

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	39
5	Die Enigma und andere Verschlüsselungsmaschinen	59

Teil 2 Moderne Kryptografie

6	Der Data Encryption Standard	81
7	Chiffren-Design	93
8	Der Advanced Encryption Standard (AES)	127
9	AES-Kandidaten	139
10	Symmetrische Verschlüsselungsverfahren, die nach dem AES entstanden sind	159
11	Asymmetrische Verschlüsselung	175
12	Digitale Signaturen	201
13	Weitere asymmetrische Krypto-Verfahren	211
14	Kryptografische Hashfunktionen	225
15	Kryptografische Zufallsgeneratoren	265
16	Stromchiffren	281

Teil 3 Implementierung von Kryptografie

17	Real-World-Attacks	319
18	Standardisierung in der Kryptografie	347
19	Betriebsarten und Datenformatierung	367

20	Kryptografische Protokolle	383
21	Authentifizierung	403
22	Verteilte Authentifizierung	421
23	Krypto-Hardware und Krypto-Software	435
24	Weitere kryptografische Werkzeuge	455
25	Evaluierung und Zertifizierung	481

Teil 4 Public-Key-Infrastrukturen

26	Public-Key-Infrastrukturen	505
27	Digitale Zertifikate	535
28	PKI-Prozesse im Detail	549
29	Spezielle Fragen beim Betrieb einer PKI	573
30	Beispiel-PKIs	589

Teil 5 Kryptografische Netzwerkprotokolle

31	Kryptografie im OSI-Modell	605
32	Krypto-Standards für OSI-Schicht 1	617
33	Krypto-Standards für OSI-Schicht 2	627
34	IPsec (Schicht 3)	645
35	SSL und TLS (Schicht 4)	655
36	E-Mail-Verschlüsselung und -Signierung (Schicht 7)	663
37	Weitere Krypto-Protokolle der Anwendungsschicht	673
38	Noch mehr Kryptografie in der Anwendungsschicht	695

Teil 6 Mehr über Kryptografie

39	Wo Sie mehr zum Thema erfahren	719
40	Kryptografisches Sammelsurium	733

Anhang

Bildnachweis	763
Literatur	765
Index	791

Inhaltsverzeichnis

Teil 1

Wozu Kryptografie?

1	Einleitung	3
1.1	Kryptografie heute.	4
1.2	Die fünfte Ausgabe	5
1.3	Mein Bedauern, meine Bitten und mein Dank	6
2	Was ist Kryptografie und warum ist sie so wichtig?	9
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?	12
2.3.1	Wirtschaftsspionage	13
2.3.2	Kommerz im Netz	13
2.3.3	Die Privatsphäre	14
2.4	Anwendungen der Kryptografie.	14
2.5	Und wer zum Teufel ist Alice?	15
3	Wie Daten abgehört werden können	17
3.1	Mallory am Übertragungsmedium.	18
3.1.1	Kupferkabel	18
3.1.2	Glasfaser	18
3.1.3	Drahtlose Datenübertragung.	19
3.1.4	Satellit	19
3.2	Mallory am Gerät	20
3.2.1	Netzkomponenten.	20
3.2.2	Mitlesen und Verändern von Dateien	20

3.3	Mallory in Computernetzen	21
3.3.1	Telefon	21
3.3.2	Abhören im LAN	21
3.3.3	ISDN-Sicherheitsprobleme	22
3.3.4	DSL	23
3.3.5	Mobilfunk	23
3.3.6	WLANs	24
3.4	Mallory im Internet	24
3.4.1	ARP-Spoofing	24
3.4.2	Abhörangriffe auf Router	25
3.4.3	IP-Spoofing	25
3.4.4	DNS-Spoofing	25
3.4.5	Mitlesen von E-Mails	27
3.4.6	URL-Spoofing	27
3.4.7	Abhören von Internettelefonie	28
3.5	Ein paar Fälle aus der Praxis	28
3.5.1	Abgehörte E-Mails	28
3.5.2	Abgehörte Telefonate	29
3.5.3	Abgehörte Faxe	31
3.5.4	Weitere Fälle	32
3.6	Ist Kryptografie gefährlich?	32
3.6.1	Nachteile einer Krypto-Beschränkung	34
3.6.2	Vorteile einer Krypto-Beschränkung	35
3.6.3	Fazit	37
4	Symmetrische Verschlüsselung	39
4.1	Symmetrische Verschlüsselung	39
4.1.1	Kryptografische Fachbegriffe	41
4.1.2	Angriffe auf Verschlüsselungsverfahren	41
4.2	Monoalphabetische Substitutionschiffren	42
4.2.1	Cäsar-Chiffre	43
4.2.2	Freie Buchstabensubstitution	44
4.2.3	Homophone Chiffre	45
4.2.4	Bigramm-Substitution	47
4.2.5	Wörter-Codes und Nomenklatoren	48
4.3	Polyalphabetische Substitutionschiffren	49
4.3.1	Vigenère-Chiffre	49
4.3.2	Vernam-Chiffre	50
4.3.3	One-Time-Pad	51
4.4	Permutationschiffren	52

