1	Hintergrund	309
12.2	Beschreibung von DES	315
12.3	Sicherheit von DES	325
12.4	Differentielle und lineare Kryptanalyse	332
12.5	Die tatsächlichen Entwurfskriterien	341
12.6	Varianten von DES	342
12.7	Wie sicher ist DES heutzutage?	349
<b>13</b>	<b>Weitere Blockchiffrierungen</b>	<b>351</b>
13.1	Lucifer	351
13.2	Madryga	352
13.3	NewDES	355
13.4	FEAL	356
13.5	REDOC	361
13.6	LOKI	363
13.7	Khufu und Khafre	366
13.8	RC2	368
13.9	IDEA	370
13.10	MMB	377
13.11	CA-1.1	379
13.12	Skipjack	380
<b>14</b>	<b>Noch mehr Blockchiffrierungen</b>	<b>383</b>
14.1	GOST	383
14.2	CAST	386
14.3	Blowfish	388
14.4	SAFER	392
14.5	3-Way	395
14.6	Crab	395
14.7	SXAL8/MBAL	397
14.8	RC5	397
14.9	Weitere Blockalgorithmen	399
14.10	Theorie des Entwurfs von Blockchiffrierungen	400
14.11	Verwendung von Einweg-Hashfunktionen	406
14.12	Wahl eines Blockalgorithmus	409
<b>15</b>	<b>Kombination von Blockchiffrierungen</b>	<b>411</b>
15.1	Doppelte Verschlüsselung	411
15.2	Dreifachverschlüsselung	413
15.3	Verdopplung der Blocklänge	418

15.4	Weitere Verfahren für Mehrfachverschlüsselung	419
15.5	Schlüsselverkürzung in CDMF	421
15.6	Whitening	422
15.7	Kaskadierung mehrerer Blockalgorithmen	423
15.8	Kombination mehrerer Blockalgorithmen	424
<b>16</b>	<b>Pseudozufallsfolgeneratoren und Stromchiffrierungen</b>	<b>425</b>
16.1	Lineare Kongruenzgeneratoren	425
16.2	Lineare Schieberegister mit Rückkopplung	429
16.3	Entwurf und Analyse von Stromchiffrierungen	435
16.4	Stromchiffrierungen mit LFSRs	437
16.5	A5	446
16.6	Hughes XPD/KPD	447
16.7	Nanoteq	448
16.8	Rambutan	448
16.9	Additive Generatoren	449
16.10	Gifford	451
16.11	Algorithmus M	452
16.12	PKZIP	453
<b>17</b>	<b>Weitere Stromchiffrierungen und echte Zufallsfolgeneratoren</b>	<b>455</b>
17.1	RC4	455
17.2	SEAL	456
17.3	WAKE	459
17.4	Schieberegister mit Rückkopplung durch Übertrag	461
17.5	Stromchiffrierungen mit FCSRs	468
17.6	Schieberegister mit nichtlinearer Rückkopplung	471
17.7	Weitere Stromchiffrierungen	473
17.8	Systemtheoretischer Ansatz zum Entwurf von Stromchiffrierungen	475
17.9	Komplexitätstheoretischer Ansatz zum Entwurf von Stromchiffrierungen	476
17.10	Weitere Ansätze zum Entwurf von Stromchiffrierungen	478
17.11	Kaskadierung von Stromchiffrierungen	480
17.12	Wahl einer Stromchiffrierung	480
17.13	Erzeugung mehrerer Ströme mit einem einzigem Pseudozufallszahlengenerator	481
17.14	Echte Zufallsfolgeneratoren	482
<b>18</b>	<b>Einweg-Hashfunktionen</b>	<b>491</b>
18.1	Hintergrund	491
18.2	Snefru	493
18.3	N-Hash	495
18.4	MD4	498

