

Inhaltsverzeichnis

	Vorwort	17
	Einleitung	19
1	Warum Kryptographie?	23
1.1	Sicherheit durch Computer-Betriebssysteme	24
1.1.1	Wie Betriebssysteme funktionieren	24
1.1.2	Standardmäßige Betriebssystemsicherheit: Berechtigungen	25
1.1.3	Angriffe auf Passwörter	26
1.2	Angriffe, die das Betriebssystem umgehen	28
1.2.1	Daten-Recovery-Angriff	29
1.2.2	Memory-Reconstruction-Angriff	31
1.3	Zusätzlicher Schutz durch Kryptographie	32
1.4	Die Rolle der Kryptographie für die Sicherheit von Daten	35
2	Symmetrische Kryptographie	37
2.1	Einige Fachbegriffe der Kryptographie	41
2.2	Was ist ein Schlüssel?	43
2.3	Warum wird ein Schlüssel benötigt?	44
2.4	Einen Schlüssel erzeugen	50
2.4.1	Ein Zufallszahlengenerator	51
2.4.2	Ein Pseudozufallszahlengenerator	51
2.5	Angriffe auf verschlüsselte Daten	54
2.5.1	Den Schlüssel angreifen	54
2.5.2	Den Algorithmus brechen	61
2.5.3	Die Zeit messen, die zum Brechen Ihrer Nachricht benötigt wird	62
2.6	Symmetrische Algorithmen: Die Schlüsseltabelle	63
2.7	Symmetrische Algorithmen: Block- und Stromchiffrierungen im Vergleich	64
2.7.1	Blockchiffrierungen	64
2.7.2	Stromchiffrierungen	69
2.7.3	Block oder Stream – was ist besser?	71
2.8	Digital Encryption Standard	72

2.9	Triple DES	73
2.10	Kommerzielle DES-Alternativen	76
2.10.1	Advanced Encryption Standard	77
2.11	Zusammenfassung	77
2.12	Ein Beispiel aus der Praxis: Oracle-Datenbanken	78
3	Die Verwaltung symmetrischer Schlüssel	81
3.1	Passwortbasierte Chiffrierung	81
3.1.1	Algorithmen und den KEK mischen	84
3.1.2	Die Notwendigkeit von Salt	85
3.1.3	Salt mit Chiffretext speichern	86
3.1.4	Gründe für den Einsatz zweier Schlüssel (Sitzungsschlüssel und KEK)	86
3.1.5	Leichtes Programmieren	89
3.1.6	Passwortbasierte Chiffrierungen brechen	91
3.1.7	Ein Angriff auf ein Passwort verzögern	93
3.1.8	Gute Passwörter	96
3.1.9	Passwortgeneratoren	98
3.2	Hardwarebasierte SchlüsselSpeicherung	98
3.2.1	Tokens	99
3.2.2	Smart-Cards	101
3.2.3	USB-Token	102
3.2.4	Tokens als Passwort-Speichergeräte	103
3.2.5	Kryptobeschleuniger	103
3.2.6	Hardwaregeräte und Zufallszahlen	105
3.3	Biometrie	106
3.4	Zusammenfassung	107
3.5	Beispiele aus der Praxis	107
3.5.1	Keon-Desktop	107
3.5.2	Andere Produkte	109
4	Das Schlüsselverteilungsproblem und die Public-Key-Verschlüsselung	111
4.1	Schlüssel im Voraus austauschen	113
4.1.1	Probleme bei dieser Vorgehensweise	114
4.2	Mit einer vertrauenswürdigen dritten Partei arbeiten	115
4.3	Probleme dieses Verfahrens	118
4.4	Public-Key-Verschlüsselung und der digitale Umschlag	118

