



Auf einen Blick

Über den Autor	7
Einleitung	19
Teil I: Verschlüsseln	25
Kapitel 1: Sicherheit in Zeiten des Internet	27
Kapitel 2: Klassische Verschlüsselung	33
Kapitel 3: Public-Key-Verschlüsselung	47
Teil II: Kryptische Mathematik	57
Kapitel 4: Menge, Relation, Abbildung	59
Kapitel 5: Teilbarkeit und Modulo-Rechnung	63
Kapitel 6: Gruppe	73
Teil III: Kryptografische Verfahren	85
Kapitel 7: RSA: Korrektheit und Schlüsselerzeugung	87
Kapitel 8: Diffie-Hellman, ElGamal und Shamir	95
Kapitel 9: AES-Verschlüsselungsverfahren	105
Kapitel 10: AES-Mathematik: Rechnen in einem Körper	117
Kapitel 11: Diffie-Hellman-Schlüsselvereinbarung mit elliptischer Kurve	127
Teil IV: Berechnungsverfahren	135
Kapitel 12: Python-Einführung	137
Kapitel 13: Erweiterter euklidischer Algorithmus	145
Kapitel 14: Schnelle Exponentiation und Primzahltest	155
Kapitel 15: Chinesischer Restsatz	167
Kapitel 16: Elliptische Kurven implementieren	175
Kapitel 17: Kryptografische Verfahren implementieren	183
Teil V: Authentifizieren	189
Kapitel 18: Kryptografische Hashfunktion	191
Kapitel 19: Authentizität und Integrität von Nachrichten	199
Kapitel 20: Teilnehmer-Authentifizierung	209
Teil VI: Sicherheit	221
Kapitel 21: Angriffe auf das RSA-Verfahren	223
Kapitel 22: Faktorisierungsangriff	235
Kapitel 23: Angriffe auf Hashfunktionen	243
Teil VII: Zufall	249
Kapitel 24: Zufallsbits und Pseudozufallsbits	251
Kapitel 25: Kryptografisch sichere Zufallsbits	257





10 Auf einen Blick

Teil VIII: Anwendungen	263
Kapitel 26: Zertifizierte Sicherheit	265
Teil IX: Der Top-Ten-Teil	273
Kapitel 27: 10/2 Mal die glorreichen Sieben	275
Anhänge	289
Anhang A: Zum Weiterlesen	289
Anhang B: Lösungen zu den Übungsaufgaben	291
Literaturverzeichnis	297
Stichwortverzeichnis	298





Inhaltsverzeichnis

Über den Autor	7
Einleitung	19
Über dieses Buch	19
Konventionen in diesem Buch	20
Was Sie nicht lesen müssen	20
Törichte Annahmen über den Leser	20
Wie dieses Buch aufgebaut ist	21
Teil I: Verschlüsseln	21
Teil II: Kryptische Mathematik	21
Teil III: Kryptografische Verfahren	21
Teil IV: Berechnungsverfahren	22
Teil V: Authentifizieren	22
Teil VI: Sicherheit	22
Teil VII: Zufall	22
Teil VIII: Anwendungen	23
Teil IX: Top-Ten-Teil	23
Anhänge	23
Symbole, die in diesem Buch verwendet werden	23
Wie es weitergeht	23
TEIL I	
VERSCHLÜSSELN	25
Kapitel 1	
Sicherheit in Zeiten des Internet	27
Authentizität	28
Zertifikat	28
Vertraulichkeit und Integrität	30
Verschlüsselung	30
Kapitel 2	
Klassische Verschlüsselung	33
Geheimsprache	33
Verschlüsseln wie Caesar	35
Kryptoanalyse	38
Substitutions-Verschlüsselung	40
Vigenère-Verschlüsselung	41
Vigenère knacken	41
Vernam-Verschlüsselung	42
Verschlüsseln von Bits	44





12 Inhaltsverzeichnis

Kapitel 3	
Public-Key-Verschlüsselung	47
RSA-Verschlüsselung	48
Schlüssel erzeugen	50
Ver- und Entschlüsseln	52
Sicherheit	53
TEIL II	
KRYPTISCHE MATHEMATIK	57
Kapitel 4	
Menge, Relation, Abbildung	59
Nur ganz kurz	59
Wozu brauchen wir das?	60
Was noch kommt	60
Kapitel 5	
Teilbarkeit und Modulo-Rechnung	63
Teilbarkeit	63
Miteinander teilen	63
Ist null durch null teilbar?	64
Der Teiler und das Ganze	65
Primzahlen	67
Modulo-Rechnung	68
Schubladendenken	68
Modulo n rechnen heißt einfach rechnen	70
Kapitel 6	
Gruppe	73
Gruppenaxiome	73
Elemente verknüpfen	73
Auf halbem Weg zur Gruppe	75
Und nun zur Gruppe	76
Die Gruppe \mathbb{Z}_n^*	77
Gruppentheorie	78
Untergruppe	78
Erzeugendes Element	79
Ordnung	80
Zyklische Gruppe	80
Starke Primzahl	83





