



Sicherheit

Folienskript zur Stammvorlesung

in „Praktische Informatik“

WS 97/98, 4+2h

Prof. Dr. Birgit Pfitzmann

Saarbrücken, 26.2.1998

Autorin:

Birgit Pfitzmann

Universität des Saarlandes, Fachbereich Informatik (Geb. 45, R. 536)

Im Stadtwald

D-66123 Saarbrücken

Email: pfitzmann@cs.uni-sb.de

Bibliographische Angaben

Pfitzmann, Birgit

Sicherheit; Folienskript zur Vorlesung WS97/98 / Birgit Pfitzmann. – Saarbrücken: Universität des Saarlandes, 1998

© Birgit Pfitzmann, Saarbrücken, 1997, 1998

Vorwort

Wie man leicht sieht, ist dies kein echtes Skript, sondern Folienkopien. Die Folien waren aber von vornherein auch für den Zweck entworfen, auch nachträglich noch allein lesbar zu sein, da es kein zu dieser Vorlesung ähnliches Buch gibt.

Die vorliegende Version ist im Vergleich zu den Originalfolien minimal korrigiert. Weitere Korrekturen, insbesondere auch zu nicht eingeführten oder im Index fehlenden Begriffen, sind willkommen, ebenso inhaltliche Kommentare für spätere Versionen.

Für Diskussionen über diese Vorlesung danke ich *Michael Waidner* und den Übungsleitern, *Ammar Alkassar*, *Daniel Kröning*, *Rainer Schmid* und *Jan-Holger (Max) Schmidt*. Außer der zitierten öffentlich erhältlichen Literatur habe ich in manchen Teilen auch Skripten von *Joachim Biskup* und *Jimmy Brüggemann* von der Uni Hildesheim verwendet.

Saarbrücken, Februar 1998

Birgit Pfitzmann

Gliederung

0.A	Überblick.....	1
0.B	Verwaltung.....	5
0.C	Literatur.....	6
1	Einführung: Sicherheitsbegriffe.....	12
1.1	Überblick.....	12
1.2	Einteilung von Schutzzielen.....	13
1.3	Vertrauen.....	15
1.3.1	Konkrete Angriffs- und Fehlerquellen.....	16
1.3.2	Abstrakte Vertrauensmodelle.....	17
1.4	Entdecken / verhindern.....	21
1.5	Technisch / juristisch.....	22
1.6	Weiterführende Literatur zu Kap. 1.....	23
TEIL I Grundlegende kryptographische Systeme.....		25
2	Systemtypen.....	28
2.1	Verschlüsselung.....	29
2.1.1	Symmetrische Verschlüsselung.....	29
2.1.2	Asymmetrische Verschlüsselung.....	32
2.2	Authentikation.....	35
2.2.1	Symmetrische Authentikation.....	35
2.2.2	Signaturssysteme.....	37
2.3	Einwegfunktionen u.ä.....	41
2.3.1	Normale Einwegfunktionen.....	41
2.3.2	Trapdoor-Einwegpermutationen.....	44
2.4	Hashfunktionen.....	46
2.5	Pseudozufallsgeneratoren.....	48
2.6	Etwas genauer.....	50
2.7	Weiterführende Literatur.....	51
3	Sicherheitsgrade.....	52
3.1	Erfolgsarten eines Angreifers.....	53
3.2	Angriffstypen.....	56
3.3	Rechenfähigkeiten.....	60
3.3.1	Hauptunterscheidung.....	60
3.3.2	Was geht informationstheoretisch?.....	61
3.3.3	Mehr über kryptographische Sicherheit.....	62
A.	Angriffe durch vollständige Suche.....	62
B.	Nicht nur Worst-case-Komplexität.....	64
C.	Probabilistische Algorithmen.....	64
D.	Leicht und schwer.....	65
E.	Echt beweisbare Sicherheit?.....	66
F.	Beweisziel.....	67
3.3.4	Notation und Beispielformulierung.....	68
A.	Probabilistische Algorithmen.....	68
B.	Definition Einwegfunktion als Beispiel.....	70