4.5	Sicherheitsprobleme	123
4.5.1	Einen Public-Key-Algorithmus brechen	124
4.6	Einige geschichtliche Anmerkungen zur Public-Key-Verschlüsselung	125
4.7	Wie die Public-Key-Verschlüsselung funktioniert	127
4.7.1	Der RSA-Algorithmus	130
4.7.2	Der DH-Algorithmus	138
4.7.3	Der ECDH-Algorithmus	144
4.8	Vergleich der Algorithmen	151
4.8.1	Sicherheit	151
4.8.2	Schlüssellängen	154
4.8.3	Leistungsverhalten	155
4.8.4	Übertragungsgröße	156
4.8.5	Interoperabilität	157
4.9	Private-Keys schützen	157
4.10	Den digitalen Umschlag zur Wiedergewinnung des Schlüssels verwenden	158
4.10.1	Schlüsselwiedergewinnung mittels einer vertrauenswürdigen dritten Partei	160
4.10.2	Schlüsselwiedergewinnung mittels einer Gruppe von Treuhändern	161
4.10.3	Schlüsselwiedergewinnung mit Schwellenwertverfahren	163
4.10.4	Wie ein Schwellenwertverfahren funktioniert	167
4.11	Zusammenfassung	169
4.12	Ein Beispiel aus der Praxis	170
5	Die digitale Signatur	173
5.1	Die Eindeutigkeit einer digitalen Signatur	174
5.2	Message-Digests	178
5.2.1	Kollisionen	182
5.2.2	Die drei wichtigen Digest-Algorithmen	185
5.2.3	MD2	185
5.2.4	MD5	185
5.2.5	SHA-1	186
5.3	Eine Repräsentation größerer Datenmengen	186
5.3.1	HMAC	188
5.3.2	Datenintegrität	191
5.4	Zurück zu den digitalen Signaturen	192
5.5	Betrugsversuche	196

5.6	Authentifizierung, Integrität und Verbindlichkeit implementieren	197
5.7	Die Algorithmen verstehen	198
5.7.1	RSA	199
5.7.2	DSA	199
5.7.3	ECDSA	202
5.8	Vergleich der Algorithmen	202
5.8.1	Sicherheit	202
5.8.2	Leistungsverhalten	203
5.8.3	Übertragungsgröße	204
5.8.4	Zusammenarbeit (Interoperabilität)	205
5.9	Private Schlüssel schützen	205
5.10	Einführung in Zertifikate	206
5.11	Schlüsselwiedergewinnung	209
5.12	Zusammenfassung	209
5.13	Ein Beispiel aus der Praxis	210
6	Public-Key-Infrastrukturen und der X.509-Standard	211
6.1	Public-Key-Zertifikate	212
6.1.1	Eindeutige Bezeichner	214
6.1.2	Zertifikatserweiterungen der Version 3 des Standards	214
6.1.3	Entity-Namen	218
6.1.4	ASN.1-Notation und -Chiffrierung	219
6.2	Die Komponenten einer PKI	220
6.2.1	Beglaubigungsinstanz	220
6.2.2	Registration Authority	221
6.2.3	Zertifikatsverzeichnis	221
6.2.4	Schlüsselwiedergewinnungsserver	222
6.2.5	Verwaltungsprotokolle	223
6.2.6	Operationale Protokolle	225
6.3	Zertifikate registrieren und ausstellen	225
6.4	Ein Zertifikat widerrufen	226
6.4.1	Zertifikatswiderruflisten	227
6.4.2	CRL-Eintragserweiterungen	228
6.4.3	CRL-Erweiterungen	229
6.4.4	CRL-Verteilungspunkte	230
6.4.5	Delta-CRLs	230
6.4.6	Indirekte CRLs	231
6.4.7	Ein Zertifikat temporär sperren	231

