

Auf einen Blick

Über den Autor	7
Einleitung	21
Teil I: Verschlüsseln	29
Kapitel 1: Sicherheit in Zeiten des Internet	31
Kapitel 2: Klassische Verschlüsselung	37
Kapitel 3: Public-Key-Verschlüsselung	51
Teil II: Kryptische Mathematik	61
Kapitel 4: Menge, Relation, Abbildung	63
Kapitel 5: Teilbarkeit und Modulo-Rechnung	67
Kapitel 6: Gruppe	77
Teil III: Kryptografische Verfahren	89
Kapitel 7: RSA: Korrektheit und Schlüsselerzeugung	91
Kapitel 8: Diffie-Hellman, ElGamal und Shamir	99
Kapitel 9: AES-Verschlüsselungsverfahren	111
Kapitel 10: AES-Mathematik: Rechnen in einem Körper	123
Kapitel 11: Diffie-Hellman-Schlüsselvereinbarung mit elliptischer Kurve	133
Teil IV: Berechnungsverfahren	141
Kapitel 12: Python-Einführung	143
Kapitel 13: Erweiterter euklidischer Algorithmus	149
Kapitel 14: Schnelle Exponentiation und Primzahltest	159
Kapitel 15: Chinesischer Restsatz	171
Kapitel 16: Elliptische Kurven implementieren	179
Kapitel 17: Kryptografische Verfahren implementieren	187
Teil V: Authentifizieren	193
Kapitel 18: Kryptografische Hashfunktion	195
Kapitel 19: Authentizität und Integrität von Nachrichten	207
Kapitel 20: Digitale Signatur	215
Kapitel 21: Teilnehmer-Authentifizierung	225
Teil VI: Sicherheit	237
Kapitel 22: Angriffe auf das RSA-Verfahren	239
Kapitel 23: Faktorisierungsangriff	251
Kapitel 24: Angriffe auf Hashfunktionen	261
Teil VII: Zufall	267
Kapitel 25: Zufallsbits und Pseudozufallsbits	269
Kapitel 26: Kryptografisch sichere Zufallsbits	275

Teil VIII: Anwendungen	281
Kapitel 27: Zertifizierte Sicherheit.....	283
Teil IX: Top-Ten-Teil	291
Kapitel 28: Die glorreichen Sieben.....	293
Anhang	307
Anhang A: Zum Weiterlesen.....	309
Anhang B: Lösungen zu den Übungsaufgaben.....	311
Literaturverzeichnis	323
Abbildungsverzeichnis	325
Stichwortverzeichnis	329

Inhaltsverzeichnis

Über den Autor	7
Einleitung	21
Über dieses Buch	21
Konventionen in diesem Buch	22
Was Sie nicht lesen müssen	22
Törichte Annahmen über den Leser	22
Wie dieses Buch aufgebaut ist	23
Teil I: Verschlüsseln	23
Teil II: Kryptische Mathematik	23
Teil III: Kryptografische Verfahren	24
Teil IV: Berechnungsverfahren	24
Teil V: Authentifizieren	24
Teil VI: Sicherheit	24
Teil VII: Zufall	25
Teil VIII: Anwendungen	25
Teil IX: Top-Ten-Teil	25
Anhänge	25
Symbole, die in diesem Buch verwendet werden	25
Wie es weitergeht	26
TEIL I	
VERSCHLÜSSELN	29
Kapitel 1	
Sicherheit in Zeiten des Internet	31
Authentizität	32
Zertifikat	32
Vertraulichkeit und Integrität	34
Sicher surfen mit https	35
Kapitel 2	
Klassische Verschlüsselung	37
Geheimsprache	37
Verschlüsseln wie Caesar	39
Kryptoanalyse	42
Substitutions-Verschlüsselung	43
Vigenère-Verschlüsselung	45
Vigenère knacken	45
Vernam-Verschlüsselung	46
Verschlüsseln von Bits	48

