

# Inhaltsübersicht

## Teil 1 Wozu Kryptografie?

1	Einleitung	3
2	Was ist Kryptografie und warum ist sie so wichtig?	9
3	Wie Daten abgehört werden können	17
4	Symmetrische Verschlüsselung	41
5	Die Enigma und andere Verschlüsselungsmaschinen	59

## Teil 2 Moderne Kryptografie

6	Der Data Encryption Standard	81
7	Weitere symmetrische Verschlüsselungsverfahren	93
8	Der Advanced Encryption Standard (AES)	127
9	Noch weitere symmetrische Verschlüsselungsverfahren	139
10	Asymmetrische Verschlüsselung	159
11	Digitale Signaturen	183
12	Weitere asymmetrische Krypto-Verfahren	193
13	Kryptografische Hashfunktionen	207
14	Kryptografische Zufallsgeneratoren	245
15	Stromchiffren	263

## Teil 3 Implementierung von Kryptografie

16	Real-World-Attacken	301
17	Standardisierung in der Kryptografie	329
18	Betriebsarten und Datenformatierung	343

19	Kryptografische Protokolle	359
20	Authentifizierung	379
21	Verteilte Authentifizierung	401
22	Krypto-Hardware und Krypto-Software	415
23	Weitere kryptografische Werkzeuge	443
24	Evaluierung und Zertifizierung	467

#### Teil 4 Public-Key-Infrastrukturen

25	Public-Key-Infrastrukturen	491
26	Digitale Zertifikate	521
27	PKI-Prozesse im Detail	537
28	Spezielle Fragen beim Betrieb einer PKI	561
29	Beispiel-PKIs	579

#### Teil 5 Kryptografische Netzwerkprotokolle

30	Kryptografie im OSI-Modell	597
31	Krypto-Standards für OSI-Schicht 1	607
32	Krypto-Standards für OSI-Schicht 2	617
33	IPsec (Schicht 3)	637
34	SSL und TLS (Schicht 4)	647
35	Verschlüsselte und signierte E-Mails (Schicht 7)	657
36	Weitere Krypto-Protokolle der Anwendungsschicht	669
37	Noch mehr Kryptografie in der Anwendungsschicht	693

#### Teil 6 Mehr über Kryptografie

38	Krypto-Wettbewerbe	715
39	Wer in der Kryptografie eine Rolle spielt	727
40	Wo Sie mehr zum Thema erfahren	747
41	Das letzte Kapitel	765

#### Anhang

Bildnachweis	787
Literatur	789
Index	811

# Inhaltsverzeichnis

## Teil 1

### Wozu Kryptografie?

<b>1</b>	<b>Einleitung</b>	<b>3</b>
1.1	Kryptografie heute. . . . .	4
1.2	Die vierte Auflage . . . . .	5
1.3	Mein Bedauern, meine Bitten und mein Dank . . . . .	6
<b>2</b>	<b>Was ist Kryptografie und warum ist sie so wichtig?</b>	<b>9</b>
2.1	The Name of the Game . . . . .	9
2.1.1	Die kurze Antwort . . . . .	9
2.1.2	Die lange Antwort. . . . .	9
2.2	Die Kryptografie – ein wichtiges Teilgebiet . . . . .	11
2.3	Warum ist die Kryptografie so wichtig? . . . . .	13
2.3.1	Wirtschaftsspionage . . . . .	13
2.3.2	Kommerz im Netz . . . . .	14
2.3.3	Die Privatsphäre . . . . .	14
2.4	Anwendungen der Kryptografie. . . . .	15
2.5	Und wer zum Teufel ist Alice? . . . . .	15
<b>3</b>	<b>Wie Daten abgehört werden können</b>	<b>17</b>
3.1	Mallory am Übertragungsmedium. . . . .	18
3.1.1	Kupferkabel . . . . .	18
3.1.2	Koaxialkabel. . . . .	18
3.1.3	Glasfaser . . . . .	18
3.1.4	Drahtlose Datenübertragung. . . . .	19
3.1.5	Satellit. . . . .	19