4.5	Ungelöste Verschlüsselungen	55
4.5.1	Das Voynich-Manuskript	56
4.5.2	Das Thouless-Kryptogramm	56
4.5.3	Dorabella-Chiffre	57
5	Die Enigma und andere Verschlüsselungsmaschinen	59
5.1	Rotorchiffren.	60
5.1.1	Heberns Rotormaschine	61
5.1.2	Die Enigma	62
5.1.3	Weitere Rotor-Chiffriermaschinen	66
5.2	Andere Verschlüsselungsmaschinen	67
5.2.1	Die Kryha-Maschine	67
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

6	Der Data Encryption Standard	81
6.1	DES-Grundlagen	81
6.2	Funktionsweise des DES	83
6.2.1	Die Rundenfunktion F.	84
6.2.2	Die Schlüsselaufbereitung des DES	85
6.2.3	Entschlüsseln mit dem DES	86
6.3	Sicherheit des DES.	87
6.3.1	Vollständige Schlüsselsuche.	87
6.3.2	Differenzielle und lineare Kryptoanalyse	88
6.3.3	Schwache Schlüssel	88
6.4	Triple-DES	89
6.4.1	Doppel-DES	89
6.4.2	Triple-DES	91
6.5	DES-Fazit	91
7	Chiffren-Design	93
7.1	Chiffren-Design.	93
7.1.1	Anforderungen an die Sicherheit	94
7.1.2	Die ideale Schlüssellänge	97
7.1.3	Hintertüren	99

7.2	Aufbau symmetrischer Verschlüsselungsverfahren	100
7.2.1	Einfache Operationen.	101
7.2.2	Linearität	102
7.2.3	Konfusion und Diffusion	103
7.2.4	Rundenprinzip	104
7.3	Kryptoanalyse-Methoden	107
7.3.1	Differenzielle Kryptoanalyse.	107
7.3.2	Lineare Kryptoanalyse	110
7.3.3	Kryptoanalyse mit Quantencomputern.	112
7.3.4	Weitere Kryptoanalyse-Methoden	112
7.4	Beispiele für symmetrische Verschlüsselungsverfahren	114
7.4.1	RC2 und RC5	114
7.4.2	RC2	114
7.4.3	RC5	117
7.4.4	Blowfish.	119
7.4.5	IDEA und IDEA NXT	121
7.4.6	Skipjack	123
7.4.7	TEA	123
7.4.8	GOST.	125
7.4.9	Weitere Beispiele	125
8	Der Advanced Encryption Standard (AES)	127
8.1	Funktionsweise des AES	128
8.1.1	Rundenaufbau	129
8.1.2	Entschlüsselung mit dem AES.	132
8.1.3	Schlüsselaufbereitung	132
8.2	Mathematische Betrachtung des AES	134
8.3	Sicherheit des AES	135
8.3.1	AES als algebraische Formel.	135
8.3.2	Quadratische Kryptoanalyse	137
8.3.3	Biclique-Kryptoanalyse.	137
8.3.4	Weitere Angriffe.	137
8.4	Bewertung des AES.	138
9	AES-Kandidaten	139
9.1	Serpent	139
9.1.1	Funktionsweise von Serpent	140
9.1.2	S-Box-Design	141
9.1.3	Schlüsselaufbereitung von Serpent	142
9.1.4	Bewertung von Serpent.	143