## Inhaltsverzeichnis

18.5	MD5	498
18.6	MD2	503
18.7	Secure Hash Algorithm (SHA)	504
18.8	RIPE-MD	508
18.9	HAVAL	508
18.10	Weitere Einweg-Hashfunktionen	508
18.11	Einweg-Hashfunktionen mit symmetrischen Blockalgorithmen	509
18.12	Einsatz von Public-Key-Algorithmen	519
18.13	Wahl einer Einweg-Hashfunktion	519
18.14	Message Authentication Codes	520
<b>19</b>	<b>Public-Key-Algorithmen</b>	<b>525</b>
19.1	Hintergrund	525
19.2	Rucksackalgorithmen	526
19.3	RSA	531
19.4	Pohlig-Hellman	541
19.5	Rabin	541
19.6	ElGamal	543
19.7	McEliece	546
19.8	Kryptosysteme auf Basis elliptischer Kurven	548
19.9	LUC	549
19.10	Public-Key-Kryptosysteme mit endlichen Automaten	550
<b>20</b>	<b>Public-Key-Algorithmen für digitale Signaturen</b>	<b>553</b>
20.1	Digital Signature Algorithm (DSA)	553
20.2	Varianten von DSA	565
20.3	Algorithmus für digitale Signaturen mit GOST	566
20.4	Signaturverfahren mit diskreten Logarithmen	567
20.5	Ong-Schnorr-Shamir	570
20.6	ESIGN	570
20.7	Zelluläre Automaten	572
20.8	Weitere Public-Key-Algorithmen	572
<b>21</b>	<b>Identifizierungsverfahren</b>	<b>575</b>
21.1	Feige-Fiat-Shamir	575
21.2	Guillou-Quisquater	581
21.3	Schnorr	583
21.4	Umwandlung von Identifizierungsverfahren in Signaturverfahren	585
<b>22</b>	<b>Algorithmen für den Schlüsselaustausch</b>	<b>587</b>
22.1	Diffie-Hellman	587
22.2	Station-to-Station-Protokoll	590
22.3	Three-Pass-Protokoll von Shamir	590
22.4	COMSET	592
22.5	Encrypted Key Exchange	592

22.6	Fortified Key Negotiation	597
22.7	Schlüsselverteilung auf Konferenzen und geheimer Rundruf	598
<b>23</b>	<b>Spezielle Algorithmen für Protokolle</b>	<b>601</b>
23.1	Public-Key-Kryptographie mit mehreren Schlüsseln	601
23.2	Secret-Sharing-Algorithmen	602
23.3	Verdeckter Kanal	606
23.4	Verbindliche digitale Signaturen	612
23.5	Signaturen mit designierter Bestätigung	615
23.6	Rechnen mit chiffrierten Daten	616
23.7	Faires Münzenwerfen	617
23.8	Einweg-Akkumulatoren	619
23.9	Alles-oder-Nichts-Geheimnisenenthüllung	620
23.10	Faire und ausfallsichere Kryptosysteme	623
23.11	Zero-Knowledge-Beweise des Wissensstands	624
23.12	Blinde Signaturen	626
23.13	Oblivious Transfer	627
23.14	Sichere Berechnungen mit mehreren Parteien	627
23.15	Probabilistische Verschlüsselung	629
23.16	Quantenkryptographie	632

## Teil IV Kryptographie in der Praxis 635

<b>24</b>	<b>Implementierungsbeispiele</b>	<b>637</b>
24.1	IBM-Protokoll zur Verwaltung geheimer Schlüssel	637
24.2	MITRENET	638
24.3	ISDN	639
24.4	STU-III	641
24.5	Kerberos	642
24.6	KryptoKnight	649
24.7	SESAME	650
24.8	Common Cryptographic Architecture von IBM	650
24.9	ISO Authentication Framework	652
24.10	Privacy-Enhanced Mail (PEM)	656
24.11	Message Security Protocol (MSP)	663
24.12	Pretty Good Privacy (PGP)	664
24.13	Smart-Cards	667
24.14	Public-Key Cryptography Standards (PKCS)	668
24.15	Universal Electronic Payment System (UEPS)	670
24.16	Clipper	672
24.17	Capstone	675
24.18	AT&T Model 3600 Telephone Security Device (TSD)	675



25	Politik	677
25.1	National Security Agency (NSA)	677
25.2	National Computer Security Center (NCSC)	679
25.3	National Institute of Standards and Technology (NIST)	680
25.4	RSA Data Security, Inc.	684
25.5	Public Key Partners	684
25.6	International Association for Cryptologic Research (IACR)	686
25.7	RACE Integrity Primitives Evaluation (RIPE)	686
25.8	Conditional Access for Europe (CAFE)	686
25.9	ISO/IEC 9979	687
25.10	Berufsverbände, Bürgerrechtsgruppen und Industrievereinigungen	688
25.11	sci.crypt	689
25.12	Cypherpunks	690
25.13	Patente	690
25.14	Ausfuhrbestimmungen der USA	691
25.15	Einfuhr und Ausfuhr von Kryptographie in anderen Staaten	698
25.16	Rechtliche Fragen	699
	 Nachwort von Matt Blaze	 701
	 TeilV Sourcecode	 705
	 Literaturverzeichnis	 757
	 Stichwortverzeichnis	 825