

Inhaltsverzeichnis

1	Aufgaben und Grundzüge der Kryptografie	1
1.1	Geheimhaltung - Vertraulichkeit - der passive Angreifer	3
1.2	Authentifikation und Integrität	7
1.3	Andere Sicherheitsmechanismen: Steganographie, physikalische Sicherheit	9
1.4	Dienste, Mechanismen, Algorithmen	9
I	Symmetrische Verschlüsselungen	11
2	Historisches	13
2.1	Monoalphabetische Chiffren	13
2.1.1	Transpositionen	13
2.1.2	Cäsar-Chiffren	13
2.1.3	Monoalphabetische Chiffren	14
2.2	Polyalphabetische Chiffren	15
2.2.1	Vigenère-Chiffre	15
2.2.2	Grundidee der Kryptoanalyse	16
2.2.3	Der Kasiski-Angriff	16
2.2.4	Der Friedman-Angriff	16
2.3	Übungen	19
3	Formalisierung und Modelle	22
3.1	Das Modell von Shannon	22
3.2	Mathematische Formalisierung	23
3.3	Angriffsarten auf Verschlüsselungen	24
3.4	Übungen	29
4	Perfekte Sicherheit	32
4.1	Formalisierung der perfekten Sicherheit	33
4.2	Perfekte Ununterscheidbarkeit	41
4.3	Übungen	43
5	Effiziente Sicherheit - Computational Security	45
5.1	Algorithmen	45
5.2	Komplexitätstheorie	48
5.3	Effiziente Sicherheit	48
5.4	Übungen	50

6	Stromchiffren	51
6.1	Pseudozufallszahlen	52
6.2	Statistische Tests	53
6.3	Lineare Schieberegister	54
6.4	Vorhersagbarkeit von linearen Schieberegistern	62
6.5	Kombinationen von linearen Schieberegistern	62
6.6	Lineare Komplexität	63
6.7	Übungen	64
7	Blockchiffren	66
7.1	Vollständige Schlüsselsuche	67
7.2	Wertetabellen	68
7.3	Folgerungen	69
7.4	Designkriterien	70
7.5	Feistel-Chiffren	72
7.6	Der Data Encryption Standard - DES	74
7.6.1	Das Schema	74
7.6.2	Die Rundenfunktion	75
	Die Expansionsabbildung	76
	Die S-Boxen	76
	Permutation	78
	Zusammenspiel der Einzelkomponenten	78
7.6.3	Schlüsselauswahl	79
7.6.4	Eigenschaften des DES, Ergebnisse, Bewertung	80
7.7	Der Advanced Encryption Standard (AES)	81
7.7.1	Das Schema des AES	82
7.7.2	Algebraische Grundlagen	84
7.8	Die Rundenfunktion	85
7.8.1	Schlüsselauswahl	87
7.8.2	Entschlüsselung	88
7.8.3	Bewertung	88
7.9	Übungen	88
8	Kaskadenverschlüsselungen und Betriebsmodi	90
8.1	Kaskadenverschlüsselungen	90
8.1.1	Two-Key-Triple-DES	92
8.2	Betriebsmodi	92
8.2.1	Der Electronic-Codebook-Modus	93
8.2.2	Cipher-Block-Chaining-Modus	94
8.2.3	Counter-Modus	97
8.2.4	Cipher-Feedback-Modus	98
8.2.5	Output-Feedback-Modus	100
8.3	Übungen	100

18 Teilnehmerauthentifikation	216
18.1 Festcode-Verfahren	218
18.2 Wechselcode-Verfahren	219
18.3 Challenge-and-Response-Protokolle	221
18.4 Authentifikation mit Zero-Knowledge-Beweisen	223
18.5 Eigenschaften von Authentifikationsprotokollen	225
18.6 Übungen	226
19 Schlüsseletablierungsprotokolle	228
19.1 Angriffe auf Protokolle	229
19.1.1 Die Impersonation	230
19.1.2 Die Replay-Attacke	231
19.1.3 Reflektionsangriff	232
19.1.4 Der Man-in-the-middle-Angriff	233
19.2 Schlüsseltransportprotokolle	234
19.2.1 Das Breitmaulfrosch-Protokoll	235
19.2.2 Needham-Schroeder-Protokoll	236
19.2.3 Otway-Rees-Protokoll	237
19.2.4 Das TMN-Protokoll	238
19.3 Schlüsselvereinbarungsprotokolle	240
19.4 Sicherheit von Protokollen	245
19.5 Übungen	247
20 Multiparty-Computations	249
20.1 Modell	249
20.2 Secret-Sharing-Verfahren	252
20.2.1 Schwellenschemata	254
Das Schwellenschema von Shamir	254
20.2.2 Verifizierbare Geheimnisaufteilung	256
20.3 Threshold-Signaturverfahren	257
20.4 Der Münzwurf am Telefon	259
20.5 Oblivious-Transfer	260
20.6 Übungen	263
21 Anonymität	265
21.1 MIX-Netze	265
21.1.1 Kryptografische Sicherheit eines MIXes	268
21.1.2 Weitere Sicherheitsmaßnahmen	269
21.2 Blinde Signaturen	270
21.2.1 Elektronisches Geld	271
Das offline Münzsystem von D. Chaum, A. Fiat und M. Naor	273
21.3 Pseudonyme	276
21.3.1 Elektronische Wahlen	276

22 Internetsicherheit und Mobilfunk	278
22.1 Secure Sockets Layer (SSL)	278
22.1.1 Das Handshake-Protokoll	279
22.1.2 Change-Cipher-Spec-Nachricht	283
22.1.3 Record-Layer-Protokoll	284
22.1.4 Alert-Protokoll	284
22.1.5 Analyse des SSL-Protokolls Version 3.0	285
22.2 Pretty Good Privacy	286
22.2.1 Operationen	286
22.2.2 Schlüsselverwaltung	287
22.3 Das GSM-Mobilfunknetz	289
22.3.1 Authentifizierung	290
22.3.2 Verschlüsselung	291
22.3.3 Authentifikation in fremden GSM-Netzen	292
23 Quantenkryptografie und Quanten Computing	293
23.1 Quantenkryptografie	293
23.2 Quanten Computing	296
23.2.1 Physikalische Grundlagen	296
23.2.2 Quantencomputer	298
23.2.3 Faktorisierung mit Quantencomputern	299
23.2.4 Auswirkungen auf die Kryptografie	301
23.2.5 Ausblick	302
Literaturverzeichnis	303
Index	318