3.2	Mallory in Computernetzen . . . . .	20
3.2.1	Mitlesen und Verändern von Dateien . . . . .	20
3.2.2	Abhören analoger Telefonleitungen . . . . .	20
3.2.3	Abhören im LAN . . . . .	21
3.2.4	ISDN-Sicherheitsprobleme . . . . .	22
3.2.5	DSL . . . . .	23
3.2.6	Mobilfunk . . . . .	24
3.2.7	WLANs . . . . .	24
3.3	Mallory im Internet . . . . .	25
3.3.1	ARP-Spoofing . . . . .	25
3.3.2	Abhörangriffe auf Router und Gateways . . . . .	26
3.3.3	IP-Spoofing . . . . .	26
3.3.4	DNS-Spoofing . . . . .	26
3.3.5	Mitlesen von E-Mails . . . . .	28
3.3.6	URL-Spoofing . . . . .	29
3.3.7	Abhören von Internettelefonie . . . . .	29
3.4	Ein paar Fälle aus der Praxis . . . . .	29
3.4.1	Passwort-Schnüffeleien . . . . .	30
3.4.2	Abgehörte E-Mails . . . . .	30
3.4.3	Echelon . . . . .	31
3.4.4	Weitere Fälle . . . . .	32
3.5	Ist Kryptografie gefährlich? . . . . .	34
3.5.1	Nachteile einer Krypto-Beschränkung . . . . .	36
3.5.2	Vorteile einer Krypto-Beschränkung . . . . .	37
3.5.3	Fazit . . . . .	39
<b>4</b>	<b>Symmetrische Verschlüsselung</b>	<b>41</b>
4.1	Symmetrische Verschlüsselung . . . . .	42
4.1.1	Kryptografische Fachbegriffe . . . . .	43
4.1.2	Angriffe auf Verschlüsselungsverfahren . . . . .	43
4.2	Monoalphabetische Substitutionschiffren . . . . .	45
4.2.1	Cäsar-Chiffre . . . . .	45
4.2.2	Weitere Substitutionschiffren . . . . .	46
4.2.3	Homophone Chiffre . . . . .	47
4.3	Polyalphabetische Substitutionschiffren . . . . .	49
4.3.1	Vigenère-Chiffre . . . . .	50
4.3.2	Vernam-Chiffre . . . . .	51
4.3.3	One-Time-Pad . . . . .	51
4.4	Permutationschiffren . . . . .	53

4.5	Ungelöste Verschlüsselungen . . . . .	55
4.5.1	Das Voynich-Manuskript . . . . .	55
4.5.2	Rohonczi-Kodex . . . . .	57
4.5.3	Dorabella-Chiffre . . . . .	58
<b>5</b>	<b>Die Enigma und andere Verschlüsselungsmaschinen</b>	<b>59</b>
5.1	Rotorchiffren. . . . .	60
5.1.1	Heberns Rotormaschine . . . . .	60
5.1.2	Die Enigma . . . . .	62
5.1.3	Weitere Rotor-Chiffriermaschinen . . . . .	66
5.2	Andere Verschlüsselungsmaschinen . . . . .	67
5.2.1	Die Kryha-Maschine . . . . .	68
5.2.2	Hagelin-Maschinen . . . . .	69
5.2.3	Die Purple . . . . .	71
5.2.4	Der Geheimschreiber . . . . .	73
5.2.5	Lorenz-Maschine. . . . .	75
5.2.6	Schlüsselgerät 41 (Hitler-Mühle). . . . .	76

## Teil 2

### Moderne Kryptografie

<b>6</b>	<b>Der Data Encryption Standard</b>	<b>81</b>
6.1	DES-Grundlagen . . . . .	82
6.2	Funktionsweise des DES . . . . .	84
6.2.1	Die Rundenfunktion F. . . . .	85
6.2.2	Die Schlüsselaufbereitung des DES . . . . .	86
6.2.3	Entschlüsseln mit dem DES . . . . .	87
6.3	Sicherheit des DES. . . . .	87
6.3.1	Vollständige Schlüsselsuche bis 1997 . . . . .	87
6.3.2	Die DES-Challenge . . . . .	88
6.3.3	Differenzielle Kryptoanalyse . . . . .	89
6.3.4	Lineare Kryptoanalyse. . . . .	89
6.3.5	Schwache Schlüssel . . . . .	89
6.3.6	Wie sicher ist der DES heute? . . . . .	90
6.4	DES-Fazit . . . . .	91
<b>7</b>	<b>Weitere symmetrische Verschlüsselungsverfahren</b>	<b>93</b>
7.1	Chiffren-Design . . . . .	94
7.1.1	Anforderungen an die Sicherheit . . . . .	94
7.1.2	Die ideale Schlüssellänge . . . . .	98
7.1.3	Aufbau symmetrischer Verschlüsselungsverfahren. . . . .	100

7.2	Triple-DES . . . . .	106
7.2.1	Doppel-DES . . . . .	106
7.2.2	Triple-DES . . . . .	107
7.3	SAFER . . . . .	108
7.3.1	Funktionsweise von SAFER+ . . . . .	109
7.3.2	Bewertung von SAFER+ . . . . .	111
7.4	RC2, RC5 und RC6 . . . . .	112
7.4.1	RC2 . . . . .	112
7.4.2	RC5 . . . . .	115
7.4.3	RC6 . . . . .	117
7.5	Blowfish und Twofish . . . . .	120
7.5.1	Blowfish . . . . .	120
7.5.2	Twofish . . . . .	123
<b>8</b>	<b>Der Advanced Encryption Standard (AES)</b>	<b>127</b>
8.1	Funktionsweise des AES . . . . .	128
8.1.1	Rundenaufbau . . . . .	129
8.1.2	Entschlüsselung mit dem AES. . . . .	132
8.1.3	Schlüsselaufbereitung . . . . .	132
8.1.4	Mathematische Betrachtung des AES . . . . .	134
8.2	Bewertung des AES. . . . .	135
8.2.1	AES als algebraische Formel. . . . .	136
8.2.2	Quadratische Kryptoanalyse . . . . .	137
<b>9</b>	<b>Noch weitere symmetrische Verschlüsselungsverfahren</b>	<b>139</b>
9.1	MISTY1, KASUMI und Camellia . . . . .	139
9.1.1	MISTY1 . . . . .	140
9.1.2	KASUMI . . . . .	140
9.1.3	Camellia . . . . .	142
9.2	Serpent . . . . .	142
9.2.1	Funktionsweise von Serpent . . . . .	143
9.2.2	S-Box-Design . . . . .	145
9.2.3	Schlüsselaufbereitung von Serpent . . . . .	146
9.2.4	Bewertung von Serpent. . . . .	146
9.3	AES-Kandidaten . . . . .	147
9.3.1	Die besten drei . . . . .	147
9.3.2	Die weiteren zwei Finalisten . . . . .	147
9.3.3	Wegen geringer Performanz ausgeschieden. . . . .	148
9.3.4	Die Unsicheren . . . . .	148
9.3.5	Einige AES-Kandidaten im Detail. . . . .	149
9.3.6	Fazit . . . . .	154