9.2	Twofish	143
9.2.1	Funktionsweise von Twofish	144
9.2.2	Bewertung von Twofish	145
9.3	RC6	145
9.3.1	Funktionsweise von RC6	146
9.3.2	Schlüsselaufbereitung von RC6	147
9.3.3	Bewertung von RC6	148
9.4	MARS	148
9.5	SAFER	149
9.5.1	Funktionsweise von SAFER+	150
9.5.2	Schlüsselaufbereitung von SAFER+	152
9.5.3	Bewertung von SAFER+	152
9.6	CAST	153
9.7	MAGENTA	154
9.8	Die restlichen AES-Kandidaten	156
9.9	Fazit	157
10	Symmetrische Verschlüsselungsverfahren, die nach dem AES entstanden sind	159
10.1	MISTY1, KASUMI und Camellia	159
10.1.1	MISTY1	160
10.1.2	KASUMI	161
10.1.3	Camellia	162
10.2	CLEFIA	163
10.2.1	Funktionsweise von CLEFIA	163
10.2.2	Bewertung von CLEFIA	164
10.3	Schlanke Verschlüsselungsverfahren	165
10.3.1	SEA	166
10.3.2	PRESENT	168
10.3.3	Bewertung schlanker Verfahren	169
10.4	Tweak-Verfahren	170
10.4.1	Beispiele	170
10.4.2	Threefish	171
10.4.3	Bewertung von Tweak-Verfahren	173
10.5	Weitere symmetrische Verschlüsselungsverfahren	173
11	Asymmetrische Verschlüsselung	175
11.1	Ein bisschen Mathematik	178
11.1.1	Modulo-Rechnen	178
11.1.2	Einwegfunktionen und Falltürfunktionen	184

11.2	Der Diffie-Hellman-Schlüsselaustausch.	185
11.2.1	Funktionsweise von Diffie-Hellman	185
11.2.2	MQV	188
11.3	RSA	190
11.3.1	Funktionsweise des RSA-Verfahrens	190
11.3.2	Ein Beispiel.	192
11.3.3	Sicherheit des RSA-Verfahrens	192
11.3.4	RSA und der Chinesische Restsatz	196
11.4	Symmetrisch und asymmetrisch im Zusammenspiel	198
11.4.1	Unterschiede zwischen symmetrisch und asymmetrisch . . .	198
11.4.2	Hybridverfahren.	199
12	Digitale Signaturen	201
12.1	Was ist eine digitale Signatur?	202
12.2	RSA als Signaturverfahren	203
12.2.1	Funktionsweise.	203
12.2.2	Sicherheit von RSA-Signaturen.	203
12.3	Signaturen auf Basis des diskreten Logarithmus	204
12.3.1	ElGamal-Verfahren	205
12.3.2	DSA	206
12.3.3	Weitere DLSSs	209
12.4	Unterschiede zwischen DLSSs und RSA	209
13	Weitere asymmetrische Krypto-Verfahren	211
13.1	Krypto-Systeme auf Basis elliptischer Kurven	212
13.1.1	Mathematische Grundlagen	212
13.1.2	ECC-Verfahren	215
13.1.3	Die wichtigsten ECC-Verfahren	216
13.2	Weitere asymmetrische Verfahren.	217
13.2.1	NTRU	217
13.2.2	XTR.	220
13.2.3	Krypto-Systeme auf Basis hyperelliptischer Kurven	220
13.2.4	HFE	221
13.2.5	Weitere asymmetrische Verfahren	223
14	Kryptografische Hashfunktionen	225
14.1	Was ist eine kryptografische Hashfunktion?	226
14.1.1	Nichtkryptografische Hashfunktionen	226
14.1.2	Kryptografische Hashfunktionen	227
14.1.3	Angriffe auf kryptografische Hashfunktionen	228