Kapitel 3	
Public-Key-Verschlüsselung	51
RSA-Verschlüsselung.....	52
Schlüssel erzeugen.....	54
Ver- und Entschlüsseln.....	56
Sicherheit.....	57
TEIL II	
KRYPTISCHE MATHEMATIK	61
Kapitel 4	
Menge, Relation, Abbildung	63
Nur ganz kurz.....	63
Wozu brauchen wir das?.....	64
Was noch kommt.....	65
Kapitel 5	
Teilbarkeit und Modulo-Rechnung	67
Teilbarkeit.....	67
Miteinander teilen.....	67
Ist null durch null teilbar?.....	68
Der Teiler und das Ganze.....	69
Primzahlen.....	71
Modulo-Rechnung.....	72
Schubladendenken.....	72
Modulo n rechnen heißt einfach rechnen.....	74
Kapitel 6	
Gruppe	77
Gruppenaxiome.....	77
Elemente verknüpfen.....	77
Auf halbem Weg zur Gruppe.....	79
Und nun zur Gruppe.....	80
Die Gruppe \mathbb{Z}_n^*	81
Gruppentheorie.....	82
Untergruppe.....	82
Erzeugendes Element.....	83
Ordnung.....	84
Zyklische Gruppe.....	84
Starke Primzahl.....	87
TEIL III	
KRYPTOGRAFISCHE VERFAHREN	89
Kapitel 7	
RSA: Korrektheit und Schlüsselerzeugung	91
Sätze von Euler und Fermat.....	91
Satz von Euler.....	91

Satz von Fermat.....	92
Modifizierter Satz von Euler.....	93
Korrektheit des RSA-Verfahrens.....	94
Öffentlichen und privaten Schlüssel erzeugen.....	94
Multiplikativ inverses Element berechnen.....	95
Sicherheit.....	96

Kapitel 8

Diffie-Hellman, ElGamal und Shamir..... 99

Diffie-Hellman-Schlüsselvereinbarung.....	99
Protokoll.....	100
Auswahl von g	100
Auswahl von p	101
Sicherheit.....	102
ElGamal-Verschlüsselung.....	103
Prinzip.....	103
Realisierung.....	104
Sicherheit.....	105
Shamirs No-Key-Verschlüsselung.....	107
Idee.....	107
Implementierung.....	107
Sicherheit.....	108

Kapitel 9

AES-Verschlüsselungsverfahren..... 111

Verschlüsseln.....	112
AES-Verschlüsselung.....	112
Entschlüsseln.....	114
Rundenschlüssel erzeugen.....	116
Entwurfskriterien.....	118
Betriebsarten bei Block-Verschlüsselung.....	118

Kapitel 10

AES-Mathematik: Rechnen in einem Körper..... 123

Ring und Körper.....	123
Ring.....	124
Ring mit Eins.....	125
Körper.....	125
Erweiterungskörper \mathbb{F}_{2^8}	125
Addition und Multiplikation im Erweiterungskörper \mathbb{F}_{2^8}	126
Polynome aus \mathbb{F}_{2^8} als Bitvektoren darstellen.....	127
Bitvektoren als Bytes hexadezimal darstellen.....	129