9.4	Weitere Verfahren . . . . .	154
9.4.1	Chiasmus und Libelle . . . . .	154
9.4.2	IDEA und IDEA NXT . . . . .	154
9.4.3	Skipjack . . . . .	156
9.4.4	TEA . . . . .	157
9.4.5	Weitere Verfahren . . . . .	158
<b>10</b>	<b>Asymmetrische Verschlüsselung</b>	<b>159</b>
10.1	Ein bisschen Mathematik . . . . .	162
10.1.1	Modulo-Rechnen . . . . .	162
10.1.2	Einwegfunktionen und Falltürfunktionen . . . . .	168
10.2	Der Diffie-Hellman-Schlüsselaustausch . . . . .	169
10.2.1	Funktionsweise von Diffie-Hellman . . . . .	170
10.2.2	MQV . . . . .	171
10.3	RSA . . . . .	174
10.3.1	Funktionsweise des RSA-Verfahrens . . . . .	174
10.3.2	Ein Beispiel . . . . .	175
10.3.3	Sicherheit des RSA-Verfahrens . . . . .	176
10.4	Symmetrisch und asymmetrisch im Zusammenspiel . . . . .	180
10.4.1	Unterschiede zwischen symmetrisch und asymmetrisch . . . . .	180
10.4.2	Hybridverfahren . . . . .	181
<b>11</b>	<b>Digitale Signaturen</b>	<b>183</b>
11.1	Was ist eine digitale Signatur? . . . . .	184
11.2	RSA als Signaturverfahren . . . . .	185
11.2.1	Funktionsweise . . . . .	185
11.2.2	Sicherheit von RSA-Signaturen . . . . .	185
11.3	Signaturen auf Basis des diskreten Logarithmus . . . . .	186
11.3.1	ElGamal-Verfahren . . . . .	187
11.3.2	DSA . . . . .	188
11.4	Unterschiede zwischen DLSSs und RSA . . . . .	191
<b>12</b>	<b>Weitere asymmetrische Krypto-Verfahren</b>	<b>193</b>
12.1	Krypto-Systeme auf Basis elliptischer Kurven . . . . .	194
12.1.1	Mathematische Grundlagen . . . . .	194
12.1.2	ECC-Verfahren . . . . .	196
12.1.3	Die wichtigsten ECC-Verfahren . . . . .	198

12.2	Weitere asymmetrische Verfahren. . . . .	199
12.2.1	NTRU . . . . .	199
12.2.2	XTR . . . . .	202
12.2.3	Krypto-Systeme auf Basis hyperelliptischer Kurven . . . . .	202
12.2.4	HFE . . . . .	203
12.2.5	Weitere asymmetrische Verfahren . . . . .	205
<b>13</b>	<b>Kryptografische Hashfunktionen</b>	<b>207</b>
13.1	Was ist eine kryptografische Hashfunktion? . . . . .	208
13.1.1	Nichtkryptografische Hashfunktionen . . . . .	208
13.1.2	Kryptografische Hashfunktionen . . . . .	209
13.1.3	Angriffe auf kryptografische Hashfunktionen . . . . .	210
13.2	Die wichtigsten kryptografischen Hashfunktionen . . . . .	218
13.2.1	SHA-1 . . . . .	218
13.2.2	Neue SHA-Varianten . . . . .	222
13.2.3	MD4 . . . . .	223
13.2.4	MD5 . . . . .	223
13.2.5	RIPEMD-160 . . . . .	224
13.2.6	Tiger . . . . .	228
13.2.7	WHIRLPOOL . . . . .	231
13.2.8	RadioGatún . . . . .	233
13.2.9	Weitere kryptografische Hashfunktionen . . . . .	235
13.2.10	Hashfunktionen aus Verschlüsselungsverfahren . . . . .	236
13.2.11	SHA-3 . . . . .	238
13.3	Schlüsselabhängige Hashfunktionen . . . . .	239
13.3.1	Anwendungsbereiche . . . . .	240
13.3.2	Die wichtigsten schlüsselabhängigen Hashfunktionen . . . . .	240
13.4	Weitere Anwendungen kryptografischer Hashfunktionen . . . . .	243
13.4.1	Hashbäume . . . . .	243
13.4.2	Weitere Anwendungen . . . . .	244
<b>14</b>	<b>Kryptografische Zufallsgeneratoren</b>	<b>245</b>
14.1	Zufallszahlen in der Kryptografie . . . . .	246
14.1.1	Anforderungen der Kryptografie . . . . .	247
14.1.2	Echte Zufallsgeneratoren . . . . .	247
14.1.3	Pseudozufallsgeneratoren . . . . .	248
14.1.4	Die Grauzone zwischen echt und pseudo . . . . .	250
14.1.5	Mischen von Zufallsquellen . . . . .	250