14.2	MD4-artige Hashfunktionen	236
14.2.1	SHA-1	236
14.2.2	Neue SHA-Varianten	239
14.2.3	MD4	240
14.2.4	MD5	241
14.2.5	RIPEMD-160	241
14.3	SHA-3 (Keccak).	245
14.3.1	Funktionsweise von Keccak.	247
14.4	Weitere Hashfunktionen	250
14.4.1	Tiger	250
14.4.2	WHIRLPOOL	253
14.4.3	Weitere kryptografische Hashfunktionen	256
14.4.4	Hashfunktionen aus Verschlüsselungsverfahren	256
14.4.5	Hashfunktionen aus Tweak-Verfahren	259
14.5	Schlüsselabhängige Hashfunktionen	259
14.5.1	Anwendungsbereiche.	260
14.5.2	Die wichtigsten schlüsselabhängigen Hashfunktionen	260
14.6	Weitere Anwendungen kryptografischer Hashfunktionen	263
14.6.1	Hashbäume	263
14.6.2	Weitere Anwendungen	264
15	Kryptografische Zufallsgeneratoren	265
15.1	Zufallszahlen in der Kryptografie	266
15.1.1	Anforderungen der Kryptografie	267
15.1.2	Echte Zufallsgeneratoren.	267
15.1.3	Pseudozufallsgeneratoren	268
15.1.4	Die Grauzone zwischen echt und pseudo.	269
15.1.5	Mischen von Zufallsquellen	270
15.2	Die wichtigsten Pseudozufallsgeneratoren	271
15.2.1	Kryptografische Hashfunktionen als Fortschaltfunktion.	272
15.2.2	Schlüsselabhängige Hashfunktionen als Fortschaltfunktion.	274
15.2.3	Blockchiffren als Fortschaltfunktion	275
15.2.4	Linear rückgekoppelte Schieberegister.	276
15.2.5	Nichtlinear rückgekoppelte Schieberegister	278
15.2.6	Zahlentheoretische Pseudozufallsgeneratoren	278
15.3	Primzahlgeneratoren	279

16	Stromchiffren	281
16.1	Aufbau und Eigenschaften von Stromchiffren	282
16.1.1	Wie eine Stromchiffre funktioniert	283
16.1.2	Angriffe auf Stromchiffren	284
16.1.3	Stromchiffren und Blockchiffren im Vergleich	284
16.2	RC4	285
16.2.1	Funktionsweise von RC4	286
16.2.2	Bewertung von RC4	287
16.3	A5	289
16.3.1	Funktionsweise von A5	289
16.3.2	Bewertung von A5	290
16.4	E0	290
16.4.1	Funktionsweise von E0	291
16.4.2	Bewertung von E0	294
16.5	Crypto1	295
16.5.1	Funktionsweise von Crypto1	296
16.5.2	Bewertung von Crypto1	296
16.6	Die Verfahren des eSTREAM-Wettbewerbs	297
16.6.1	HC-128	298
16.6.2	Rabbit	300
16.6.3	Salsa20	304
16.6.4	Sosemanuk	306
16.6.5	Trivium	307
16.6.6	Grain	309
16.6.7	MICKEY	311
16.6.8	Erkenntnisse aus dem eSTREAM-Wettbewerb	313
16.7	Welche Stromchiffre ist die beste?	314
16.7.1	Weitere Stromchiffren	314
16.7.2	Welche Stromchiffren sind empfehlenswert?	315

Teil 3

Implementierung von Kryptografie

17	Real-World-Attacks	319
17.1	Seitenkanalangriffe	319
17.1.1	Zeitangriffe	320
17.1.2	Stromangriffe	321
17.1.3	Fehlerangriffe	324
17.1.4	Weitere Seitenkanalangriffe	324

17.2	Malware-Angriffe	325
17.2.1	Malware und digitale Signaturen	326
17.2.2	Vom Entwickler eingebaute Hintertüren	327
17.2.3	Gegenmaßnahmen	328
17.3	Physikalische Angriffe	329
17.3.1	Die wichtigsten physikalischen Angriffe	329
17.3.2	Gegenmaßnahmen	330
17.4	Schwachstellen durch Implementierungsfehler	332
17.4.1	Implementierungsfehler in der Praxis	333
17.4.2	Implementierungsfehler in vielen Variationen	334
17.4.3	Gegenmaßnahmen	335
17.5	Insiderangriffe	337
17.5.1	Unterschätzte Insider	337
17.5.2	Gegenmaßnahmen	338
17.6	Der Anwender als Schwachstelle	339
17.6.1	Schwachstellen durch Anwenderfehler	339
17.6.2	Gegenmaßnahmen	342
17.7	Fazit	345
18	Standardisierung in der Kryptografie	347
18.1	Standards	347
18.1.1	Standardisierungsgremien	348
18.1.2	Standardisierung im Internet	349
18.2	Wissenswertes zum Thema Standards	349
18.3	Wichtige Kryptografie-Standards	350
18.3.1	PKCS	350
18.3.2	IEEE P1363	351
18.3.3	ANSI X.9	352
18.3.4	NSA Suite B	353
18.4	Standards für verschlüsselte und signierte Daten	354
18.4.1	PKCS#7	354
18.4.2	XML Signature und XML Encryption	356
18.4.3	Weitere Formate	358
18.5	Standardisierungswettbewerbe	359
18.5.1	Der DES-Wettbewerb	359
18.5.2	Der AES-Wettbewerb	360
18.5.3	Der SHA-3-Wettbewerb	363
18.5.4	Weitere Wettbewerbe	364