Kapitel 11

Diffie-Hellman-Schlüsselvereinbarung mit elliptischer Kurve..... 133

Elliptische Kurven.....	134
Punkte verknüpfen.....	135

14 Inhaltsverzeichnis

Gruppenstruktur von E	136
Berechnung des Schnittpunktes.....	136
Elliptische Kurven über endlichen Körpern.....	138
TEIL IV	
BERECHNUNGSVERFAHREN.....	141
Kapitel 12	
Python-Einführung.....	143
Anweisungen.....	143
Wertzuweisung.....	143
Bedingte Anweisungen.....	144
Programmschleifen.....	144
Funktionen.....	145
Klassen und Objekte.....	146
Python-Module.....	147
Kapitel 13	
Erweiterter euklidischer Algorithmus.....	149
Größten gemeinsamen Teiler berechnen.....	149
Erweiterter euklidischer Algorithmus.....	152
Rekursive Version.....	154
Multiplikativ inverses Element modulo n berechnen.....	156
Implementierung.....	157
Kapitel 14	
Schnelle Exponentiation und Primzahltest.....	159
Schnelle Exponentiation.....	159
Idee.....	159
Programm.....	160
Primzahltest.....	161
Verteilung der Primzahlen.....	161
Klassische Methode.....	162
Fermat-Test.....	162
Miller-Rabin-Test.....	164
Zufällige Primzahlen.....	167
Kapitel 15	
Chinesischer Restsatz.....	171
Problem.....	172
Berechnung.....	172
Implementierung.....	174
Chinesischer-Restsatz-Algorithmus.....	175
RSA: Chinesisch entschlüsseln.....	175

Kapitel 16	
Elliptische Kurven implementieren	179
Klasse EcPoint.....	180
Klasse ModInt.....	182
Standard-Punkt auf Standard-Kurve.....	184
Kapitel 17	
Kryptografische Verfahren implementieren	187
RSA-Schlüssel erzeugen	187
Diffie-Hellman-Schlüssel vereinbaren	189
TEIL V	
AUTHENTIFIZIEREN	193
Kapitel 18	
Kryptografische Hashfunktion	195
Hashfunktion.....	195
Kryptografische Sicherheit.....	197
Kryptografische Hashfunktionen in der Praxis	198
Der SHA-1-Hashalgorithmus.....	199
Ablauf des Verfahrens.....	200
Der SHA-256-Hashalgorithmus.....	202
Ablauf des Verfahrens.....	203
Kapitel 19	
Authentizität und Integrität von Nachrichten	207
Authentizität und Integrität bei symmetrischer Verschlüsselung.....	207
Authentisierte Verschlüsselung im GCM-Modus.....	208
Ein- und Ausgabewerte beim Verschlüsseln.....	209
Ein- und Ausgabewerte beim Entschlüsseln.....	210
Authentisierung mittels Hashfunktion	211
Hash-Keyed Message Authentication Code (HMAC).....	211
Kapitel 20	
Digitale Signatur	215
Eigenschaften einer Unterschrift.....	215
RSA-Signatur.....	216
Sicherheitsprobleme.....	217
Hashwert signieren.....	218
Eigenschaften der RSA-Signatur	218
Der Digitale-Signatur-Algorithmus – DSA.....	219
Korrektheit.....	222
Sicherheit	222

Kapitel 21

Teilnehmer-Authentifizierung **225**

- Isomorphe Graphen 227
- Bit-Commitment 229
 - Eine Münze werfen 229
 - Sich committen 229
 - Sicherheit des Protokolls 230
 - Münzwurf telefonisch 231
- Teilnehmer-Authentifizierung 232
 - Zero-Knowledge-Eigenschaft 232
- Fiat-Shamir-Protokoll 233
 - Bit-Commitment-Protokoll 233
 - Sicherheit 233
 - Teilnehmer-Authentifizierung 235
 - Zero-Knowledge-Eigenschaft 235

TEIL VI

SICHERHEIT **237**

Kapitel 22

Angriffe auf das RSA-Verfahren **239**

- Faktorisieren mithilfe von $\varphi(n)$ 240
- Low-Exponent-Angriff auf das RSA-Verfahren 241
 - Implementierung 242
- Klartext-Aufbereitung 245
- Replay-Angriff 247
- Seitenkanal-Angriff 248

Kapitel 23

Faktorisierungsangriff **251**

- Idee 251
- Quadratisches Sieb 252
 - Sieb 253
 - Auswahl von Exponentenvektoren 255
- Die $p-1$ -Methode 256
 - Idee 256
 - Implementierung 257
 - Programm 258

Kapitel 24

Angriffe auf Hashfunktionen **261**

- Passwort-Dateien angreifen 261
 - Angriff mit roher Gewalt 262
 - Wörterbuchangriff 262
- Geeignete Hashalgorithmen 263
- Zum Geburtstag ein Angriff 263

