

# Inhaltsverzeichnis

<b>1</b>	<b>Ziele und Wege der Kryptographie .....</b>	<b>1</b>
1.1	Historische Verfahren .....	3
1.1.1	Skytale .....	3
1.1.2	Caesar-Chiffre .....	4
1.1.3	Vigenère-Chiffre .....	7
1.1.4	Vernam-Chiffre .....	10
1.1.5	Enigma .....	12
1.2	Sicherheitsdienste .....	14
1.2.1	Vertraulichkeit .....	15
1.2.2	Authentizität und Integrität .....	15
1.2.3	Verbindlichkeit .....	17
1.2.4	Anonymität .....	17
1.2.5	Zugriffskontrolle, Autorisierung .....	18
1.2.6	Sicherheitsdienste im Überblick .....	18
1.2.7	Bedrohungen und Sicherheitsdienste .....	19
1.3	Sicherheitsmechanismen .....	21
1.3.1	Verschlüsselung als Abbildung .....	21
1.3.2	Symmetrische Verschlüsselung .....	22
1.3.3	Asymmetrische Verfahren .....	26
1.3.4	Digitale Signaturen .....	28
1.3.5	Hilfs-Funktionen .....	31
1.3.6	Sicherheitsprotokolle .....	36
1.4	Sicherheit, Angriffe und perfekte Sicherheit .....	37
1.4.1	IT-Sicherheit .....	37
1.4.2	Kryptographische Sicherheit .....	37
<b>2</b>	<b>Symmetrische Chiffren .....</b>	<b>43</b>
2.1	Rechnen mit endlichen Zahlenmengen und Restklassen .....	43
2.1.1	Arithmetik modulo n, Restklassen .....	44
2.1.2	Axiome für Gruppe, Ring und Körper .....	45
2.1.3	Multiplikativ inverse Elemente, praktische Ermittlung .....	49
2.1.4	Übungen .....	51

2.2	DES, Data Encryption Standard.....	52
2.2.1	DES, Eigenschaften .....	53
2.2.2	DES, Verschlüsselung und Entschlüsselung.....	54
2.2.3	Triple-DES .....	57
2.2.4	DES-Anwendungen .....	58
2.2.5	Übungen .....	62
2.3	IDEA, International Data Encryption Algorithm .....	62
2.3.1	IDEA, im Überblick .....	63
2.3.2	IDEA, Verschlüsselung .....	64
2.3.3	IDEA, Entschlüsselung.....	65
2.3.4	Übungen .....	67
2.4	Stromchiffren RC4 und A5 .....	68
2.4.1	RC4.....	69
2.4.2	A5 .....	70
2.4.3	Sicherheit von Stromchiffren.....	72
2.5	Rechnen mit Polynom-Restklassen und Erweiterungskörpern.....	72
2.5.1	Polynom-Restklassen.....	73
2.5.2	Irreduzible Polynome .....	75
2.5.3	Axiome für Erweiterungskörper und Beispiel.....	76
2.5.4	Übungen .....	79
2.6	AES, Advanced Encryption Standard .....	81
2.6.1	AES, Verschlüsselung und Entschlüsselung.....	81
2.6.2	AES, Transformationsfunktionen .....	83
2.6.3	Übungen .....	85
2.7	Betriebsarten von Block-Chiffren: ECB, CBC, CFB, OFB, CTR.....	88
2.7.1	Wozu Betriebsarten?.....	88
2.7.2	Eigenschaft der Betriebsarten.....	89
3	<b>Hash-Funktionen.....</b>	95
3.1	Anwendungen und Arten von Hash-Funktionen .....	95
3.1.1	Arten von Hash-Funktionen .....	96
3.1.2	Angriffe auf Hash-Funktionen.....	97
3.2	Hash-Funktionen auf Basis von Block-Chiffren .....	100
3.3	Eigenständige Hash-Funktionen .....	101

3.3.1	MD5.....	103
3.3.2	SHA-1.....	104
3.3.3	SHA-2.....	105
3.3.4	SHA-Nachfolger.....	106
3.4	HMAC, MAC auf Basis von Hash.....	106
3.4.1	HMAC-Algorithmus.....	107
3.4.2	Vergleich von MAC mit HMAC .....	108
<b>4</b>	<b>Asymmetrische Chiffren.....</b>	<b>109</b>
4.1	Rechnen mit Potenzen modulo n.....	109
4.1.1	Potenzen modulo n .....	110
4.1.2	Sätze von Fermat und Euler, Eulersche $\Phi$ -Funktion .....	111
4.1.3	Berechnung großer Potenzen.....	114
4.1.4	Diskreter Logarithmus .....	115
4.1.5	Quadratwurzeln in der Rechnung modulo n .....	116
4.1.6	Chinesischer Restsatz .....	118
4.1.7	Übungen .....	120
4.2	RSA, Rivest/Shamir/Adleman .....	121
4.2.1	RSA, Schlüssel, Verschlüsselung, Signaturen.....	121
4.2.2	Zur Implementierung von RSA .....	124
4.2.3	Sicherheit von RSA .....	125
4.2.4	RSA-Beschleunigung durch Chinesischen Restsatz.....	127
4.2.5	Übungen .....	128
4.3	Diffie-Hellman-Schlüsselvereinbarung .....	129
4.4	ElGamal-Verfahren .....	131
4.4.1	Schlüsselvereinbarung nach ElGamal .....	131
4.4.2	Digitale Signatur und Verifikation nach ElGamal.....	133
4.4.3	Effizienz des ElGamal-Verfahrens .....	134
4.5	Elliptische Kurven, ECC-Kryptographie .....	135
4.5.1	Einführung .....	135
4.5.2	Mathematische Grundlagen .....	136
4.5.3	Geometrische Definition der Additionsoperation auf der Kurve.....	137
4.5.4	Bestimmung algebraischer Formeln für die Addition .....	139
4.5.5	Elliptische Kurven im diskreten Fall .....	141
4.5.6	Standardisierte Kurven .....	143

