

Inhaltsverzeichnis

1	Einführung in die Kryptografie und Datensicherheit	1
1.1	Überblick über die Kryptografie (und dieses Buch)	1
1.2	Symmetrische Kryptografie	4
1.2.1	Grundlagen	4
1.2.2	Die Substitutionschiffre	7
1.3	Kryptanalyse	10
1.3.1	Angriffe gegen kryptografische Verfahren	10
1.3.2	Wie viele Schlüsselbit braucht man?	13
1.4	Modulare Arithmetik und weitere historische Chiffren	14
1.4.1	Modulare Arithmetik	15
1.4.2	Restklassenringe	18
1.4.3	Die Verschiebe- oder Cäsar-Chiffre	20
1.4.4	Affine Chiffre	22
1.5	Diskussion und Literaturempfehlungen	23
1.6	Lessons Learned	26
1.7	Aufgaben	26
	Literatur	31
2	Stromchiffren	33
2.1	Einführung	33
2.1.1	Stromchiffren und Blockchiffren	33
2.1.2	Die Ver- und Entschlüsselung mit Stromchiffren	35
2.2	Zufallszahlen und eine unknackbare Chiffre	39
2.2.1	Zufallszahlengeneratoren	39
2.2.2	Das One-Time-Pad	40
2.2.3	Wie konstruiert man praktische Stromchiffren?	43
2.3	Stromchiffren basierend auf Schieberegistern	47
2.3.1	Linear rückgekoppelte Schieberegister	47
2.3.2	Ein Angriff auf LFSR mit bekanntem Klartext	51
2.3.3	Trivium	53

2.4	Diskussion und Literaturempfehlungen	56
2.5	Lessons Learned	58
2.6	Aufgaben	59
	Literatur	62
3	Der Data Encryption Standard und Alternativen	63
3.1	Einführung zum DES	63
3.1.1	Konfusion und Diffusion	65
3.2	Übersicht über den DES-Algorithmus	66
3.3	Interne Struktur des DES	69
3.3.1	Eingangs- und Ausgangspermutation	69
3.3.2	Die f -Funktion	70
3.3.3	Schlüsselfahrplan	76
3.4	Entschlüsselung	78
3.4.1	Umgekehrter Schlüsselfahrplan	78
3.4.2	Entschlüsselung mit Feistel-Chiffren	80
3.5	Sicherheit von DES	82
3.5.1	Vollständige Schlüsselsuche	83
3.5.2	Analytische Angriffe	85
3.6	Implementierung in Software und Hardware	87
3.6.1	Software	87
3.6.2	Hardware	88
3.7	DES-Alternativen	88
3.7.1	Der Advanced Encryption Standard (AES) und die AES-Finalisten	88
3.7.2	Triple-DES (3DES) und DESX	89
3.7.3	Die Lightweight-Chiffre PRESENT	90
3.8	Diskussion und Literaturempfehlungen	93
3.9	Lessons Learned	95
3.10	Aufgaben	95
	Literatur	100
4	Der Advanced Encryption Standard	103
4.1	Einführung	103
4.2	Übersicht über den AES-Algorithmus	105
4.3	Eine kurze Einführung in endliche Körper	106
4.3.1	Die Existenz endlicher Körper	108
4.3.2	Primzahlkörper	109
4.3.3	Erweiterungskörper $GF(2^m)$	111
4.3.4	Addition und Subtraktion in $GF(2^m)$	112
4.3.5	Multiplikation in $GF(2^m)$	113
4.3.6	Inversion in $GF(2^m)$	115

