
Inhaltsverzeichnis

1	Einführung	1
2	Historische Chiffren und deren Analyse	3
2.1	Beispiele für Verschlüsselungen	3
2.2	Häufigkeitsverteilung der Buchstaben	5
2.3	Die Vigenère-Chiffre und deren Analyse	9
2.4	Die Enigma	18
2.5	Zusammenfassung	22
2.6	Übungen	23
3	Kryptographische Systeme und ihre Schlüsselverteilung	25
3.1	Kryptographie als Schutzmechanismus	25
3.1.1	Bedrohungen und Schutzziele	25
3.1.2	Angreifermodelle	29
3.2	Beschreibung kryptographischer Systeme	33
3.3	Kriterien zur Klassifizierung	34
3.4	Symmetrisches Konzelationssystem	37
3.5	Symmetrisches Authentikationssystem	41
3.6	Asymmetrisches Konzelationssystem	42
3.7	Asymmetrisches Authentikationssystem bzw. digitales Signatursystem	47
3.8	Weitere Anmerkungen zum Schlüsselaustausch	52
3.8.1	Wem werden Schlüssel zugeordnet?	52
3.8.2	Wie viele Schlüssel müssen ausgetauscht werden?	53
3.8.3	Sicherheit des Schlüsselaustauschs begrenzt kryptographisch erreichbare Sicherheit	54
3.9	Hybride kryptographische Systeme	55
3.10	Zusammenfassung	57
3.11	Übungen	58

4	Sicherheit kryptographischer Systeme	63
4.1	Aussagen zur Sicherheit: Ziele und Grenzen	63
4.2	Angriffsziele und Angriffserfolge	65
4.3	Klassifizierung von Angriffen	67
4.3.1	Passive Angriffe	67
4.3.2	Aktive Angriffe	68
4.3.3	Zusammenhang zwischen beobachtendem/ veränderndem und passivem/aktivem Angreifer	71
4.4	Informationstheoretische Sicherheit nach SHANNON	72
4.4.1	Informationstheoretische Grundlagen	72
4.4.2	Definition der informationstheoretischen Sicherheit	76
4.4.3	Bedingungen für informationstheoretische Sicherheit	79
4.4.4	Nachrichten- und Schlüsseläquivokation	86
4.4.5	Eindeutigkeitsdistanz	88
4.5	Grundsätzliches über Systeme mit geringerer Sicherheit	90
4.6	Weitere Sicherheitsbegriffe	93
4.6.1	Beschränkungen der „beweisbaren Sicherheit“	93
4.6.2	Semantische Sicherheit und probabilistische Verschlüsselung	94
4.6.3	Sicherheit gegen aktive Angriffe: Non-Malleability	96
4.7	Anforderungen an sichere Verschlüsselungsoperationen	98
4.8	Anforderungen an die Sicherheit kryptographischer Systeme	99
4.9	Überblick über die hier vorgestellten kryptographischen Systeme	101
4.10	Zusammenfassung	102
4.11	Übungen	103
5	Praktischer Betrieb kryptographischer Systeme	107
5.1	Schutz gegen zufällige Fehler	107
5.2	Verwendung mehrerer kryptographischer Systeme	108
5.3	Blockchiffren und Stromchiffren	111
5.4	Betriebsarten von Blockchiffren	113
5.4.1	Überblick	113
5.4.2	Electronic Codebook (ECB)	114
5.4.3	Cipher Block Chaining (CBC)	116
5.4.4	Cipher Feedback (CFB)	119
5.4.5	Output Feedback (OFB)	121
5.4.6	Counter Mode (CTR)	122
5.4.7	Zusammenfassung der Eigenschaften der Betriebsarten zur Konzelation	123
5.4.8	Cipher-Based Message Authentication Code (CMAC)	125
5.4.9	Betriebsarten zur Konzelation und Authentikation	125
5.5	Zusammenfassung	126
5.6	Übungen	127