6.4.8	Instanzwiderrufslisten	232
6.4.9	Online Certificate Status Protocol	232
6.5	Vertrauensmodelle	233
6.5.1	Zertifikatshierarchien	234
6.5.2	Kreuzzertifizierung	235
6.5.3	X.509-Zertifikatskette	236
6.5.4	Das Push-Modell im Vergleich zum Pull-Model	237
6.6	Schlüsselpaare verwalten	238
6.6.1	Schlüsselpaare generieren	239
6.6.2	Private Schlüssel schützen	240
6.6.3	Mehrere Schlüsselpaare verwalten	241
6.6.4	Schlüsselpaare aktualisieren	242
6.6.5	Die History von Schlüsselpaaren speichern	243
6.7	Eine PKI einsetzen	243
6.8	Die Zukunft von PKIs	244
6.8.1	Roaming Certificates	244
6.8.2	Attribute Certificates	246
6.9	Zertifizierungsvorschriften und Certification Practice Statements	247
6.10	Zusammenfassung	249
6.11	Beispiele aus der Praxis	250
6.11.1	Keon Certificate Server	250
6.11.2	Keon Web PassPort	250
7	Netzwerk- und Transport-sicherheitsprotokolle	251
7.1	Internet Protocol Security	252
7.1.1	IP-Sicherheitsarchitektur	252
7.1.2	IPSec-Dienste	253
7.2	Das Authentication Header Protocol	253
7.2.1	Berechnung des Integrity Check Value	254
7.2.2	Transport- und Tunnelmodi	255
7.3	Das Encapsulating Security Payload Protocol	257
7.3.1	Chiffrieralgorithmen	258
7.3.2	ESP im Transport- und im Tunnelmodus	259
7.4	Security Associations	260
7.4.1	Security Associations kombinieren	261
7.5	Sicherheitsdatenbanken	264
7.5.1	Security Policy Database	264
7.5.2	Security Association Database	265

7.6	Schlüsselverwaltung	266
7.6.1	Internet Key Exchange	266
7.6.2	Main Mode	267
7.6.3	Aggressive Mode	268
7.6.4	Quick Mode	268
7.7	Secure Sockets Layer	269
7.7.1	Die Geschichte des SSL	270
7.8	Sitzungs- und Verbindungszustände	271
7.9	Das Record Layer Protocol	273
7.10	Das Change Cipher Spec Protocol	274
7.11	Das Alert Protocol	274
7.12	Das Handshake Protocol	276
7.12.1	Die Client Hello Message	277
7.12.2	Die Server Hello Message	278
7.12.3	Die Server Certificate Message	279
7.12.4	Die Server Key Exchange Message	279
7.12.5	Die Certificate Request Message	280
7.12.6	Die Server-Hello-Done Message	280
7.12.7	Die Client Certificate Message	280
7.12.8	Die Client Key Exchange Message	280
7.12.9	Die Certificate Verify Message	281
7.12.10	Die Finished Message	281
7.12.11	Eine Sitzung und eine Verbindung beenden	282
7.12.12	Sitzungen wieder aufnehmen	282
7.12.13	Kryptographische Berechnungen	283
7.13	Chiffrier- und Authentifizierungsalgorithmen	284
7.14	Zusammenfassung	284
7.15	Beispiel aus der Praxis	285
8	Sicherheitsprotokolle der Anwendungsschicht	287
8.1	S/MIME	287
8.1.1	Überblick	288
8.1.2	S/MIME-Funktionalität	288
8.1.3	Kryptographische Algorithmen	289
8.1.4	S/MIME-Nachrichten	291
8.1.5	Verbesserte Sicherheitsdienste	296
8.1.6	Interoperabilität	297