TEIL VII	
ZUFALL	267
Kapitel 25	
Zufallsbits und Pseudozufallsbits	269
Zufallszahlen erzeugen.....	270
Zufallsbits mit rückgekoppeltem Schieberegister.....	270
Linear rückgekoppeltes Schieberegister.....	271
Kryptografische (Un-)Sicherheit.....	272
Kapitel 26	
Kryptografisch sichere Zufallsbits	275
Startwert wählen.....	275
Pseudozufallsbits per Hashfunktion.....	276
Blum-Blum-Shub-Zufallsbits.....	276
Algorithmus.....	277
Implementierung.....	277
Sicherheit.....	278
Blum-Micali Zufallsbits.....	279
Algorithmus.....	279
Implementierung.....	279
Sicherheit.....	280
TEIL VIII	
ANWENDUNGEN	281
Kapitel 27	
Zertifizierte Sicherheit	283
TLS - Daten sicher transportieren.....	284
Ablauf des TLS-Handshakes.....	285
Zertifikat - Echtheit garantiert.....	286
E-Mails verschlüsseln und signieren.....	288
TEIL IX	
TOP-TEN-TEIL	291
Kapitel 28	
Die glorreichen Sieben	293
Die 7 verrücktesten Dinge.....	293
Primzahltest.....	293
Diffie-Hellman-Schlüsselvereinbarung.....	294
Public-Key-Verschlüsselung.....	294
Shamirs No-Key-Verschlüsselung.....	295
Nichtunterscheidbarkeit.....	295
Bit-Commitment.....	295
Zero-Knowledge-Authentifizierung.....	296
Die 7 bedeutendsten Anwendungszwecke.....	296
Vertraulichkeit.....	296

18 Inhaltsverzeichnis

Integrität.....	297
Authentizität.....	297
Verbindlichkeit.....	297
Festlegung.....	298
Anonymität.....	298
Kooperation.....	298
Die 7 elementarsten Berechnungsverfahren.....	298
Bitweise Addition modulo 2.....	299
Schnelle modulare Exponentiation.....	299
Größter gemeinsamer Teiler.....	299
Erweiterter euklidischer Algorithmus.....	299
Primzahltest.....	300
Chinesischer Restsatz.....	300
Punkte einer elliptischen Kurve verknüpfen.....	300
Die 7 wichtigsten Einwegfunktionen.....	300
Faktorisierung.....	300
Problem des diskreten Logarithmus.....	301
Problem des diskreten Logarithmus elliptischer Kurven.....	301
Wurzeln modulo n ziehen.....	302
Graphisomorphismus.....	302
Kryptografische Hashfunktion invertieren.....	302
AES-Known-Plaintext-Angriff.....	303
Die 7 häufigsten Angriffe.....	303
Brute-Force-Angriff.....	303
Ciphertext-Only-Angriff.....	303
Known-Plaintext-Angriff.....	304
Man-in-the-Middle-Angriff.....	304
Geburtstagsangriff.....	304
Replay-Angriff.....	305
Seitenkanal-Angriff.....	305
ANHANG.....	307
Anhang A: Zum Weiterlesen.....	309
Anhang B: Lösungen zu den Übungsaufgaben.....	311
Kapitel 2.....	311
Kapitel 4.....	311
Kapitel 5.....	311
Kapitel 6.....	312
Kapitel 7.....	313
Kapitel 8.....	313
Kapitel 10.....	314
Kapitel 11.....	315
Kapitel 13.....	315
Kapitel 14.....	316
Kapitel 15.....	317

Kapitel 16.....	317
Kapitel 18.....	318
Kapitel 20.....	318
Kapitel 22.....	319
Kapitel 23.....	319
Kapitel 25.....	320
Kapitel 26.....	321
Literaturverzeichnis.....	323
Abbildungsverzeichnis.....	325
Stichwortverzeichnis.....	329