19	Betriebsarten und Datenformatierung	367
19.1	Betriebsarten von Blockchiffren	368
19.1.1	Electronic-Codebook-Modus	368
19.1.2	Cipher-Block-Chaining-Modus	369
19.1.3	Output-Feedback-Modus	370
19.1.4	Cipher-Feedback-Modus	371
19.1.5	Counter-Modus	373
19.1.6	Fazit	374
19.2	Betriebsarten von Tweak-Verfahren	375
19.3	Formaterhaltende Verschlüsselung	376
19.4	Datenformatierung für das RSA-Verfahren.	377
19.4.1	Der PKCS#1-Standard	377
19.4.2	Datenformatierung für die RSA-Verschlüsselung	377
19.4.3	Datenformatierung für RSA-Signaturen	380
19.5	Datenformatierung für DLSSs.	382
20	Kryptografische Protokolle	383
20.1	Protokolle.	383
20.1.1	Konzeptprotokolle	384
20.1.2	Netzwerkprotokolle	385
20.1.3	Eigenschaften von Netzwerkprotokollen	385
20.2	Protokolle in der Kryptografie	387
20.2.1	Eigenschaften kryptografischer Netzwerkprotokolle	388
20.3	Angriffe auf kryptografische Protokolle	389
20.3.1	Replay-Attacke.	390
20.3.2	Spoofing-Attacke	391
20.3.3	Man-in-the-Middle-Attacke	391
20.3.4	Hijacking-Attacke	392
20.3.5	Known-Key-Attacken.	393
20.3.6	Verkehrsflussanalyse	396
20.3.7	Denial-of-Service-Attacke.	397
20.3.8	Sonstige Angriffe	398
20.4	Beispielprotokolle.	398
20.4.1	Beispielprotokoll: Messgerät sendet an PC	398
20.4.2	Weitere Beispielprotokolle	401
21	Authentifizierung	403
21.1	Authentifizierung im Überblick.	403
21.1.1	Etwas, was man weiß.	405
21.1.2	Was man hat	406
21.1.3	Was man ist	407

21.2	Biometrische Authentifizierung	407
21.2.1	Grundsätzliches zur biometrischen Authentifizierung	407
21.2.2	Biometrische Merkmale.	409
21.2.3	Fazit	412
21.3	Authentifizierung in Computernetzen	413
21.3.1	Passwörter im Internet	413
21.3.2	Authentifizierung mit asymmetrischen Verfahren	417
21.3.3	Biometrie in Computernetzen	420
22	Verteilte Authentifizierung	421
22.1	Credential-Synchronisation	422
22.2	Single Sign-On.	422
22.2.1	Lokales SSO	423
22.2.2	Ticket-SSO	424
22.2.3	Web-SSO.	424
22.3	Kerberos	425
22.3.1	Vereinfachtes Kerberos-Protokoll	425
22.3.2	Vollständiges Kerberos-Protokoll	427
22.3.3	Vor- und Nachteile von Kerberos	428
22.4	RADIUS und andere Triple-A-Server.	429
22.4.1	Triple-A-Server	429
22.4.2	Beispiele für Triple-A-Server	431
22.5	SAML	431
22.5.1	Funktionsweise von SAML	432
22.5.2	SAML in der Praxis.	433
23	Krypto-Hardware und Krypto-Software	435
23.1	Krypto-Hardware oder Krypto-Software?	435
23.1.1	Pro Software	436
23.1.2	Pro Hardware	437
23.1.3	Ist Hardware oder Software besser?	437
23.2	Smartcards	438
23.2.1	Smartcards und andere Chipkarten	438
23.2.2	Smartcard-Formfaktoren.	440
23.2.3	Smartcards und Kryptografie	440
23.3	Hardware-Security-Module.	445
23.4	Kryptografie in eingebetteten Systemen	445
23.4.1	Eingebettete Systeme und Kryptografie	446
23.4.2	Kryptografische Herausforderungen in eingebetteten Systemen	447