4.4	Die interne Struktur des AES	116
4.4.1	Byte-Substitution-Schicht	118
4.4.2	Diffusionsschicht	121
4.4.3	Key-Addition-Schicht	123
4.4.4	Schlüsselfahrplan	124
4.5	Entschlüsselung	128
4.5.1	Inverse MixColumn-Transformation	130
4.5.2	Inverse ShiftRows-Transformation	131
4.5.3	Inverse Byte-Substitution-Schicht	131
4.6	Implementierung in Software und Hardware	133
4.6.1	Software	133
4.6.2	Hardware	134
4.7	Diskussion und Literaturempfehlungen	134
4.8	Lessons Learned	135
4.9	Aufgaben	136
	Literatur	140
5	Mehr über Blockchiffren	143
5.1	Verschlüsselung mit Blockchiffren: Betriebsmodi	143
5.1.1	Electronic-Codebook-Modus	144
5.1.2	Cipher-Block-Chaining-Modus	148
5.1.3	Output-Feedback-Modus	151
5.1.4	Cipher-Feedback-Modus	152
5.1.5	Counter-Modus	154
5.1.6	Galois-Counter-Modus	155
5.2	Mehr zur vollständigen Schlüsselsuche	157
5.3	Erhöhung der Sicherheit von Blockchiffren	159
5.3.1	Zweifachverschlüsselung und Meet-in-the-Middle-Angriff	159
5.3.2	Dreifachverschlüsselung	162
5.3.3	Key Whitening	163
5.4	Diskussion und Literaturempfehlungen	165
5.5	Lessons Learned	167
5.6	Aufgaben	167
	Literatur	171
6	Einführung in die asymmetrische Kryptografie	173
6.1	Symmetrische versus asymmetrische Kryptografie	173
6.1.1	Die Symmetrie bei der symmetrischen Kryptografie	174
6.1.2	Das Prinzip der asymmetrischen Kryptografie	176
6.2	Praktische Aspekte der asymmetrischen Kryptografie	178
6.2.1	Sicherheitsmechanismen	178
6.2.2	Das verbleibende Problem: Authentizität der öffentlichen Schlüssel	179

6.2.3	Wichtige asymmetrische Algorithmen	179
6.2.4	Schlüssellängen und Sicherheitsniveau	180
6.3	Grundlagen der Zahlentheorie für asymmetrische Algorithmen	182
6.3.1	Der euklidische Algorithmus	182
6.3.2	Der erweiterte euklidische Algorithmus	185
6.3.3	Die eulersche Phi-Funktion	190
6.3.4	Der kleine fermatsche Satz und der Satz von Euler	192
6.4	Diskussion und Literaturempfehlungen	193
6.5	Lessons Learned	195
6.6	Aufgaben	195
	Literatur	198
7	Das RSA-Kryptosystem	199
7.1	Einführung	199
7.2	Ver- und Entschlüsselung	200
7.3	Schlüsselerzeugung und Korrektheitsbeweis	202
7.4	Schnelle Exponentiation	206
7.5	RSA-Beschleunigung	210
7.5.1	Schnelle Verschlüsselung mit kurzen öffentlichen Exponenten	210
7.5.2	Schnelle Entschlüsselung mit dem chinesischen Restsatz	211
7.6	Finden großer Primzahlen	214
7.6.1	Wie häufig sind Primzahlen?	215
7.6.2	Primzahltests	216
7.7	RSA in der Praxis: Padding	219
7.8	Angriffe	221
7.8.1	Protokollangriffe	222
7.8.2	Mathematische Angriffe	222
7.8.3	Seitenkanalangriffe	223
7.9	Implementierung in Soft- und Hardware	225
7.10	Diskussion und Literaturempfehlungen	226
7.11	Lessons Learned	227
7.12	Aufgaben	228
	Literatur	233
8	Asymmetrische Verfahren basierend auf dem diskreten Logarithmusproblem	235
8.1	Diffie-Hellman-Schlüsselaustausch	236
8.2	Ein wenig abstrakte Algebra	238
8.2.1	Gruppen	239
8.2.2	Zyklische Gruppen	240
8.2.3	Untergruppen	244

8.3	Das diskrete Logarithmusproblem	247
8.3.1	Das diskrete Logarithmusproblem in Primzahlkörpern	247
8.3.2	Das verallgemeinerte diskrete Logarithmusproblem	248
8.3.3	Angriffe gegen das diskrete Logarithmusproblem	250
8.4	Sicherheit des Diffie-Hellman-Schlüsselaustauschs	255
8.5	Das Verschlüsselungsverfahren nach Elgamal	256
8.5.1	Vom Diffie-Hellman-Schlüsselaustausch zur Elgamal-Verschlüsselung	256
8.5.2	Das Elgamal-Protokoll	258
8.5.3	Rechenkomplexität	260
8.5.4	Sicherheit	261
8.6	Diskussion und Literaturempfehlungen	263
8.7	Lessons Learned	264
8.8	Aufgaben	265
	Literatur	270
9	Kryptosysteme mit elliptischen Kurven	273
9.1	Rechnen auf elliptischen Kurven	274
9.1.1	Definition von elliptischen Kurven	274
9.1.2	Das Gruppengesetz elliptischer Kurven	276
9.2	Das diskrete Logarithmusproblem über elliptischen Kurven	280
9.3	Diffie-Hellman-Schlüsselaustausch mit elliptischen Kurven	284
9.4	Sicherheit	286
9.5	Implementierung in Software und Hardware	287
9.6	Diskussion und Literaturempfehlungen	289
9.7	Lessons Learned	291
9.8	Aufgaben	291
	Literatur	294
10	Digitale Signaturen	297
10.1	Einführung	297
10.1.1	Autos in ungewöhnlichen Farben oder warum symmetrische Kryptografie allein nicht ausreicht	298
10.1.2	Das Prinzip digitaler Signaturen	299
10.1.3	Sicherheitsdienste	301
10.2	RSA-Signaturen	303
10.2.1	RSA-Signaturen – Schulbuchmethode	303
10.2.2	Praktische Aspekte	305
10.2.3	Sicherheit	306
10.2.4	RSA mit Padding: Der Probabilistische Signaturstandard (PSS)	307
10.3	Digitale Signaturen nach Elgamal	309
10.3.1	Schulbuchversion des Elgamal-Signaturverfahrens	309

