

Inhalt

Vorwort	13
1 Grundlagen der Kryptographie.....	15
1.1 Was ist Kryptographie?	16
1.2 Politik und Wirtschaft	17
1.2.1 National Security Agency.....	19
1.2.2 Exportbeschränkungen	20
1.2.3 Schlüsselhinterlegung.....	21
1.3 Klassische Kryptographie	23
1.3.1 Caesars Addition	23
1.3.2 Substitution und Permutation.....	26
1.3.3 Transposition.....	27
1.3.4 Rotormaschinen	28
1.4 Die andere Seite: Kryptanalyse.....	30
1.4.1 Allgemeine Vorgehensweise	31
1.4.2 Negativsuche	32
1.4.3 Statistische Methoden.....	33
1.5 Weitere Verfahren	36
1.5.1 Bitweises XOR.....	36
1.5.2 Individueller Schlüssel	36
1.5.3 Steganographie.....	39
1.5.4 Digitale Wasserzeichen	41
1.6 Zusammenfassung.....	41
2 Zahlentheorie.....	43
2.1 Modulare Arithmetik.....	47
2.1.1 Ermittlung des Kehrwerts einer Zahl	48
2.1.2 Der kleine Satz von Fermat	50
2.1.3 Eulersche Phi-Funktion	51
2.1.4 Primitive Zahlen.....	52
2.2 Primzahltests	54
2.2.1 Sieb des Eratosthenes	56
2.2.2 Die klassische Methode	57
2.2.3 Primzahltest nach Pierre de Fermat	58
2.2.4 Probabilistische Tests	60
2.3 Zufälliges	61
2.3.1 Pseudozufallsfolgen.....	62

Inhalt

2.3.2	Kryptographisch sichere Zufallsfolgen	63
2.4	Einwegfunktionen	64
2.4.1	Diskreter Logarithmus	65
2.4.2	Faktorisierungsproblem.....	66
2.5	Zusammenfassung.....	67
3	Symmetrische Verfahren	69
3.1	Das erste moderne Verfahren: DES.....	77
3.1.1	Funktionsweise von DES	78
3.1.2	Sicherheit von DES.....	80
3.1.3	Differentielle Kryptanalyse	81
3.1.4	Lineare Kryptanalyse	82
3.2	Dreifache Sicherheit: TripleDES.....	82
3.3	Der einstige Hoffnungsträger: IDEA	84
3.3.1	Funktionsweise	84
3.3.2	Sicherheit und Patente.....	88
3.4	Der neue Standard – AES.....	89
3.4.1	Eine intensive Suche	89
3.4.2	... and the winner is.....	90
3.4.3	Funktionsweise von Rijndael	91
3.4.4	Sicherheit von Rijndael.....	94
3.5	Veröffentlichtes Geheimnis: RC4.....	94
3.5.1	Beschreibung von RC4	94
3.5.2	Sicherheit von RC4.....	96
3.6	Gut, schnell, lizenzfrei: Blowfish.....	96
3.6.1	Gesamtablauf.....	97
3.6.2	Funktionen und Teilschlüssel.....	99
3.6.3	Sicherheit von Blowfish.....	100
3.6.4	Ein würdiger Nachfolger.....	100
3.7	Implementierung in Perl.....	102
3.7.1	Installation der Module	102
3.7.2	Caesar-Addition	102
3.7.3	DES im ECB-Modus.....	103
3.7.4	Blowfish im CBC-Modus.....	104
3.7.5	Stromchiffrierung mit RC4	105
3.8	Zusammenfassung.....	105
4	Asymmetrische Verfahren.....	109
4.1	Schlüsselaustauschverfahren	111
4.2	Diffie-Hellman-Verfahren.....	112
4.2.1	Funktionsweise	112
4.2.2	Sicherheit des Diffie-Hellman-Verfahrens.....	114