3.4	Weiterführende Literatur.....	72
4	Überblick konkrete Systeme	73
5	Zahlentheoretische Grundlagen	75
5.1	Rechnen in Restklassenringen \mathbb{Z}_n	75
	A. Grundlegende Definitionen.....	75
	B. Algorithmen	79
5.2	Multiplikative Gruppe \mathbb{Z}_n^*	82
5.3	Körper \mathbb{Z}_p	87
5.4	Grundlagen für Systeme mit Faktorisierungsannahme	88
5.4.1	Chinesischer Restsatz.....	89
5.4.2	Faktorisierung, Annahme	95
	A. Standardannahme.....	95
	B. Varianten der Annahme	96
	C. Stand der Faktorisierung.....	97
5.4.3	Primzahlerzeugung.....	98
5.5	Grundlagen für Systeme mit Diskreter-Log-Annahme.....	100
5.5.1	Zyklische Gruppen.....	102
	A. Gruppenordnungen.....	102
	B. Elementordnungen, zyklische Gruppen.....	103
	C. Lemmas über zyklische Gruppen.....	106
5.5.2	Diskreter Logarithmus, Annahmen.....	110
	A. „Standard“.....	110
	B. In Untergruppe.....	111
	C. Sonstige Varianten.....	113
5.5.3	Schlüsselerzeugung	116
	A. Standard	116
	B. In Untergruppe.....	119
5.6	Weiterführende Literatur.....	121
6	Konkrete Systeme.....	122
6.1	Symmetrische Verschlüsselung.....	122
6.1.1	Informationstheoretische Geheimhaltung.....	122
	A. Definition	123
	B. Hinreichendes Kriterium.....	126
	C. Vernam-Chiffre = One-time-Pad.....	128
	D. Mehrere Nachrichten	129
	E. Vernam-Chiffre allgemeiner	129
	F. Optimalität	130
	G. Literatur.....	130
6.1.2	DES.....	131
	A. Konstruktion	137
	B. Effizienz	137
	C. Sicherheit	138
	D. Gegenmaßnahmen gegen vollständige Suche	140
	E. Literatur.....	142
6.1.3	Betriebsarten von Blockchiffren.....	143
	A. Ziele	143
	B. Begriffe.....	145
	C. „Electronic Codebook“ (ECB)	147

	D. „Cipher-Block Chaining“ (CBC)	149
	E. „Cipher Feedback“ (CFB).....	151
	F. „Output Feedback“ (OFB).....	153
	G. Sonstiges zu Betriebsarten.....	156
	H. Literatur.....	157
6.1.4	Sonstige symmetrische Verschlüsselung	158
6.2	Asymmetrische Verschlüsselung	159
6.2.1	RSA-Verschlüsselung	159
	A. Kernidee: RSA als Trapdoor-Einwegpermutationen	159
	B. Naiver und unsicherer Einsatz von RSA zur Verschlüsselung.....	164
	C. Gegenmaßnahmen.....	166
	D. Effizienzverbesserungen.....	172
6.2.2	ElGamal-Verschlüsselung (und Diffie-Hellman-Schlüsselaustausch)	176
	A. Konstruktionsidee	177
	B. Diffie-Hellman-Schlüsselaustausch	178
	C. Naive und unsichere ElGamal-Verschlüsselung.....	181
	D. Zur Sicherheit	183
6.2.3	Weitere Ad-hoc-Systeme	189
6.2.4	Skizze von Sicherheitsdefinitionen und beweisbar sicheren Systemen	190
	A. Keine partielle Information	190
	B. Sicherheit gegen aktive Angriffe.....	192
6.2.5	Literatur.....	193
6.3	Symmetrische Authentikation.....	195
6.3.1	Informationstheoretisch sichere symmetrische Authentikation.....	195
	A. Definition	196
	B. Hinreichendes Kriterium.....	199
	C. Bekannteste konkrete Funktionen: Wegman-Carter-Basissystem	201
	D. Optimalität für kurze Nachrichten.....	203
	E. Mehrere Nachrichten	204
	F. Lange Nachrichten.....	205
	G. Variante mit stärkerem Ziel, Skizze.....	206
6.3.2	Beweisbar kryptographisch sichere Authentikation	207
6.3.3	Authentikationsbetriebsarten von Blockchiffren	208
	A. „CBC-Auth“	208
	B. „CFB-Auth“.....	209
6.3.4	Sonstige symmetrische Authentikation	210
6.3.5	Literatur.....	211
6.4	Signaturssysteme	213
6.4.1	RSA-Signaturen	213
	A. Naiver und unsicherer Einsatz von RSA zum Signieren.....	213
	B. Gegenmaßnahmen.....	216
	C. Effizienzverbesserungen.....	221
6.4.2	ElGamal-artige Signaturssysteme.....	222
	A. Grundidee	223
	B. Naives und unsicheres	224
	C. Sicherheit	225
	D. Gegenmaßnahmen.....	226
	E. Varianten.....	228
6.4.3	Weitere Ad-hoc-Systeme	230
6.4.4	Skizze von Sicherheitsdefinitionen und beweisbar sicheren Systemen	231
	A. Definition	231