14.2	Die wichtigsten Pseudozufallsgeneratoren . . . . .	251
14.2.1	Kryptografische Hashfunktionen als Fortschaltfunktion . . .	252
14.2.2	Schlüsselabhängige Hashfunktionen als Fortschaltfunktion. . . . .	255
14.2.3	Blockchiffren als Fortschaltfunktion . . . . .	256
14.2.4	Linear rückgekoppelte Schieberegister. . . . .	257
14.2.5	Nichtlinear rückgekoppelte Schieberegister . . . . .	259
14.2.6	Zahlentheoretische Pseudozufallsgeneratoren . . . . .	259
14.3	Primzahlgeneratoren . . . . .	260
<b>15</b>	<b>Stromchiffren</b>	<b>263</b>
15.1	Aufbau und Eigenschaften von Stromchiffren . . . . .	264
15.1.1	Wie eine Stromchiffre funktioniert . . . . .	264
15.1.2	Angriffe auf Stromchiffren . . . . .	266
15.1.3	Stromchiffren und Blockchiffren im Vergleich. . . . .	267
15.2	RC4. . . . .	268
15.2.1	Funktionsweise von RC4. . . . .	268
15.2.2	Bewertung von RC4 . . . . .	269
15.3	A5 . . . . .	271
15.3.1	Funktionsweise von A5 . . . . .	272
15.3.2	Bewertung von A5. . . . .	272
15.4	E0 . . . . .	273
15.4.1	Funktionsweise von $E_0$ . . . . .	273
15.4.2	Schlüsselaufbereitung von $E_0$ . . . . .	275
15.4.3	Bewertung von $E_0$ . . . . .	276
15.5	Crypto1. . . . .	277
15.5.1	Funktionsweise von Crypto1. . . . .	278
15.5.2	Bewertung von Crypto1 . . . . .	278
15.6	Die Verfahren des eSTREAM-Wettbewerbs . . . . .	279
15.6.1	HC-128. . . . .	280
15.6.2	Rabbit. . . . .	282
15.6.3	Salsa20 . . . . .	286
15.6.4	Sosemanuk . . . . .	288
15.6.5	Trivium. . . . .	290
15.6.6	Grain. . . . .	291
15.6.7	MICKEY. . . . .	293
15.6.8	Erkenntnisse aus dem eSTREAM-Wettbewerb . . . . .	295
15.7	Welche Stromchiffre ist die beste? . . . . .	296
15.7.1	Weitere Stromchiffren . . . . .	296
15.7.2	Welche Stromchiffren sind empfehlenswert? . . . . .	297

## Teil 3

### Implementierung von Kryptografie

<b>16</b>	<b>Real-World-Attacks</b>	<b>301</b>
16.1	Seitenkanalangriffe . . . . .	301
16.1.1	Zeitangriffe . . . . .	302
16.1.2	Stromangriffe . . . . .	304
16.1.3	Fehlerangriffe . . . . .	306
16.1.4	Weitere Seitenkanalangriffe . . . . .	307
16.2	Malware-Angriffe . . . . .	307
16.2.1	Malware und digitale Signaturen . . . . .	308
16.2.2	Vom Entwickler eingebaute Hintertüren . . . . .	310
16.2.3	Gegenmaßnahmen . . . . .	311
16.3	Physikalische Angriffe . . . . .	311
16.3.1	Die wichtigsten physikalischen Angriffe . . . . .	312
16.3.2	Gegenmaßnahmen . . . . .	312
16.4	Schwachstellen durch Implementierungsfehler . . . . .	315
16.4.1	Implementierungsfehler in der Praxis . . . . .	315
16.4.2	Implementierungsfehler in vielen Variationen. . . . .	316
16.4.3	Gegenmaßnahmen . . . . .	318
16.5	Insiderangriffe . . . . .	320
16.5.1	Unterschätzte Insider . . . . .	320
16.5.2	Gegenmaßnahmen . . . . .	320
16.6	Der Anwender als Schwachstelle. . . . .	322
16.6.1	Schwachstellen durch Anwenderfehler . . . . .	322
16.6.2	Gegenmaßnahmen . . . . .	325
16.7	Fazit . . . . .	328
<b>17</b>	<b>Standardisierung in der Kryptografie</b>	<b>329</b>
17.1	Standards . . . . .	329
17.1.1	Standardisierungsgremien. . . . .	330
17.1.2	Standardisierung im Internet . . . . .	331
17.2	Wissenswertes zum Thema Standards. . . . .	332
17.2.1	Standards und die Realität . . . . .	332
17.2.2	OIDs . . . . .	332
17.3	Wichtige Krypto-Standards. . . . .	333
17.3.1	PKCS . . . . .	333
17.3.2	IEEE P1363 . . . . .	334
17.3.3	ANSI X.9 . . . . .	335
17.3.4	NSA Suite B . . . . .	336