10.3.2 Praktische Aspekte	312
10.3.3 Sicherheit	312
10.4 Der Digital-Signature-Algorithmus	315
10.4.1 Algorithmus	315
10.4.2 Praktische Aspekte	319
10.4.3 Sicherheit	320
10.5 Der Elliptic-Curve-Digital-Signature-Algorithmus	321
10.5.1 Der ECDSA-Standard	321
10.5.2 Praktische Aspekte	325
10.5.3 Sicherheit	325
10.6 Diskussion und Literaturempfehlungen	326
10.7 Lessons Learned	328
10.8 Aufgaben	328
Literatur	332
 11 Hash-Funktionen	 335
11.1 Motivation: Das Signieren langer Nachrichten	335
11.2 Sicherheitseigenschaften von Hash-Funktionen	338
11.2.1 Urbildresistenz	339
11.2.2 Schwache Kollisionsresistenz oder zweite Urbildresistenz	340
11.2.3 Kollisionsresistenz und das Geburtstagsparadox	341
11.3 Überblick über Hash-Funktionen	346
11.3.1 Dedizierte Hash-Funktionen: Die MD4-Familie und SHA-3	346
11.3.2 Hash-Funktionen basierend auf Blockchiffren	348
11.4 Der Secure-Hash-Algorithmus SHA-1	351
11.4.1 Vorverarbeitung	352
11.4.2 Berechnen des Hash-Werts	353
11.4.3 Implementierung	356
11.5 Diskussion und Literaturempfehlungen	356
11.6 Lessons Learned	358
11.7 Aufgaben	359
Literatur	362
 12 Message Authentication Codes (MACs)	 363
12.1 Die Grundidee von Message-Authentication-Codes	363
12.2 MAC-Konstruktionen mit Hash-Funktionen	365
12.2.1 Schwachstellen von Secret-Prefix-MAC	366
12.2.2 Schwachstellen von Secret-Suffix-MAC	367
12.2.3 HMAC	367
12.3 MAC mit Blockchiffren: CBC-MAC	369
12.3.1 MAC-Erzeugung	369
12.3.2 MAC Verifikation	370

12.4	Der Galois-Message-Authentication-Code	371
12.5	Diskussion und Literaturempfehlungen	371
12.6	Lessons Learned	372
12.7	Aufgaben	372
	Literatur	374
13	Schlüsselerzeugung	377
13.1	Einführung	378
13.1.1	Terminologie	378
13.1.2	Schlüsselaktualisierung und Schlüsselableitung	378
13.1.3	Das n^2 -Schlüsselverteilungsproblem	380
13.2	Schlüsselverteilung mithilfe symmetrischer Techniken	382
13.2.1	Schlüsselaufbau mithilfe eines Schlüsselservers	382
13.2.2	Kerberos	387
13.2.3	Verbleibende Probleme der symmetrischen Schlüsselverteilung	388
13.3	Schlüsselverteilung mithilfe asymmetrischer Techniken	389
13.3.1	Mann-in-der-Mitte-Angriff	390
13.3.2	Zertifikate	392
13.3.3	Public-Key-Infrastrukturen und Certification Authorities	396
13.4	Diskussion und Literaturempfehlungen	400
13.5	Lessons Learned	401
13.6	Aufgaben	401
	Literatur	407
	Sachverzeichnis	409