8.2	Secure Electronic Transaktion (SET)	297
8.2.1	Geschäftliche Anforderungen	299
8.2.2	SET-Funktionen	299
8.2.3	SET-Teilnehmer	300
8.3	Doppelte Unterschriften	302
8.3.1	SET-Zertifikate	303
8.3.2	Zahlungsverarbeitung	305
8.4	Zusammenfassung	310
8.5	Beispiele aus der Praxis	310
9	Hardware-Lösungen: Software-Beschränkungen überwinden	313
9.1	Kryptographische Beschleuniger	313
9.2	Authentifizierungs-Tokens	315
9.3	Token-Formfaktoren	315
9.3.1	Kontaktfreie Tokens	317
9.3.2	Einmal-Passwort-Generatoren	318
9.3.3	Kontakt-Tokens	320
9.4	Smart-Cards	320
9.4.1	Smart-Card-Standards	321
9.4.2	Arten von Smart-Cards	322
9.4.3	Leser und Terminals	324
9.5	JavaCards	325
9.5.1	Geschichte und Standards	325
9.5.2	JavaCard-Operationen	326
9.6	Andere Java-Tokens	327
9.7	Biometrie	328
9.7.1	Überblick über biometrische Systeme	328
9.7.2	Erkennungsverfahren	332
9.7.3	Biometrische Genauigkeit	335
9.8	Authentifizierungsmethoden kombinieren	336
9.9	Zusammenfassung	337
9.10	Anbieter	338
10	Digitale Signaturen: Jenseits der Sicherheit	341
10.1	Gesetzgebung	343
10.2	Rechtliche Richtlinien der American Bar Association	343

10.3	Rechtliche Konzepte, die digitale Signaturen betreffen	344
10.3.1	Verbindlichkeit	344
10.3.2	Authentifizierung	346
10.3.3	Ein Vergleich schriftlicher und digitaler Signaturen	347
10.4	Anforderungen an den Einsatz digitaler Signaturen	348
10.4.1	Public-Key-Infrastrukturen	348
10.4.2	Kontrolle des Schlüsselwiderrufs	349
10.4.3	Zeitstempel	349
10.5	Die aktuelle und schwebende Gesetzgebung	351
10.5.1	Der E-SIGN Act	352
10.6	Umgang mit rechtlichen Ungewissheiten	354
10.7	Zusammenfassung	357
10.8	Beispiele aus der Praxis	358
II	Unrecht tun: Einbrüche	359
II.1	Verluste messen	359
II.2	Arten von Sicherheitsbedrohungen	360
II.2.1	Nichtautorisierte Offenlegung von Daten	360
II.2.2	Nichtautorisierte Änderung von Daten	361
II.2.3	Nichtautorisierter Zugang	362
II.2.4	Offenlegung von Netzwerkverkehr	363
II.2.5	Spoofing von Netzwerkverkehr	363
II.3	Eindringlinge identifizieren	364
II.3.1	Insider	365
II.3.2	Hacker	365
II.3.3	Terroristen	365
II.3.4	Ausländische Geheimdienste	366
II.3.5	Hacktivisten	366
II.3.6	Kenntnisse der Eindringlinge	367
II.4	Fallstudien	367
II.4.1	Daten bei der Übertragung	368
II.4.2	Daten in Ruhe	369
II.4.3	Authentifizierung	369
II.4.4	Unzureichende Implementierung	371
II.5	Informationssicherheit: Durchsetzung von Gesetzen	372
II.6	Zusammenfassung	373

12	Richtig vorgehen: Standards beachten	375
12.1	Sicherheitsdienste und -mechanismen	375
12.1.1	Authentifizierung	376
12.1.2	Vertraulichkeit	378
12.1.3	Integrität	378
12.1.4	Verbindlichkeit	379
12.2	Standards, Richtlinien und Vorschriften	379
12.2.1	Die Internet Engineering Task Force	379
12.2.2	National Institute of Standards und Technology	381
12.2.3	Common Criteria	382
12.2.4	Der Health Insurance Portability Act	383
12.3	Unterstützung von Entwicklern	384
12.3.1	Versicherungen	385
12.3.2	Sicherheitsforschung	385
12.4	Fallstudien	386
12.4.1	Implementierung	386
12.4.2	Authentifizierung	387
12.4.3	Daten in Ruhe	388
12.4.4	Daten bei der Übertragung	389
12.5	Zusammenfassung	389
A	Bits, Bytes, Hex und ASCII	391
A.1	Mit dezimalen, binären und hexadezimalen Zahlen arbeiten	391
A.2	Bits und Bytes verwenden	394
A.3	ASCII-Zeichen verwenden	394
A.4	Computer in der Kryptographie	396
B	Eine Einführung in eine Untermenge von ASN.1, BER und DER für Laien	397
B.1	Zusammenfassung	397
B.2	Abschnitt 1: Einführung	398
B.2.1	Abschnitt 1.1: Terminologie und Notation	399
B.3	Abschnitt 2: Abstract Syntax Notation 1	399
B.3.1	Abschnitt 2.1: Einfache Typen	401
B.3.2	Abschnitt 2.2: Strukturierte Typen	402
B.3.3	Abschnitt 2.3: Typen mit impliziten und expliziten Tags	403
B.3.4	Abschnitt 2.4: Andere Typen	403