4.3	Der Quasi-Standard: RSA.....	115
4.3.1	Funktionsweise von RSA.....	115
4.3.2	Sicherheit von RSA.....	118
4.3.3	Man-in-the-Middle-Angriff	120
4.3.4	Patente	120
4.4	ElGamal.....	121
4.5	Höhere Mathematik: ECC	122
4.6	Zusammenfassung.....	123
5	Digitale Signaturen.....	125
5.1	Hashfunktionen	127
5.2	Arbeitsweise einzelner Verfahren.....	129
5.2.1	MD5.....	130
5.2.2	SHA	131
5.2.3	Sicherheit der Verfahren.....	132
5.2.4	Weitere Verfahren.....	133
5.3	Digitale Signaturen.....	133
5.3.1	Das deutsche Signaturgesetz.....	134
5.3.2	Digital Signature Standard.....	136
5.4	Anwendung digitaler Signaturen	137
5.4.1	Erzeugen eines Hashwerts	137
5.4.2	Signieren mit ElGamal	138
5.5	Sicherheit digitaler Signaturen	140
5.5.1	Der Geburtstagsangriff	140
5.5.2	Verdeckte Kanäle.....	141
5.6	Zusammenfassung.....	143
6	OpenSSH.....	145
6.1	Sicherheit im lokalen Netz	145
6.1.1	Sniffer.....	145
6.1.2	IP-Spoofing	147
6.1.3	Gegenmaßnahmen.....	151
6.2	Secure Shell – SSH	152
6.2.1	Das OpenSSH-Projekt	153
6.2.2	Installation von OpenSSL.....	155
6.3	Installation von OpenSSH	157
6.4	Konfiguration von OpenSSH	161
6.4.1	Die Server-Konfiguration	161
6.4.2	Die Konfiguration des Clients	164
6.5	Die einzelnen Programme	166
6.5.1	Erzeugen der Schlüsselpaare: ssh-keygen	166
6.5.2	Datentransfer: scp.....	167

6.5.3	Das Client-Programm: ssh.....	170
6.5.4	Die Verwaltung der Passphrase	175
6.5.5	Port-Forwarding.....	177
6.5.6	Eine alternative zu FTP: sftp.....	178
6.5.7	Scanner im eigenen Dienst.....	179
6.6	Sicherheit von OpenSSH.....	180
6.6.1	Die Qual der Wahl	180
6.6.2	Abwehr von Man-in-the-middle-Angriffen.....	182
6.7	Zusammenfassung.....	183
7	E-Mail.....	185
7.1	Übertragungsprotokolle.....	185
7.2	E-Mail als Sicherheitsrisiko	187
7.2.1	Echelon.....	187
7.2.2	Carnivore	191
7.2.3	Magic Lantern	193
7.3	Sichere Übertragung von E-Mails	195
7.3.1	Der erste Standard: PEM.....	195
7.3.2	Mailtrust	197
7.3.3	S/MIME.....	198
7.3.4	OpenPGP	199
7.4	Pretty Good Privacy – PGP	200
7.4.1	Entwicklung.....	200
7.4.2	Funktionsweise von PGP.....	202
7.4.3	Web of Trust.....	203
7.5	PGP der ersten Stunde.....	205
7.5.1	Installation und Konfiguration	205
7.5.2	Schlüsselpaar erzeugen	209
7.5.3	Schlüsselverwaltung.....	213
7.5.4	E-Mails verschlüsseln	218
7.5.5	Nachrichten signieren	220
7.5.6	Kurzübersicht.....	224
7.6	GnuPG.....	226
7.6.1	Installation und Konfiguration	226
7.6.2	Schlüsselpaar generieren.....	228
7.6.3	Im- und Export der öffentlichen Schlüssel.....	232
7.6.4	E-Mails verschlüsseln	234
7.6.5	Nachrichten signieren	235
7.6.6	Schlüsselverwaltung.....	237
7.6.7	Öffentliche Keyserver	240
7.6.8	Kurzübersicht.....	242
7.6.9	Grafische Unterstützung.....	244

7.7	Sicherheit von PGP und GnuPG	246
7.7.1	Schutz des privaten Schlüssels.....	246
7.7.2	Sicherheit öffentlicher Schlüssel.....	247
7.7.3	PGP geknackt?	249
7.8	Zusammenfassung	250
8	SSL-Server.....	253
8.1	Die Gefahren im globalen Netz	253
8.2	Gesicherte Übertragung mit SSL	254
8.2.1	Protokollaufbau	254
8.2.2	Verbindungsaufbau	256
8.3	Apache-Webserver	258
8.3.1	Installation	258
8.3.2	Konfiguration	268
8.4	Zertifikate	274
8.4.1	X.509-Zertifikate.....	275
8.4.2	X.509v3-Zertifikate.....	276
8.4.3	Netscape Certificate Extensions	278
8.4.4	OpenSSL konfigurieren	279
8.5	Generieren der Zertifikate	282
8.5.1	Root-CA.....	282
8.5.2	Server-CA	285
8.5.3	SSL-Server-Zertifikate	287
8.6	Client-Authentifizierung.....	288
8.6.1	Client-Authentifizierung über Passwortabfrage	289
8.6.2	Client-Authentifizierung mit Zertifikaten	293
8.7	Zertifikate widerrufen: CRL.....	295
8.7.1	Konfiguration	297
8.7.2	Widerruf eines Zertifikats.....	298
8.8	Zusammenfassung	299
9	Virtual Private Networks.....	301
9.1.1	Vorteile von VPNs	301
9.1.2	Konzepte	302
9.2	Übertragungsprotokolle	303
9.2.1	Point-to-Point Tunneling Protocol	303
9.2.2	Layer 2 Tunneling Protocol	304
9.2.3	IP Security Protocol Suite.....	304
9.2.4	Schlüsselverwaltung	307
9.3	Das FreeS/WAN-Projekt	308
9.3.1	Installation	308
9.3.2	Authentifizierungsmöglichkeiten.....	311