23.5	RFID und Kryptografie	449
23.5.1	Sicherheitsprobleme beim Einsatz von EPC-Chips	450
23.5.2	RFID und Kryptografie	451
24	Weitere kryptografische Werkzeuge	455
24.1	Management geheimer Schlüssel.	455
24.1.1	Schlüsselgenerierung.	456
24.1.2	Schlüsselspeicherung	458
24.1.3	Schlüsselauthentifizierung	459
24.1.4	Schlüsseltransport und Schlüssel-Backup	459
24.1.5	Schlüsselaufteilung	460
24.1.6	Schlüsselwechsel.	461
24.1.7	Löschen eines Schlüssels.	462
24.1.8	Key Recovery	462
24.2	Trusted Computing und Kryptografie.	463
24.2.1	Trusted Computing und Kryptografie	464
24.2.2	Das Trusted Platform Module	465
24.2.3	Funktionen und Anwendungen des TPM	467
24.2.4	Fazit.	469
24.3	Krypto-APIs	469
24.3.1	PKCS#11	469
24.3.2	MS-CAPI	473
24.3.3	Cryptography API Next Generation (CNG)	475
24.3.4	TokenD	475
24.3.5	ISO/IEC 24727.	475
24.3.6	Universelle Krypto-APIs	477
25	Evaluierung und Zertifizierung	481
25.1	ITSEC.	483
25.2	Common Criteria	485
25.3	FIPS 140.	490
25.3.1	Die vier Stufen von FIPS 140	491
25.3.2	Die Sicherheitsbereiche von FIPS 140	492
25.3.3	Bewertung von FIPS-140	499
25.4	Fazit und Alternativen	500
25.4.1	Open Source als Alternative	500
25.4.2	Theorie und Praxis.	501

Teil 4

Public-Key-Infrastrukturen

26	Public-Key-Infrastrukturen	505
26.1	Warum brauchen wir eine PKI?	505
26.1.1	Authentizität der Schlüssel	506
26.1.2	Sperrung von Schlüsseln	506
26.1.3	Verbindlichkeit	506
26.1.4	Durchsetzen einer Policy	506
26.2	Digitale Zertifikate	507
26.3	Vertrauensmodelle.	508
26.3.1	Direct Trust.	509
26.3.2	Web of Trust.	510
26.3.3	Hierarchical Trust.	511
26.3.4	PKI-Varianten.	512
26.4	PKI-Standards	516
26.4.1	X.509	516
26.4.2	PKIX.	517
26.4.3	Common PKI	517
26.4.4	OpenPGP	518
26.5	Aufbau und Funktionsweise einer PKI.	518
26.5.1	Komponenten einer PKI	518
26.5.2	Rollen in einer PKI	525
26.5.3	Prozesse in einer PKI.	526
26.6	Identitätsbasierte Krypto-Systeme	530
26.6.1	Funktionsweise	530
26.6.2	Das Boneh-Franklin-Verfahren	531
27	Digitale Zertifikate	535
27.1	X.509v1- und X.509v2-Zertifikate	535
27.1.1	Das Format	536
27.1.2	Nachteile von X.509v1 und v2	537
27.2	X.509v3-Zertifikate	537
27.2.1	Die X.509v3-Standarderweiterungen	538
27.3	Weitere X.509-Profile	540
27.3.1	Die PKIX-Erweiterungen.	540
27.3.2	Die Common-PKI-Erweiterungen	541
27.3.3	Attributzertifikate	542
27.3.4	X.509-Fazit.	543