4.5.7	Anwendung der elliptischen Kurven in Algorithmen .....	144
4.5.8	Ausblick.....	147
<b>5</b>	<b>Authentifikations-Protokolle.....</b>	<b>149</b>
5.1	Authentifikation mit Passwort.....	150
5.1.1	Verfahren mit Dauer-Passwort .....	150
5.1.2	Verfahren mit Einmal-Passwort .....	150
5.2	Challenge-Response-Authentifikation .....	152
5.3	Authentifikation mit digitalen Signaturen .....	153
5.4	Fiat-Shamir-Authentifikation .....	155
5.4.1	Vertrauenswürdige Schlüsselbank.....	155
5.4.2	Authentifikations-Runde .....	156
5.4.3	Sicherheit für die Authentifikation .....	158
5.4.4	Zero-Knowledge-Protokoll.....	159
5.5	Authentifikation mit symmetrischen Schlüsseln .....	159
5.5.1	Protokollziel .....	159
5.5.2	Kerberos-Protokoll .....	160
5.6	Angriffe auf Authentifikations-Protokolle .....	162
<b>6</b>	<b>Sicherheitsprotokolle und Schlüsselverwaltung .....</b>	<b>165</b>
6.1	Public Key Infrastrukturen.....	166
6.1.1	Komponenten und Prozesse in einer PKI .....	166
6.1.2	PKI-Standards und Gesetzgebung .....	171
6.2	Sicherheitsprotokolle im Internet .....	174
6.2.1	Das Internet und die Internet-Protokollsuite.....	174
6.2.2	Sicherheitsprotokolle in der Internet-Protokollsuite .....	175
6.3	Das SSL/TLS-Protokoll .....	177
6.3.1	Das SSL-Handshake .....	177
6.3.2	Sicherung über SSL-Records.....	179
6.3.3	Secure Shell, SSH.....	180
6.4	IP-Sicherheit mit IPSec .....	181
6.4.1	Internet Key Exchange .....	181
6.4.2	Authentication Header.....	185
6.4.3	Encapsulated Security Payload.....	187
6.4.4	Tunnel-Modus .....	188

6.4.5	Transport-Modus .....	189
6.5	Sicherheit bei der Echtzeit-Datenübertragung.....	190
6.5.1	SRTP und SRTCP .....	191
6.5.2	MIKEY .....	192
6.5.3	Z RTP .....	193
6.5.4	DTLS .....	193
6.6	Sicherheit in Funknetzen.....	194
6.6.1	EAP .....	194
6.6.2	WEP.....	196
6.6.3	WPA und WPA-2 .....	198
7	<b>Chipkarten und Sicherheitsmodule.....</b>	<b>199</b>
7.1	Historie.....	199
7.2	Chipkarten-Technologie.....	199
7.2.1	Arten von Chipkarten .....	199
7.2.2	Anwendungen.....	200
7.3	Aktuelle und zukünftige Chipkarten-Architekturen.....	201
7.3.1	Sicherheit von Chipkarten .....	202
7.3.2	Chipkarten-Architektur nach ISO/IEC 7816 .....	204
7.3.3	Interpreter-basierende Chipkarten-Betriebssysteme .....	207
7.4	Einsatz von Chipkarten .....	214
7.4.1	Schnittstellen zur Chipkartenintegration .....	214
7.5	Chipkarten-Anwendungen .....	223
7.5.1	Mobilfunk Chipkarten .....	223
7.5.2	Zukünftiger Einsatz neuer Internet-Chipkarten .....	233
7.6	Trusted Computing und Trusted Platform Module .....	234
7.6.1	Die Trusted Computing Group .....	234
7.6.2	Das Trusted Platform Module .....	235
7.6.3	Zusammenspiel der TCG Komponenten .....	238
7.6.4	Integritätsmessung.....	240
<b>Literatur .....</b>	<b>241</b>	
<b>Glossar .....</b>	<b>249</b>	
<b>Deutsch-Englisch, Begriffe.....</b>	<b>255</b>	
<b>Sachwortverzeichnis.....</b>	<b>257</b>	