B.4	Abschnitt 3: Basic Encoding Rules	404
B.4.1	Abschnitt 3.1: Primitive-Definite-Length-Methode	405
B.4.2	Abschnitt 3.2: Constructed-Definite-Length-Methode	406
B.4.3	Abschnitt 3.3: Constructed-Indefinite-Length-Methode	407
B.5	Abschnitt 4: Distinguished Encoding Rules	407
B.6	Abschnitt 5: Notation und Codierungen für einige Typen	408
B.6.1	Abschnitt 5.1: Typen mit impliziten Tags	408
B.6.2	Abschnitt 5.2: Typen mit expliziten Tags	410
B.6.3	Abschnitt 5.3: ANY	411
B.6.4	Abschnitt 5.4: BIT STRING	413
B.6.5	Abschnitt 5.5: CHOICE	414
B.6.6	Abschnitt 5.6: IA5String	415
B.6.7	Abschnitt 5.7: INTEGER	416
B.6.8	Abschnitt 5.8: NULL	418
B.6.9	Abschnitt 5.9: OBJECT IDENTIFIER	418
B.6.10	ASN.1-Notation	419
B.6.11	Abschnitt 5.10: OCTET STRING	421
B.6.12	ASN.1-Notation	421
B.6.13	Abschnitt 5.11: PrintableString	422
B.6.14	Abschnitt 5.12: SEQUENCE	423
B.6.15	Abschnitt 5.13: SEQUENCE OF	424
B.6.16	Abschnitt 5.14: SET	425
B.6.17	Abschnitt 5.15: SET OF	426
B.6.18	Abschnitt 5.16: TG1String	427
B.6.19	Abschnitt 5.17: UTCTime	428
B.7	Abschnitt 6: Ein Beispiel	430
B.7.1	Abschnitt 6.1: Abstract Notation	430
B.7.2	Abschnitt 6.2: DER-Codierung	431
B.7.3	AttributeValue	432
B.7.4	AttributeValueAssertion	433
B.7.5	RelativeDistinguishedName	433
B.7.6	RDNSequence	434
B.7.7	Name	434
B.8	Quellennachweis	435
B.9	Revisionsgeschichte	436
B.9.1	Version vom 3. Juni 1991	436
B.9.2	Version vom 1. November 1993	436

C	Weitere technische Einzelheiten	439
C.1	Wie digest-basierte PRNGs funktionieren	439
C.2	Feedback-Modi	441
C.2.1	Der Cipher-Feedback-Modus	441
C.2.2	Der Output-Feedback-Modus	443
C.2.3	Der Counter-Modus	444
C.3	Wie man Informationslecks von IVs und Salts stopfen kann	445
C.4	Manipulationssichere Hardware	446
C.5	RSA-Padding	447
C.5.1	PKCS #1 Block 02 Padding	448
C.5.2	Der Bleichenbacher-Angriff	449
C.5.3	Optimal Asymmetric Encryption Padding	451
C.6	Timing-Angriffe	453
C.7	Kerberos	456
C.8	DH-, ECDH-, DAS- und ECDSA-Zertifikate	457
C.9	Probleme beim Schutz von Kreditkarten mit SSL	459
	Stichwortverzeichnis	461