Inhaltsverzeichnis 13

TEIL III	
KRYPTOGRAFISCHE VERFAHREN	85
Kapitel 7	
RSA: Korrektheit und Schlüsselerzeugung	87
Sätze von Euler und Fermat	87
Satz von Euler	87
Satz von Fermat	88
Modifizierter Satz von Euler	89
Korrektheit des RSA-Verfahrens	90
Öffentlichen und privaten Schlüssel erzeugen	90
Multiplikativ inverses Element berechnen	90
Sicherheit	92
Kapitel 8	
Diffie-Hellman, ElGamal und Shamir	95
Diffie-Hellman-Schlüsselvereinbarung	95
Protokoll	96
Auswahl von g	96
Auswahl von p	97
Sicherheit	98
ElGamal-Verschlüsselung	99
Prinzip	99
Realisierung	99
Sicherheit	100
Shamirs No-Key-Verschlüsselung	102
Idee	103
Implementierung	103
Kapitel 9	
AES-Verschlüsselungsverfahren	105
Verschlüsseln	106
Entschlüsseln	109
Rundenschlüssel erzeugen	110
Entwurfskriterien	113
Betriebsarten bei Block-Verschlüsselung	113
Kapitel 10	
AES-Mathematik: Rechnen in einem Körper	117
Ring und Körper	117
Ring	118
Ring mit Eins	119
Körper	119
Erweiterungskörper \mathbb{F}_{2^8}	120
Addition und Multiplikation im Erweiterungskörper \mathbb{F}_{2^8}	120
Polynome aus \mathbb{F}_{2^8} als Bitvektoren darstellen	121
Bitvektoren als Bytes hexadezimal darstellen	123





14 Inhaltsverzeichnis

Kapitel 11	
Diffie-Hellman-Schlüsselvereinbarung mit elliptischer Kurve	127
Elliptische Kurven	128
Punkte verknüpfen	129
Gruppenstruktur von E	130
Berechnung des Schnittpunktes	130
Elliptische Kurven über endlichen Körpern	132
TEIL IV	
BERECHNUNGSVERFAHREN	135
Kapitel 12	
Python-Einführung	137
Anweisungen	137
Wertzuweisung	137
Bedingte Anweisungen	138
Programmschleifen	138
Funktionen	139
Klassen und Objekte	140
Python-Module	141
Kapitel 13	
Erweiterter euklidischer Algorithmus	145
Größten gemeinsamen Teiler berechnen	145
Erweiterter euklidischer Algorithmus	148
Rekursive Version	150
Multiplikativ inverses Element modulo n berechnen	153
Implementierung	153
Kapitel 14	
Schnelle Exponentiation und Primzahltest	155
Schnelle Exponentiation	155
Idee	155
Programm	156
Primzahltest	157
Verteilung der Primzahlen	157
Klassische Methode	158
Fermat-Test	158
Miller-Rabin-Test	160
Zufällige Primzahlen	163
Kapitel 15	
Chinesischer Restsatz	167
Problem	168
Berechnung	168





Inhaltsverzeichnis 15

Implementierung.....	170
RSA: Chinesisch entschlüsseln	171

Kapitel 16 **Elliptische Kurven implementieren..... 175**

Klasse <i>EcPoint</i>	176
Klasse <i>ModInt</i>	178
Standard-Punkt auf Standard-Kurve.....	180

Kapitel 17 **Kryptografische Verfahren implementieren..... 183**

RSA-Schlüssel erzeugen	184
Diffie-Hellman-Schlüssel vereinbaren.....	185

TEIL V **AUTHENTIFIZIEREN..... 189**

Kapitel 18 **Kryptografische Hashfunktion..... 191**

Hashfunktion.....	191
Kryptografische Sicherheit	193
Kryptografische Hashfunktionen in der Praxis.....	194
Der SHA-1-Hashalgorithmus.....	195
Ablauf des Verfahrens.....	196

Kapitel 19 **Authentizität und Integrität von Nachrichten..... 199**

Authentizität und Integrität bei symmetrischer Verschlüsselung.....	199
Authentizitätscode erstellen	200
Hash-Keyed Message Authentication Code (HMAC).....	200
Digitale Signatur	203
Eigenschaften einer Unterschrift.....	203
Digitale Signatur	204
Sicherheitsprobleme	204
Hash-Signatur	205
Eigenschaften der RSA-Signatur	206