27.4	PGP-Zertifikate	543
27.4.1	OpenPGP-Pakete	544
27.4.2	PGP-Zertifikatsformat	546
27.4.3	Unterschiede zu X.509	547
27.5	CV-Zertifikate	548
28	PKI-Prozesse im Detail	549
28.1	Anwender-Enrollment	549
28.1.1	Schritt 1: Registrierung	550
28.1.2	Schritt 2: Zertifikate-Generierung	551
28.1.3	Schritt 3: PSE-Übergabe	552
28.1.4	Enrollment-Beispiele	552
28.1.5	Zertifizierungsanträge	556
28.2	Recovery	558
28.2.1	Schlüsselverlust-Problem	559
28.2.2	Chef-Sekretärin-Problem	560
28.2.3	Urlauber-Vertreter-Problem	560
28.2.4	Virens Scanner-Problem	561
28.2.5	Geht es auch ohne Recovery?	563
28.3	Abruf von Sperrinformationen	563
28.3.1	Sperrlisten	563
28.3.2	Online-Sperrprüfung	567
28.3.3	Weitere Formen des Abrufs von Sperrinformationen	569
29	Spezielle Fragen beim Betrieb einer PKI	573
29.1	Outsourcing oder Eigenbetrieb?	573
29.2	Gültigkeitsmodelle	575
29.2.1	Schalenmodell	576
29.2.2	Kettenmodell	577
29.3	Certificate Policy und CPS	578
29.3.1	Was steht in einem CPS und einer Certification Policy? ...	579
29.3.2	Nachteile von RFC 3647	582
29.4	Policy-Hierarchien	586
29.4.1	Hierarchietiefe	586
29.4.2	Policy Mapping	587
29.4.3	Policy-Hierarchien in der Praxis	588

30	Beispiel-PKIs	589
30.1	Signaturgesetze und dazugehörnde PKIs	590
30.1.1	EU-Signaturrechtlinie.	590
30.1.2	Deutsches Signaturgesetz.	591
30.1.3	Österreichisches Signaturgesetz.	594
30.1.4	Schweizer ZertES	594
30.1.5	Fazit	595
30.2	Die PKIs elektronischer Ausweise	595
30.2.1	Die PKI des elektronischen Reisepasses	595
30.2.2	PKIs elektronischer Personalausweise	596
30.2.3	PKIs elektronischer Krankenversichertenkarten.	597
30.3	Weitere PKIs	598
30.3.1	Organisationsinterne PKIs.	598
30.3.2	Kommerzielle Trust Center	599
30.4	Übergreifende PKIs	600
30.4.1	European Bridge-CA	600
30.4.2	Verwaltungs-PKI.	601
30.4.3	Wurzel-CAs.	601

Teil 5
Kryptografische Netzwerkprotokolle

31	Kryptografie im OSI-Modell	605
31.1	Das OSI-Modell	605
31.1.1	Die Schichten des OSI-Modells	606
31.1.2	Die wichtigsten Netzwerkprotokolle im OSI-Modell.	607
31.2	In welcher Schicht wird verschlüsselt?	609
31.2.1	Kryptografie in Schicht 7 (Anwendungsschicht)	609
31.2.2	Kryptografie in Schicht 4 (Transportschicht).	610
31.2.3	Schicht 3 (Vermittlungsschicht).	611
31.2.4	Schicht 2 (Sicherungsschicht).	612
31.2.5	Schicht 1 (Bit-Übertragungsschicht).	612
31.2.6	Fazit	613
31.3	Design eines kryptografischen Netzwerkprotokolls	613
31.3.1	Initialisierungsroutine	613
31.3.2	Datenaustauschroutine	614

32	Krypto-Standards für OSI-Schicht 1	617
32.1	Krypto-Erweiterungen für ISDN	617
32.2	Kryptografie im GSM-Standard	618
32.2.1	Wie GSM Kryptografie einsetzt	619
32.2.2	Sicherheit von GSM	620
32.3	Kryptografie im UMTS-Standard	621
32.3.1	Von UMTS verwendete Krypto-Verfahren	621
32.3.2	UMTS-Krypto-Protokolle	623
33	Krypto-Standards für OSI-Schicht 2	627
33.1	Krypto-Erweiterungen für PPP	628
33.1.1	CHAP und MS-CHAP	628
33.1.2	EAP	629
33.1.3	ECP und MPPE	630
33.1.4	Virtuelle Private Netze in Schicht 2	630
33.2	Kryptografie im WLAN	632
33.2.1	WEP	633
33.2.2	WPA	636
33.2.3	WPA2	638
33.3	Kryptografie für Bluetooth	638
33.3.1	Grundlagen der Bluetooth-Kryptografie	639
33.3.2	Bluetooth-Authentifizierung und -Verschlüsselung	643
33.3.3	Angriffe auf die Bluetooth-Sicherheitsarchitektur	644
34	IPsec (Schicht 3)	645
34.1	Bestandteile von IPsec	646
34.1.1	ESP	646
34.1.2	AH	647
34.2	IKE	648
34.2.1	ISAKMP	649
34.2.2	Wie IKE ISAKMP nutzt	650
34.3	Kritik an IPsec	652
34.4	Virtuelle Private Netze mit IPsec	653
35	SSL und TLS (Schicht 4)	655
35.1	Funktionsweise von SSL	656
35.1.1	Protokolleigenschaften	657
35.1.2	SSL-Teilprotokolle	657