17.4	Standards für verschlüsselte und signierte Daten . . . . .	337
17.4.1	PKCS#7. . . . .	337
17.4.2	XML Signature und XML Encryption. . . . .	338
17.4.3	Weitere Formate . . . . .	341
<b>18</b>	<b>Betriebsarten und Datenformatierung</b>	<b>343</b>
18.1	Betriebsarten von Blockchiffren. . . . .	344
18.1.1	Electronic-Codebook-Modus . . . . .	344
18.1.2	Cipher-Block-Chaining-Modus . . . . .	345
18.1.3	Output-Feedback-Modus . . . . .	346
18.1.4	Cipher-Feedback-Modus. . . . .	348
18.1.5	Counter-Modus. . . . .	349
18.1.6	Fazit . . . . .	350
18.2	Datenformatierung für das RSA-Verfahren . . . . .	352
18.2.1	Der PKCS#1-Standard. . . . .	352
18.2.2	Datenformatierung für die RSA-Verschlüsselung. . . . .	353
18.2.3	Datenformatierung für RSA-Signaturen . . . . .	356
18.3	Datenformatierung für DLSSs . . . . .	357
<b>19</b>	<b>Kryptografische Protokolle</b>	<b>359</b>
19.1	Protokolle . . . . .	360
19.1.1	Konzeptprotokolle . . . . .	360
19.1.2	Netzwerkprotokolle . . . . .	361
19.1.3	Eigenschaften von Netzwerkprotokollen. . . . .	362
19.2	Protokolle in der Kryptografie. . . . .	364
19.2.1	Eigenschaften kryptografischer Netzwerkprotokolle . . . . .	364
19.3	Angriffe auf kryptografische Protokolle. . . . .	366
19.3.1	Replay-Attacke . . . . .	366
19.3.2	Spoofing-Attacke. . . . .	367
19.3.3	Man-in-the-Middle-Attacke . . . . .	368
19.3.4	Hijacking-Attacke. . . . .	369
19.3.5	Known-Key-Attacken . . . . .	369
19.3.6	Verkehrsflussanalyse . . . . .	373
19.3.7	Denial-of-Service-Attacke . . . . .	374
19.3.8	Sonstige Angriffe . . . . .	375
19.4	Beispielprotokolle . . . . .	375
19.4.1	Beispielprotokoll: Messgerät sendet an PC . . . . .	375
19.4.2	Weitere Beispielprotokolle. . . . .	378

<b>20</b>	<b>Authentifizierung</b>	<b>379</b>
20.1	Authentifizierung im Überblick. ....	379
20.1.1	Etwas, was man weiß. ....	381
20.1.2	Was man hat. ....	383
20.1.3	Was man ist. ....	383
20.2	Biometrische Authentifizierung. ....	383
20.2.1	Grundsätzliches zur biometrischen Authentifizierung. ....	384
20.2.2	Biometrische Merkmale. ....	386
20.2.3	Fazit. ....	391
20.3	Authentifizierung in Computernetzen. ....	392
20.3.1	Passwörter im Internet. ....	392
20.3.2	Authentifizierung mit asymmetrischen Verfahren. ....	397
20.3.3	Biometrie im Internet. ....	400
<b>21</b>	<b>Verteilte Authentifizierung</b>	<b>401</b>
21.1	Single Sign-On. ....	401
21.1.1	Credential-Synchronisation. ....	403
21.1.2	Lokales SSO. ....	404
21.1.3	Ticket-SSO. ....	404
21.1.4	Web-SSO. ....	405
21.2	Kerberos. ....	405
21.2.1	Vereinfachtes Kerberos-Protokoll. ....	406
21.2.2	Vollständiges Kerberos-Protokoll. ....	407
21.2.3	Vor- und Nachteile von Kerberos. ....	409
21.3	RADIUS und andere Triple-A-Server. ....	409
21.3.1	Triple-A-Server. ....	410
21.3.2	Beispiele für Triple-A-Server. ....	411
21.4	SAML. ....	412
21.4.1	Funktionsweise von SAML. ....	413
21.4.2	SAML in der Praxis. ....	414
<b>22</b>	<b>Krypto-Hardware und Krypto-Software</b>	<b>415</b>
22.1	Krypto-Hardware oder Krypto-Software? ....	415
22.1.1	Pro Software. ....	416
22.1.2	Pro Hardware. ....	417
22.1.3	Ist Hardware oder Software besser? ....	418
22.2	Smartcards. ....	418
22.2.1	Smartcards und andere Chipkarten. ....	418
22.2.2	Smartcard-Formfaktoren. ....	420
22.2.3	Smartcards und Kryptografie. ....	421

