

Inhaltsverzeichnis

1	Einführung in die Kryptografie und Datensicherheit	1
1.1	Überblick über die Kryptografie (und dieses Buch)	2
1.2	Symmetrische Kryptografie	4
1.2.1	Grundlagen	5
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	21
1.5	Diskussion und Literaturempfehlungen	23
1.6	Lessons Learned	25
1.7	Literaturverzeichnis	27
	Aufgaben	28
2	Stromchiffren	33
2.1	Einführung	34
2.1.1	Stromchiffren und Blockchiffren	34
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	41
2.2.3	Wie konstruiert man praktische Stromchiffren?	43
2.3	Stromchiffren basierend auf Schieberegistern	47
2.3.1	Linear rückgekoppelte Schieberegister (LFSR)	48
2.3.2	Ein Angriff auf LFSRs mit bekanntem Klartext	52
2.3.3	Trivium	54
2.4	Diskussion und Literaturempfehlungen	57

2.5	Lessons Learned	59
2.6	Literaturverzeichnis	60
	Aufgaben	61
3	Der Data Encryption Standard (DES) und Alternativen	65
3.1	Einführung zum DES	66
3.1.1	Konfusion und Diffusion	67
3.2	Übersicht über den DES-Algorithmus	68
3.3	Interne Struktur des DES	71
3.3.1	Eingangs- und Ausgangspermutation	71
3.3.2	Die f -Funktion	73
3.3.3	Schlüsselfahrplan	78
3.4	Entschlüsselung	80
3.4.1	Umgekehrter Schlüsselfahrplan	80
3.4.2	Entschlüsselung mit Feistelchiffren	82
3.5	Sicherheit von DES	84
3.5.1	Vollständige Schlüsselsuche	84
3.5.2	Analytische Angriffe	86
3.6	Implementierung in Software und Hardware	88
3.6.1	Software	88
3.7	DES-Alternativen	89
3.7.1	Der Advanced Encryption Standard (AES) und die AES-Finalisten	90
3.7.2	Triple-DES (3DES) und DESX	90
3.7.3	Die Lightweight-Chiffre PRESENT	91
3.8	Diskussion und Literaturempfehlungen	94
3.9	Lessons Learned	96
3.10	Literaturverzeichnis	97
	Aufgaben	99
4	Der Advanced Encryption Standard (AES)	103
4.1	Einführung	104
4.2	Übersicht über den AES-Algorithmus	105
4.3	Eine kurze Einführung in endliche Körper	107
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	117
4.4.2	Diffusionsschicht	120
4.4.3	Key-Addition-Schicht	123
4.4.4	Schlüsselfahrplan	123

4.5	Entschlüsselung	126
4.5.1	Inverse MixColumn-Transformation	129
4.5.2	Inverse ShiftRows-Transformation	130
4.5.3	Inverse Byte-Substitution-Schicht	130
4.6	Implementierung in Software und Hardware	132
4.6.1	Software	132
4.7	Diskussion und Literaturempfehlungen	133
4.8	Lessons Learned	134
4.9	Literaturverzeichnis	136
	Aufgaben	137
5	Mehr über Blockchiffren	141
5.1	Verschlüsselung mit Blockchiffren: Betriebsmodi	142
5.1.1	Electronic-Codebook-Modus (ECB)	142
5.1.2	Cipher-Block-Chaining-Modus (CBC)	147
5.1.3	Output-Feedback-Modus (OFB)	149
5.1.4	Cipher-Feedback-Modus (CFB)	150
5.1.5	Counter-Modus (CTR)	152
5.1.6	Galois-Counter-Modus (GCM)	153
5.2	Mehr zur vollständigen Schlüsselsuche	156
5.3	Erhöhung der Sicherheit von Blockchiffren	158
5.3.1	Zweifachverschlüsselung und Meet-in-the-Middle-Angriff	158
5.3.2	Dreifachverschlüsselung	161
5.3.3	Key Whitening	162
5.4	Diskussion und Literaturempfehlungen	164
5.5	Lessons Learned	165
5.6	Literaturverzeichnis	167
	Aufgaben	168
6	Einführung in die asymmetrische Kryptografie	173
6.1	Symmetrische versus asymmetrische Kryptografie	174
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	180
6.2.4	Schlüssellängen und Sicherheitsniveau	181
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	Literaturverzeichnis	196
	Aufgaben	197
7	Das RSA-Kryptosystem	201
7.1	Einführung	202
7.2	Ver- und Entschlüsselung	202
7.3	Schlüsselerzeugung und Korrektheitsbeweis	204
7.4	Schnelle Exponentiation	208
7.5	RSA-Beschleunigung	212
7.5.1	Schnelle Verschlüsselung mit kurzen öffentlichen Exponenten	212
7.5.2	Schnelle Entschlüsselung mit dem chinesischen Restsatz ..	213
7.6	Finden großer Primzahlen	216
7.6.1	Wie häufig sind Primzahlen?	217
7.6.2	Primzahltests	218
7.7	RSA in der Praxis: Padding	222
7.8	Angriffe	224
7.8.1	Protokollangriffe	224
7.8.2	Mathematische Angriffe	224
7.8.3	Seitenkanalangriffe	226
7.9	Implementierung in Soft- und Hardware	227
7.10	Diskussion und Literaturempfehlungen	228
7.11	Lessons Learned	230
7.12	Literaturverzeichnis	231
	Aufgaben	232
8	Asymmetrische Verfahren basierend auf dem diskreten Logarithmusproblem	237
8.1	Diffie-Hellman-Schlüsselaustausch	239
8.2	Ein wenig abstrakte Algebra	241
8.2.1	Gruppen	241
8.2.2	Zyklische Gruppen	243
8.2.3	Untergruppen	247
8.3	Das diskrete Logarithmusproblem	249
8.3.1	Das diskrete Logarithmusproblem in Primzahlkörpern	249
8.3.2	Das verallgemeinerte diskrete Logarithmusproblem	251
8.3.3	Angriffe gegen das diskrete Logarithmusproblem	253
8.4	Sicherheit des Diffie-Hellman-Schlüsselaustauschs	258
8.5	Das Verschlüsselungsverfahren nach Elgamal	259
8.5.1	Vom Diffie-Hellman-Schlüsselaustausch zur Elgamal-Verschlüsselung	259
8.5.2	Das Elgamal-Protokoll	260
8.5.3	Rechenkomplexität	262
8.5.4	Sicherheit	263