35.2	SSL-Protokollablauf	658
35.2.1	Das Handshake-Protokoll	658
35.2.2	Das ChangeCipherSpec-Protokoll	659
35.2.3	Das Alert-Protokoll	659
35.2.4	Das ApplicationData-Protokoll	659
35.3	SSL in der Praxis	659
35.3.1	Vergleich zwischen IPsec und SSL	660
35.3.2	VPNs mit SSL	662
36	E-Mail-Verschlüsselung und -Signierung (Schicht 7)	663
36.1	E-Mail und Kryptografie	664
36.1.1	Kryptografie für E-Mails	664
36.2	S/MIME	667
36.2.1	S/MIME-Format	667
36.2.2	S/MIME-Profil von Common PKI	668
36.2.3	Bewertung von S/MIME	668
36.3	OpenPGP	669
36.3.1	OpenPGP	669
36.3.2	Bewertung von OpenPGP	669
36.4	Abholen von E-Mails: POP und IMAP	670
36.4.1	Gefahren beim Abholen von E-Mails	671
36.4.2	Krypto-Zusätze für IMAP	671
36.4.3	Krypto-Zusätze für POP	672
37	Weitere Krypto-Protokolle der Anwendungsschicht	673
37.1	Kryptografie im World Wide Web	673
37.1.1	Basic Authentication	674
37.1.2	Digest Access Authentication	675
37.1.3	NTLM	675
37.1.4	HTTP über SSL (HTTPS)	675
37.1.5	Was es sonst noch gibt	676
37.2	Kryptografie für Echtzeitdaten im Internet (RTP)	677
37.2.1	SRTP	677
37.2.2	SRTP-Initialisierungsroutinen	678
37.2.3	Bewertung von SRTP	680
37.3	Secure Shell (SSH)	680
37.3.1	Entstehungsgeschichte der Secure Shell	680
37.3.2	Funktionsweise der Secure Shell	681
37.3.3	Bewertung der Secure Shell	684

37.4	Online-Banking mit HBCI	685
37.4.1	Der Standard	685
37.4.2	Bewertung von HBCI und FinTS	687
37.5	Weitere Krypto-Protokolle in Schicht 7	688
37.5.1	Krypto-Erweiterungen für SNMP	688
37.5.2	DNSSEC und TSIG	689
37.5.3	Kryptografie für SAP R/3	691
37.5.4	SASL	692
37.5.5	Sicheres NTP und sicheres SNTP	693
38	Noch mehr Kryptografie in der Anwendungsschicht	695
38.1	Dateiverschlüsselung	695
38.2	Festplattenverschlüsselung	697
38.3	Code Signing	699
38.4	Bezahlkarten	700
38.5	Online-Bezahlsysteme	702
38.5.1	Kreditkartensysteme	703
38.5.2	Kontensysteme	704
38.5.3	Bargeldsysteme	705
38.6	Elektronische Ausweise	706
38.6.1	Elektronische Reisepässe	707
38.6.2	Elektronische Personalausweise	708
38.6.3	Elektronische Gesundheitskarten	709
38.6.4	Weitere elektronische Ausweise	710
38.7	Digital Rights Management	710
38.7.1	Containment und Marking	711
38.7.2	Beispiele für DRM-Systeme	713
38.8	Elektronische Wahlen und Online-Wahlen	716

Teil 6

Mehr über Kryptografie

39	Wo Sie mehr zum Thema erfahren	719
39.1	Buchtipps	719
39.2	Veranstaltungen zum Thema Kryptografie	725
39.3	Zeitschriften zum Thema Kryptografie	727
39.4	Weitere Informationsquellen	729

40	Kryptografisches Sammelsurium	733
40.1	Die zehn wichtigsten Personen der Kryptografie	733
40.2	Die wichtigsten Unternehmen	743
40.3	Non-Profit-Organisationen	747
40.4	Kryptoanalyse-Wettbewerbe	750
40.5	Die zehn größten Krypto-Flops	753
40.6	Murphys zehn Gesetze der Kryptografie	759

Anhang

Bildnachweis	763
Literatur	765
Index	791