9.3.3	Konfiguration.....	312
9.4	IPSec unter BSD	316
9.4.1	Sicherheitsrichtlinien	316
9.4.2	Konfiguration.....	317
9.5	Aktivieren der Tunnel	319
9.6	Fazit.....	321
10	Verzeichnisdienste.....	323
10.1	OpenLDAP	326
10.1.1	OpenLDAP installieren	327
10.1.2	Die Server-Konfiguration.....	328
10.1.3	Die OpenLDAP-Datenbank.....	330
10.1.4	Informationen abfragen.....	333
10.1.5	Objekte hinzufügen.....	337
10.1.6	Objekte ändern und löschen	338
10.1.7	Zugriffsrechte	340
10.2	Administrations-Programme	341
10.2.1	User Directory	341
10.2.2	GQ.....	345
10.2.3	Eigene Client-Programme schreiben	347
10.3	Zusammenfassung.....	350
11	Weitere Anwendungen.....	353
11.1	Verzeichnisse verschlüsseln	353
11.1.1	Installation	354
11.1.2	Verzeichnisse anlegen.....	355
11.1.3	Fazit.....	356
11.2	Passwort-Authentifizierung	357
11.2.1	Sichere Passworte	357
11.2.2	cracklib.....	358
11.2.3	Crack	360
11.2.4	John	362
11.3	Einmalpassworte.....	363
11.3.1	Installation	363
11.3.2	Die Arbeitsweise von OPIE.....	364
11.3.3	Fazit.....	367
11.4	Das Kerberos-Authentifizierungssystem.....	367
11.4.1	Funktionsweise von Kerberos.....	368
11.4.2	KDC einrichten.....	371
11.4.3	Der Kerberos-Client.....	375
11.4.4	Fazit.....	376
11.5	Sichern der Datenintegrität	376

11.5.1	Installation	377
11.5.2	Konfiguration	378
11.5.3	Anlegen einer Referenzdatenbank	380
11.5.4	Integritätsprüfung	381
11.5.5	Datenbank aktualisieren	385
12	Public Key Infrastructure	387
12.1	Aufbau einer PKI	389
12.1.1	Umgang mit privaten Schlüsseln	389
12.1.2	Administration der CA	390
12.1.3	Bekanntgabe der CA-Zertifikate	391
12.1.4	Sicherheitsrichtlinien	392
12.1.5	Registrierungsstellen	394
12.2	Unterstützende Programme	395
12.2.1	pyCA	395
12.2.2	OpenCA	398
12.2.3	IDX-PKI	401
12.3	Standardisierungen	402
12.3.1	PKIX	403
12.3.2	SPKI	404
12.3.3	PKCS	405
12.4	Abschließende Bemerkungen	406
Anhang A:	Programme	409
A.1	Die Bibliothek GNU Multiple Precision – GMP	409
A.2	Beispiele	412
A.2.1	anz_buchstaben.c	414
A.2.2	caesar.c	415
A.2.3	fermat.c	416
A.2.4	ggt.c	417
A.2.5	ggt_mp.c	418
A.2.6	kasiski.c	419
A.2.7	prim_div_test.c	424
A.2.8	sieb.c	425
A.2.9	vigenere.c	427
A.2.10	vigenere_decrypt.c	428
A.2.11	vigenere_key.c	430
Anhang B:	Konfigurationsdateien	433
B.1	config.txt	434
B.2	httpd.conf	434
B.3	ipsec.conf	438

Inhalt

B.4	isakmpd.conf	439
B.5	isakmpd.policy.....	441
B.6	openssl.cnf.....	442
B.7	slapd.conf	447
B.8	ssh_config.....	448
B.9	sshd_config.....	448
B.10	kwmodn.c	449
Anhang C: RFCs.....		451
Anhang D: Informationsquellen.....		457
D.1	Organisationen/Institutionen	457
D.2	Newsgroups	459
D.3	Personen	460
D.4	Software	461
D.5	Protokolle/Standards	461
D.6	Zertifizierungsstellen	463
D.7	Keyserver.....	463
Literaturverzeichnis.....		465
Index		469