22.3	Kryptografie und elektronische Ausweise . . . . .	424
22.3.1	Elektronische Reisepässe . . . . .	426
22.3.2	Elektronische Personalausweise . . . . .	426
22.3.3	Elektronische Gesundheitskarten . . . . .	427
22.3.4	Weitere elektronische Ausweise . . . . .	428
22.4	Hardware-Security-Module . . . . .	429
22.5	Kryptografie in eingebetteten Systemen . . . . .	429
22.5.1	Eingebettete Systeme und Kryptografie . . . . .	430
22.5.2	Kryptografische Herausforderungen in eingebetteten Systemen . . . . .	431
22.6	RFID und Kryptografie . . . . .	433
22.6.1	Sicherheitsprobleme beim Einsatz von EPC-Chips . . . . .	434
22.6.2	RFID und Kryptografie . . . . .	435
<b>23</b>	<b>Weitere kryptografische Werkzeuge</b>	<b>443</b>
23.1	Management geheimer Schlüssel . . . . .	443
23.1.1	Schlüsselgenerierung . . . . .	444
23.1.2	Schlüsselspeicherung . . . . .	446
23.1.3	Schlüsselauthentifizierung . . . . .	447
23.1.4	Schlüsseltransport und Schlüssel-Backup . . . . .	447
23.1.5	Schlüsselaufteilung . . . . .	448
23.1.6	Schlüsselwechsel . . . . .	449
23.1.7	Löschen eines Schlüssels . . . . .	450
23.1.8	Key Recovery . . . . .	450
23.2	Trusted Computing und Kryptografie . . . . .	451
23.2.1	Trusted Computing und Kryptografie . . . . .	452
23.2.2	Das Trusted Platform Module . . . . .	453
23.2.3	Funktionen und Anwendungen des TPM . . . . .	455
23.2.4	Fazit . . . . .	456
23.3	Krypto-APIs . . . . .	457
23.3.1	PKCS#11 . . . . .	457
23.3.2	MS-CAPI . . . . .	460
23.3.3	Cryptography API Next Generation (CNG) . . . . .	462
23.3.4	ISO/IEC 24727 . . . . .	463
23.3.5	Universelle Krypto-APIs . . . . .	464
<b>24</b>	<b>Evaluierung und Zertifizierung</b>	<b>467</b>
24.1	ITSEC . . . . .	469
24.2	Common Criteria . . . . .	471

24.3	FIPS 140.....	476
24.3.1	Die vier Stufen von FIPS 140 .....	477
24.3.2	Die Sicherheitsbereiche von FIPS 140.....	478
24.3.3	Bewertung von FIPS-140 .....	485
24.4	Fazit und Alternativen .....	486
24.4.1	Open Source als Alternative .....	486
24.4.2	Theorie und Praxis.....	488

## Teil 4

### Public-Key-Infrastrukturen

<b>25</b>	<b>Public-Key-Infrastrukturen</b>	<b>491</b>
25.1	Digitale Zertifikate .....	492
25.1.1	Probleme asymmetrischer Verfahren .....	492
25.1.2	Digitale Zertifikate.....	493
25.2	Vertrauensmodelle .....	495
25.2.1	Direct Trust .....	496
25.2.2	Web of Trust .....	496
25.2.3	Hierarchical Trust .....	498
25.2.4	PKI-Varianten .....	499
25.3	PKI-Standards .....	503
25.3.1	X.509.....	503
25.3.2	PKIX .....	503
25.3.3	ISIS-MTT.....	504
25.3.4	OpenPGP.....	504
25.4	Aufbau und Funktionsweise einer PKI .....	505
25.4.1	Komponenten einer PKI.....	505
25.4.2	Rollen in einer PKI.....	512
25.4.3	Prozesse in einer PKI .....	513
25.5	Identitätsbasierte Krypto-Systeme.....	517
25.5.1	Funktionsweise.....	517
25.5.2	Das Boneh-Franklin-Verfahren.....	518
<b>26</b>	<b>Digitale Zertifikate</b>	<b>521</b>
26.1	X.509v1- und X.509v2-Zertifikate.....	522
26.1.1	Das Format .....	522
26.1.2	Nachteile von X.509v1 und v2.....	523
26.2	X.509v3-Zertifikate .....	524
26.2.1	Die X.509v3-Standarderweiterungen .....	524

26.3	Weitere X.509-Profile . . . . .	527
26.3.1	Die PKIX-Erweiterungen . . . . .	528
26.3.2	Die ISIS-MTT-Erweiterungen . . . . .	529
26.3.3	X.509-Attribut-Zertifikate . . . . .	529
26.3.4	X.509-Fazit . . . . .	531
26.4	OpenPGP-Zertifikate . . . . .	532
26.4.1	OpenPGP-Pakete . . . . .	532
26.4.2	OpenPGP-Zertifikatsformat . . . . .	534
26.4.3	Unterschiede zu X.509 . . . . .	535
26.5	CV-Zertifikate . . . . .	536
<b>27</b>	<b>PKI-Prozesse im Detail</b>	<b>537</b>
27.1	Anwender-Enrollment . . . . .	537
27.1.1	Schritt 1: Registrierung . . . . .	538
27.1.2	Schritt 2: Zertifikate-Generierung . . . . .	539
27.1.3	Schritt 3: PSE-Übergabe . . . . .	540
27.1.4	Enrollment-Beispiele . . . . .	541
27.1.5	Zertifizierungsanträge . . . . .	544
27.2	Recovery . . . . .	546
27.2.1	Schlüsselverlust-Problem . . . . .	547
27.2.2	Chef-Sekretärin-Problem . . . . .	548
27.2.3	Urlauber-Vertreter-Problem . . . . .	549
27.2.4	Virens Scanner-Problem . . . . .	550
27.3	Abruf von Sperrinformationen . . . . .	551
27.3.1	Sperrlisten . . . . .	552
27.3.2	Online-Sperrprüfung . . . . .	556
27.3.3	Weitere Formen des Abrufs von Sperrinformationen . . . . .	557
<b>28</b>	<b>Spezielle Fragen beim Betrieb einer PKI</b>	<b>561</b>
28.1	Outsourcing oder Eigenbetrieb? . . . . .	561
28.2	Gültigkeitsmodelle . . . . .	563
28.2.1	Schalenmodell . . . . .	564
28.2.2	Kettenmodell . . . . .	565
28.3	Certificate Policy und CPS . . . . .	566
28.3.1	Was steht in einem CPS und einer Certification Policy? . . . . .	567
28.3.2	Nachteile von RFC 3647 . . . . .	571
28.4	Policy-Hierarchien . . . . .	575
28.4.1	Hierarchietiefe . . . . .	575
28.4.2	Policy Mapping . . . . .	575
28.4.3	Policy-Hierarchien in der Praxis . . . . .	577