Kapitel 20 **Teilnehmer-Authentifizierung..... 209**

Isomorphe Graphen	211
Bit-Commitment.....	212
Eine Münze werfen	213
Sich committen	213
Sicherheit des Protokolls.....	214
Münzwurf telefonisch	215
Teilnehmer-Authentifizierung	216
Zero-Knowledge-Eigenschaft.....	216





16 Inhaltsverzeichnis

Fiat-Shamir-Protokoll	217
Bit-Commitment-Protokoll	217
Sicherheit	217
Teilnehmer-Authentifizierung	219
Zero-Knowledge-Eigenschaft	219

TEIL VI

SICHERHEIT 221

Kapitel 21

Angriffe auf das RSA-Verfahren 223

Faktorisieren mithilfe von $\phi(n)$	224
Low-Exponent-Angriff auf das RSA-Verfahren	225
Implementierung	226
Klartext-Aufbereitung	229
Replay-Angriff	231
Seitenkanal-Angriff	232

Kapitel 22

Faktorisierungsangriff 235

Idee	235
Quadratisches Sieb	236
Sieb	237
Auswahl von Exponentenvektoren	239
Die $p-1$ -Methode	239
Idee	240
Implementierung	241
Programm	241

Kapitel 23

Angriffe auf Hashfunktionen 243

Passwort-Dateien angreifen	243
Angriff mit roher Gewalt	244
Wörterbuchangriff	244
Zum Geburtstag ein Angriff	245

TEIL VII

ZUFALL 249

Kapitel 24

Zufallsbits und Pseudozufallsbits 251

Zufallszahlen erzeugen	252
Zufallsbits mit rückgekoppeltem Schieberegister	252
Linear rückgekoppeltes Schieberegister	252
Kryptografische (Un-)Sicherheit	254



Inhaltsverzeichnis 17

Kapitel 25	
Kryptografisch sichere Zufallsbits	257
Startwert wählen	257
Pseudozufallsbits per Hashfunktion.....	258
Blum-Blum-Shub-Zufallsbits	258
Algorithmus.....	259
Implementierung	259
Sicherheit.....	260
Blum-Micali Zufallsbits.....	260
Algorithmus.....	260
Implementierung	261
Sicherheit.....	261
TEIL VIII	
ANWENDUNGEN	263
Kapitel 26	
Zertifizierte Sicherheit	265
TLS – Daten sicher transportieren	266
Ablauf des TLS-Handshakes	267
Zertifikat – Echtheit garantiert.....	268
E-Mails verschlüsseln und signieren.....	270
TEIL IX	
DER TOP-TEN-TEIL	273
Kapitel 27	
10/2 Mal die glorreichen Sieben	275
Die 7 verrücktesten Dinge	275
Primzahltest	275
Diffie-Hellman-Schlüsselvereinbarung	276
Public-Key-Verschlüsselung.....	276
Shamirs No-Key-Verschlüsselung.....	277
Nichtunterscheidbarkeit	277
Bit-Commitment	277
Zero-Knowledge-Authentifizierung.....	278
Die 7 bedeutendsten Anwendungszwecke.....	278
Vertraulichkeit.....	278
Integrität.....	279
Authentizität.....	279
Verbindlichkeit.....	279
Festlegung.....	280
Anonymität.....	280
Kooperation.....	280
Die 7 elementarsten Berechnungsverfahren	280
Bitweise Addition modulo 2.....	281
Schnelle modulare Exponentiation.....	281



18 Inhaltsverzeichnis

Größter gemeinsamer Teiler	281
Erweiterter euklidischer Algorithmus	281
Primzahltest	282
Chinesischer Restsatz	282
Punkte einer elliptischen Kurve verknüpfen	282
Die 7 wichtigsten Einwegfunktionen	282
Faktorisierung	282
Problem des diskreten Logarithmus	283
Problem des diskreten Logarithmus elliptischer Kurven	283
Wurzeln modulo n ziehen	284
Graphisomorphismus	284
Kryptografische Hashfunktion invertieren	284
AES-Known-Plaintext-Angriff	285
Die 7 häufigsten Angriffe	285
Brute-Force-Angriff	285
Ciphertext-Only-Angriff	285
Known-Plaintext-Angriff	286
Man-in-the-Middle-Angriff	286
Geburtstagsangriff	286
Replay-Angriff	287
Seitenkanal-Angriff	287

ANHÄNGE **289**

Anhang A

Zum Weiterlesen **289**

Anhang B

Lösungen zu den Übungsaufgaben **291**

Kapitel 2	291
Kapitel 5	291
Kapitel 6	292
Kapitel 7	293
Kapitel 8	293
Kapitel 10	294
Kapitel 13	295
Kapitel 14	295
Kapitel 15	296
Kapitel 21	296

Literaturverzeichnis **297**

Stichwortverzeichnis **298**