6	Algebraische Grundlagen	129
6.1	Algebraische Strukturen	129
6.1.1	Gruppen, Ringe, Körper	129
6.1.2	Zyklische Gruppen	135
6.2	Modulare Arithmetik	138
6.2.1	Teiler und Division mit Rest	138
6.2.2	Der Restklassenring modulo n	140
6.2.3	Die prime Restklassengruppe modulo n	142
6.2.4	Effizientes Potenzieren modulo n	147
6.2.5	Chinesischer Restsatz (CRT)	148
6.2.6	Quadratwurzeln modulo p	151
6.2.6.1	Quadratwurzeln modulo p , p prim, $p \equiv 3 \pmod{4}$	152
6.2.6.2	Quadratwurzeln modulo p , p prim, $p \equiv 1 \pmod{4}$	153
6.2.7	Quadratwurzeln modulo pq	155
6.3	Primzahlen und Primzahltests	160
6.3.1	Grundlagen	160
6.3.2	Probefdivision	163
6.3.3	Satz von WILSON	164
6.3.4	AKS-Primzahltest	164
6.3.5	FERMAT-Primzahltest	167
6.3.6	RABIN-MILLER-Primzahltest	169
6.3.7	Wie findet man große Primzahlen?	171
6.4	Zusammenfassung	171
6.5	Übungen	172
7	Symmetrische Verfahren	175
7.1	Allgemeine Grundlagen	175
7.2	Informationstheoretisch sichere Kryptosysteme	177
7.2.1	Vernam-Chiffre (One-Time Pad)	177
7.2.2	Informationstheoretisch sichere Authentifikationscodes	182
7.2.2.1	Genauere Sicherheitsdefinition	183
7.2.2.2	Ausblick: Grenzen von Authentifikationscodes	184
7.3	Pseudo-One-Time-Pad	185
7.3.1	Anforderungen an Pseudozufallsbitfolgengeneratoren	185
7.3.1.1	Was ist ein Pseudozufallsbitfolgengenerator (PBG)?	185
7.3.1.2	Verwendung als Pseudo-One-Time-Pad	186
7.3.1.3	Forderungen an einen PBG	187
7.3.2	Der s^2 -mod- n -Generator	189
7.3.2.1	Sicherheitsbetrachtung	190
7.4	Data Encryption Standard (DES)	190
7.4.1	Grundlage: Feistel-Chiffre	190
7.4.2	Kurzer Überblick zur Geschichte des DES	192
7.4.3	Beschreibung des Algorithmus	192

7.4.4	Eigenschaften des DES	195
7.4.5	3-DES: Mehrfachverschlüsselung zur Erhöhung der Sicherheit	196
7.4.6	Analyse des DES	197
7.5	Advanced Encryption Standard (AES)	198
7.5.1	Kurzer Überblick zur Geschichte des AES	198
7.5.2	Beschreibung des Algorithmus	199
7.5.3	Analyse des AES	205
7.6	Zusammenfassung	205
7.7	Übungen	206
8	Asymmetrische Verfahren	209
8.1	Einwegfunktionen und Trapdoor-Einwegfunktionen	209
8.2	Das Rucksack-Problem und das Merkle-Hellman-Kryptosystem	212
8.3	Systeme auf der Grundlage des Faktorisierungsproblems	215
8.3.1	Das Faktorisierungsproblem	215
8.3.2	Das RSA-Kryptosystem	216
8.3.2.1	Mathematische Grundlagen	216
8.3.2.2	Prinzip des RSA-Kryptosystems	221
8.3.2.3	Naiver und unsicherer Einsatz von RSA	222
8.3.2.4	Angriffe, insbesondere multiplikative Angriffe von DAVIDA und MOORE	224
8.3.2.5	Sicherer Einsatz von RSA	231
8.3.2.6	Effiziente Implementierung von RSA	235
8.3.3	Faktorisierungsalgorithmen	237
8.3.3.1	Das Quadratische Sieb	237
8.3.3.2	Algorithmus von Shor	241
8.3.4	Das Blum-Goldwasser-Kryptosystem	242
8.4	Kryptosysteme auf der Grundlage des Problems des Diskreten Logarithmus	246
8.4.1	Das Problem des Diskreten Logarithmus	246
8.4.2	Der Diffie-Hellman-Schlüsselaustausch	247
8.4.3	Das ElGamal-Kryptosystem	249
8.4.3.1	Prinzip des ElGamal-Kryptosystems	249
8.4.3.2	Angriffe auf das ElGamal-Verfahren	251
8.4.3.3	Sichere Verwendung von des ElGamal-Verfahrens	252
8.4.4	Verfahren zum Lösen des Problems des diskreten Logarithmus	253
8.4.4.1	POHLIG-HELLMAN-Verfahren	254
8.4.4.2	Indexkalkül-Methode	256
8.4.5	Elliptische Kurven in der Kryptographie	257
8.5	Zusammenfassung	264
8.6	Übungen	265

9	Musterlösungen	267
9.1	Musterlösungen zu Kap. 2	267
9.2	Musterlösungen zu Kap. 3	269
9.3	Musterlösungen zu Kap. 4	281
9.4	Musterlösungen zu Kap. 5	285
9.5	Musterlösungen zu Kap. 6	287
9.6	Musterlösungen zu Kap. 7	291
9.7	Musterlösungen zu Kap. 8	293
	Literatur	297