<b>29</b>	<b>Beispiel-PKIs</b>	<b>579</b>
29.1	Signaturgesetze und dazugehörige PKIs	580
29.1.1	EU-Signaturrechtlinie	580
29.1.2	Deutsches Signaturgesetz	581
29.1.3	Österreichisches Signaturgesetz	584
29.1.4	Schweizer ZertES	585
29.1.5	Fazit	585
29.2	Die PKIs elektronischer Ausweise	586
29.2.1	Die PKI des elektronischen Reisepasses	586
29.2.2	PKIs elektronischer Personalausweise	587
29.2.3	PKIs elektronischer Krankenversichertenkarten	587
29.3	Weitere PKIs	588
29.3.1	Organisationsinterne PKIs	588
29.3.2	Kommerzielle Trust Center	589
29.4	Übergreifende PKIs	591
29.4.1	Verwaltungs-PKI	591
29.4.2	European Bridge-CA	592
29.4.3	DFN-PCA	592
29.4.4	Wurzel-CAs	593

## Teil 5

### Kryptografische Netzwerkprotokolle

<b>30</b>	<b>Kryptografie im OSI-Modell</b>	<b>597</b>
30.1	Das OSI-Modell	598
30.1.1	Die Schichten des OSI-Modells	598
30.1.2	Die wichtigsten Netzwerkprotokolle im OSI-Modell	599
30.2	In welcher Schicht wird verschlüsselt?	601
30.2.1	Kryptografie in Schicht 7 (Anwendungsschicht)	601
30.2.2	Kryptografie in Schicht 4 (Transportschicht)	602
30.2.3	Schicht 3 (Vermittlungsschicht)	603
30.2.4	Schicht 2 (Sicherungsschicht)	604
30.2.5	Schicht 1 (Bit-Übertragungsschicht)	604
30.2.6	Fazit	605
<b>31</b>	<b>Krypto-Standards für OSI-Schicht 1</b>	<b>607</b>
31.1	Krypto-Erweiterungen für ISDN	607
31.2	Kryptografie im GSM-Standard	609
31.2.1	Wie GSM Kryptografie einsetzt	610
31.2.2	Sicherheit von GSM	611



31.3	Kryptografie im UMTS-Standard .....	612
31.3.1	Von UMTS verwendete Krypto-Verfahren .....	612
31.3.2	UMTS-Krypto-Protokolle .....	613
<b>32</b>	<b>Krypto-Standards für OSI-Schicht 2</b>	<b>617</b>
32.1	Krypto-Erweiterungen für PPP .....	618
32.1.1	CHAP und MS-CHAP .....	619
32.1.2	EAP .....	619
32.1.3	ECP und MPPE .....	620
32.1.4	Virtuelle Private Netze in Schicht 2 .....	620
32.2	Kryptografie für WLANs .....	623
32.2.1	WEP .....	623
32.2.2	WPA .....	626
32.2.3	WPA2 .....	628
32.3	Kryptografie für Bluetooth .....	628
32.3.1	Grundlagen der Bluetooth-Kryptografie .....	629
32.3.2	Bluetooth-Authentifizierung und -Verschlüsselung .....	633
32.3.3	Angriffe auf die Bluetooth-Sicherheitsarchitektur .....	634
<b>33</b>	<b>IPsec (Schicht 3)</b>	<b>637</b>
33.1	Bestandteile von IPsec .....	638
33.1.1	ESP .....	638
33.1.2	AH .....	639
33.2	IKE .....	640
33.2.1	ISAKMP .....	641
33.2.2	Wie IKE ISAKMP nutzt .....	642
33.3	Kritik an IPsec .....	644
33.4	Virtuelle Private Netze mit IPsec .....	645
<b>34</b>	<b>SSL und TLS (Schicht 4)</b>	<b>647</b>
34.1	Funktionsweise von SSL .....	648
34.1.1	Protokolleigenschaften .....	649
34.1.2	SSL-Teilprotokolle .....	649
34.2	SSL-Protokollablauf .....	650
34.2.1	Das Handshake-Protokoll .....	650
34.2.2	Das ChangeCipherSpec-Protokoll .....	651
34.2.3	Das Alert-Protokoll .....	651
34.2.4	Das ApplicationData-Protokoll .....	652
34.3	SSL in der Praxis .....	652
34.3.1	Vergleich zwischen IPsec und SSL .....	653
34.3.2	VPNs mit SSL .....	655