8.6	Diskussion und Literaturempfehlungen	265
8.7	Lessons Learned	267
8.8	Literaturverzeichnis	268
	Aufgaben	269
9	Kryptosysteme mit elliptischen Kurven	275
9.1	Rechnen auf elliptischen Kurven	276
9.1.1	Definition von elliptischen Kurven	277
9.1.2	Das Gruppengesetz elliptischer Kurven	278
9.2	Das diskrete Logarithmusproblem über elliptischen Kurven	282
9.3	Diffie-Hellman-Schlüsselaustausch mit elliptischen Kurven	286
9.4	Sicherheit	288
9.5	Implementierung in Software und Hardware	289
9.6	Diskussion und Literaturempfehlungen	290
9.7	Lessons Learned	292
9.8	Literaturverzeichnis	294
	Aufgaben	295
10	Digitale Signaturen	299
10.1	Einführung	300
10.1.1	Autos in ungewöhnlichen Farben oder warum symmetrische Kryptografie alleine nicht ausreicht	300
10.1.2	Das Prinzip digitaler Signaturen	302
10.1.3	Sicherheitsdienste	304
10.2	RSA-Signaturen	305
10.2.1	RSA-Signaturen – Schulbuchmethode	305
10.2.2	Praktische Aspekte	307
10.2.3	Sicherheit	308
10.3	Digitale Signaturen nach Elgamal	311
10.3.1	Schulbuchversion des Elgamal-Signaturverfahrens	311
10.3.2	Praktische Aspekte	314
10.3.3	Sicherheit	315
10.4	Der Digital Signature Algorithm (DSA)	318
10.4.1	Algorithmus	318
10.4.2	Praktische Aspekte	321
10.4.3	Sicherheit	323
10.5	Der Elliptic Curve Digital Signature Algorithm (ECDSA)	324
10.5.1	Der ECDSA Algorithmus	324
10.5.2	Praktische Aspekte	327
10.5.3	Sicherheit	328
10.6	Diskussion und Literaturempfehlungen	329
10.7	Lessons Learned	330
10.8	Literaturverzeichnis	332
	Aufgaben	333

11	Hashfunktionen	337
11.1	Motivation: Das Signieren langer Nachrichten	338
11.2	Sicherheitseigenschaften von Hashfunktionen	340
11.2.1	Urbildresistenz	341
11.2.2	Schwache Kollisionsresistenz oder zweite Urbildresistenz ..	342
11.2.3	Kollisionsresistenz und das Geburtstagsparadox.....	343
11.3	Überblick über Hashfunktionen	348
11.3.1	Dedizierte Hashfunktionen: Die MD4-Familie und SHA-3 ..	349
11.3.2	Hashfunktionen basierend auf Blockchiffren	351
11.4	Der Secure Hash Algorithm SHA-1	353
11.4.1	Vorverarbeitung	354
11.4.2	Berechnen des Hashwerts	355
11.4.3	Implementierung	357
11.5	Diskussion und Literaturempfehlungen	358
11.6	Lessons Learned	360
11.7	Literaturverzeichnis	362
	Aufgaben	362
12	Message Authentication Codes (MACs)	365
12.1	Die Grundidee von Message Authentication Codes	366
12.2	MAC-Konstruktionen mit Hashfunktionen	368
12.2.1	Schwachstellen von Secret-Prefix-MACs	368
12.2.2	Schwachstellen von Secret-Suffix-MACs	369
12.2.3	HMAC	370
12.3	MACs mit Blockchiffren: CBC-MAC	372
12.3.1	MAC-Erzeugung	372
12.3.2	MAC Verifikation	373
12.4	Der Galois-Message-Authentication-Code (GMAC)	373
12.5	Diskussion und Literaturempfehlungen	373
12.6	Lessons Learned	374
12.7	Literaturverzeichnis	375
	Aufgaben	375
13	Schlüsselerzeugung	379
13.1	Einführung	380
13.1.1	Terminologie	380
13.1.2	Schlüsselaktualisierung und Schlüsselableitung	380
13.1.3	Das n^2 -Schlüsselverteilungsproblem	382
13.2	Schlüsselverteilung mittels symmetrischer Techniken	384
13.2.1	Schlüsselaufbau mittels eines Schlüsselservers	384
13.2.2	Kerberos	388
13.2.3	Verbleibende Probleme der symmetrischen Schlüsselverteilung	389
13.3	Schlüsselverteilung mittels asymmetrischer Techniken	390
13.3.1	Mann-in-der-Mitte-Angriff	391

Inhaltsverzeichnis	xxi
13.3.2 Zertifikate	393
13.3.3 Public-Key-Infrastrukturen (PKI) und CAs	396
13.4 Diskussion und Literaturempfehlungen	400
13.5 Lessons Learned	402
13.6 Literaturverzeichnis	403
Aufgaben	404
Sachverzeichnis	409