

Inhaltsverzeichnis

1 Einführung	1
1.1 Begriffsbestimmung	1
1.2 Klassische und moderne Kryptographie	1
1.3 Beweisbare Sicherheit	3
1.4 Was wird in diesem Buch (nicht) behandelt?	3
I Verschlüsselung	5
2 Grundlegendes	7
2.1 Verschlüsselungsarten	7
2.2 Kommunikationszenarien	9
2.3 Sicherheitsziele	9
2.4 Bedrohungsszenarien	9
2.4.1 Wissen über das Verschlüsselungsverfahren	10
2.4.2 Ressourcen des Angreifers	11
3 Einmalige symmetrische Verschlüsselung und klassische Verschlüsselungsverfahren	13
3.1 Einführung	13
3.2 Kryptosysteme und possibilistische Sicherheit	13
3.3 Wiederholung Wahrscheinlichkeitstheorie	17
3.4 Informationstheoretische Sicherheit	23
3.4.1 Beispiele	25
3.4.2 Unabhängigkeit von der Klartextverteilung	27
3.4.3 Gleichverteilung auf dem Schlüsselraum und possibilistische Sicherheit	29
3.5 Wiederholung Zahlentheorie	31
3.6 Buchstaben- und blockweise Verschlüsselung	33
3.6.1 Buchstabenweise Verschlüsselung mit einem Schlüssel	34
3.6.2 Blockweise Verschlüsselung mit einem Schlüssel	37
3.7 Aufgaben	40
3.8 Anmerkungen und Hinweise	43
4 Frische symmetrische Verschlüsselung: Blockchiffren	45
4.1 Einführung	45
4.2 Substitutionspermutationskryptosysteme	48
4.3 Lineare Kryptanalyse	52
4.4 Wiederholung Polynomringe und endliche Körper	64
4.5 AES	66

4.6	Wiederholung Algorithmen	72
4.6.1	Ressourcenverbrauch	72
4.6.2	Zufallssteuerung	73
4.6.3	Prozedurparameter	79
4.7	Algorithmische Sicherheit von Block-Kryptosystemen	80
4.8	Funktionen statt Permutationen	89
4.9	Aufgaben	93
4.10	Anmerkungen und Hinweise	97
5	Uneingeschränkte symmetrische Verschlüsselung	101
5.1	Einführung	101
5.2	Betriebsarten	103
5.3	Algorithmische Sicherheit symmetrischer Kryptoschemen	107
5.4	Sicherheit der R-CTR-Betriebsart	113
5.5	Ein alternativer Sicherheitsbegriff	121
5.5.1	Von Angreifern zu Unterscheidern	123
5.5.2	Von Unterscheidern zu Angreifern	125
5.6	Ein stärkerer Sicherheitsbegriff	130
5.7	Aufgaben	132
5.8	Anmerkungen und Hinweise	135
6	Asymmetrische Verschlüsselung	137
6.1	Einführung	137
6.2	Algorithmische Sicherheit asymmetrischer Kryptoschemen	138
6.3	Wiederholung algorithmische Zahlentheorie	140
6.4	RSA	154
6.4.1	Das RSA-Kryptoschema	155
6.4.2	RSA als Einwegfunktion mit Hintertür	158
6.4.3	RSA-basierte asymmetrische Kryptoschemen	162
6.5	ElGamal	163
6.5.1	Das ElGamal-Kryptoschema	164
6.5.2	Das Diffie-Hellman-Entscheidungsproblem	167
6.5.3	Beweisbare Sicherheit des ElGamal-Kryptoschemas	172
6.6	Hybride Verschlüsselung	175
6.7	Aufgaben	180
6.8	Anmerkungen und Hinweise	183
II	Integrität und Authentizität	187
7	Grundlegendes	189
7.1	Prinzipielle Vorgehensweise: Prüfetiketten	190
7.2	Angriffszenarien	191

8 Kryptographische Hashfunktionen	193
8.1 Einführung	193
8.2 Sicherheitsanforderungen an Hashfunktionen	194
8.3 Der Geburtstagsangriff auf Hashfunktionen	196
8.4 Kompressionsfunktionen und iterierte Hashfunktionen	197
8.5 Die SHA-Familie	202
8.6 Aufgaben	204
8.7 Anmerkungen und Hinweise	207
9 Symmetrische Authentifizierungsverfahren	211
9.1 Einführung	211
9.2 Sicherheit symmetrischer Authentifizierungsverfahren	211
9.3 Konstruktion von MACs aus Block-Kryptosystemen	213
9.3.1 Eine einfache Konstruktion	213
9.3.2 Der CBC-MAC	216
9.4 Authentifizierungsschemen basierend auf Hashfunktionen	217
9.5 Der NMAC	222
9.6 Der HMAC	224
9.7 CCA-sichere symmetrische Kryptoschemen	228
9.8 Aufgaben	232
9.9 Anmerkungen und Hinweise	235
10 Asymmetrische Authentifizierungsverfahren: Digitale Signaturen	239
10.1 Einführung: Definition und Sicherheit	239
10.2 Signieren mit RSA: erster Versuch	241
10.3 Signierschemen basierend auf Hashfunktionen	242
10.4 Signieren mit RSA und dem Zufallsorakel	245
10.4.1 Das Zufallsorakel	245
10.4.2 Das FDH-RSA-Schema	249
10.4.3 Beweisbare Sicherheit des FDH-RSA-Schemas	250
10.5 Signieren in der Praxis	256
10.5.1 PKCS#1	256
10.5.2 DSA	257
10.6 Zertifikate und Public-Key-Infrastrukturen	258
10.6.1 Das Bindungsproblem	259
10.6.2 Zertifikate	262
10.6.3 Mehrere unabhängige Zertifizierungsstellen	263
10.6.4 Hierarchien von Zertifizierungsstellen	265
10.6.5 Zertifikatsnetze – Web of Trust	266
10.6.6 Gültigkeitszeiträume, Widerruf und Attribute	269
10.7 Aufgaben	270
10.8 Anmerkungen und Hinweise	273
Literaturverzeichnis	277
Stichwortverzeichnis	293