<b>35</b>	<b>Verschlüsselte und signierte E-Mails (Schicht 7)</b>	<b>657</b>
35.1	E-Mail und Kryptografie . . . . .	658
35.1.1	Kryptografie für E-Mails . . . . .	658
35.2	S/MIME . . . . .	661
35.2.1	S/MIME-Format. . . . .	662
35.2.2	S/MIME-Profil von ISIS-MTT . . . . .	663
35.2.3	Bewertung von S/MIME. . . . .	663
35.3	OpenPGP . . . . .	664
35.3.1	OpenPGP . . . . .	664
35.3.2	Bewertung von OpenPGP. . . . .	664
35.4	Abholen von E-Mails: POP und IMAP . . . . .	665
35.4.1	Gefahren beim Abholen von E-Mails . . . . .	666
35.4.2	Krypto-Zusätze für IMAP . . . . .	667
35.4.3	Krypto-Zusätze für POP. . . . .	668
<b>36</b>	<b>Weitere Krypto-Protokolle der Anwendungsschicht</b>	<b>669</b>
36.1	Kryptografie im World Wide Web . . . . .	669
36.1.1	Basic Authentication . . . . .	670
36.1.2	Digest Access Authentication . . . . .	671
36.1.3	NTLM . . . . .	671
36.1.4	HTTP über SSL (HTTPS). . . . .	671
36.1.5	Was es sonst noch gibt . . . . .	672
36.2	Kryptografie für Echtzeitdaten im Internet (RTP). . . . .	673
36.2.1	SRTP . . . . .	673
36.2.2	SRTP-Schlüsselaustausch . . . . .	674
36.2.3	Bewertung von SRTP . . . . .	676
36.3	Secure Shell (SSH) . . . . .	676
36.3.1	Entstehungsgeschichte der Secure Shell. . . . .	677
36.3.2	Funktionsweise der Secure Shell. . . . .	678
36.3.3	Bewertung der Secure Shell. . . . .	681
36.4	Online-Banking mit HBCI . . . . .	682
36.4.1	Der Standard . . . . .	682
36.4.2	Bewertung von HBCI und FinTS . . . . .	684
36.5	Weitere Krypto-Protokolle in Schicht 7 . . . . .	685
36.5.1	Krypto-Erweiterungen für SNMP. . . . .	685
36.5.2	DNSSEC und TSIG . . . . .	686
36.5.3	Kryptografie für SAP R/3 . . . . .	689
36.5.4	SASL . . . . .	690
36.5.5	Sicheres NTP und sicheres SNTP . . . . .	691

<b>37</b>	<b>Noch mehr Kryptografie in der Anwendungsschicht</b>	<b>693</b>
37.1	Dateiverschlüsselung . . . . .	693
37.1.1	Manuelle Dateiverschlüsselung . . . . .	694
37.1.2	Transparente Dateiverschlüsselung . . . . .	695
37.2	Code Signing . . . . .	696
37.3	Online-Bezahlsysteme . . . . .	697
37.3.1	Kreditkartensysteme . . . . .	698
37.3.2	Kontensysteme . . . . .	699
37.3.3	Bargeldsysteme . . . . .	700
37.3.4	Einige aktuelle Online-Bezahlsysteme . . . . .	702
37.4	Digital Rights Management. . . . .	705
37.4.1	DRM und Kryptografie. . . . .	706
37.4.2	Beispiele für DRM-Systeme. . . . .	708

## Teil 6

### Mehr über Kryptografie

<b>38</b>	<b>Krypto-Wettbewerbe</b>	<b>715</b>
38.1	Kryptoanalyse-Wettbewerbe . . . . .	715
38.2	Algorithmen-Wettbewerbe . . . . .	721
<b>39</b>	<b>Wer in der Kryptografie eine Rolle spielt</b>	<b>727</b>
39.1	Die zehn wichtigsten Personen. . . . .	727
39.2	Die zehn wichtigsten Unternehmen . . . . .	737
39.3	Die fünf wichtigsten Non-Profit-Organisationen . . . . .	742
<b>40</b>	<b>Wo Sie mehr zum Thema erfahren</b>	<b>747</b>
40.1	Die wichtigsten Informationsquellen . . . . .	748
40.2	Die zehn wichtigsten Bücher . . . . .	754
40.3	Die zehn wichtigsten Webseiten. . . . .	761
<b>41</b>	<b>Das letzte Kapitel</b>	<b>765</b>
41.1	Die zehn größten Krypto-Flops . . . . .	765
41.2	Schlangenöl . . . . .	771
41.3	Zehn populäre Krypto-Irrtümer . . . . .	780
41.4	Murphys zehn Gesetze der Kryptografie . . . . .	783

## Anhang

<b>Bildnachweis</b>	<b>787</b>
<b>Literatur</b>	<b>789</b>
<b>Index</b>	<b>811</b>