B. Beweisbar sichere Systeme.....	235
6.4.5 Signatursysteme mit Zusatzeigenschaften	237
6.4.6 Literatur.....	238
6.5 Hashfunktionen.....	243
6.5.1 Definitionen und allgemeine Beziehungen.....	245
6.5.2 Beweisbar kollisionsfreie Hashfunktionen.....	252
A. Für relativ kurze Nachrichten	252
B. Für lange Nachrichten.....	255
6.5.3 Hashfunktionen aus Blockchiffren.....	259
6.5.4 Direkt konstruierte Hashfunktion.....	262
6.5.5 Literatur.....	263
6.6 Pseudozufallsgeneratoren	264
6.6.1 Konstruktionen aus Blockchiffren	264
A. OFB	264
B. Anderes Beispiel.....	266
6.6.2 Direkte Konstruktionen.....	267
6.6.3 BBS oder x^2 -mod- n : Beweisbar sicherer Pseudozufallsgenerator (hier ohne Beweis).....	268
6.6.4 Skizze der Sicherheitsdefinition	270
6.6.5 Literatur.....	271
6.7 Literaturverweise auf weitere Klassen	272
7 Wichtige Kombinationen	273
7.1 Hybride Verschlüsselung.....	273
7.2 Hashen vor Signieren.....	275
7.3 Betriebsarten von Blockchiffren.....	276
7.4 Einsatz von Pseudozufallsgeneratoren.....	277
7.5 Anwenderschnittstelle.....	278
TEIL II Kryptographie in der Praxis.....	280
8 Nötig: Zufallszahlen, Schlüsselverteilung	280
8.1 Erzeugung echter Zufallszahlen.....	281
8.1.1 Mögliche Quellen.....	282
8.1.2 Verwendung der Quellen	284
8.2 Schlüsselverteilung.....	286
8.2.1 Symmetrische Schlüssel.....	287
8.2.2 Asymmetrische Schlüssel	290
8.3 Literatur.....	317
9 Techniken für einfache Protokolle, v.a. Authentikationsprotokolle	320
9.1 Freshness-Maßnahmen	321
9.1.1 Ziele.....	321
9.1.2 Verfahren.....	323
9.2 Expliztheit	326
9.3 Dispute mitbetrachten	331
9.4 Identifikation meist zu wenig	333
9.5 Beispielprotokoll: Sitzungsschlüsselaustausch	336
9.6 Techniken zum Fehlerfinden.....	339
9.7 Literatur.....	348

10	Juristische Aspekte.....	350
10.1	Signaturen.....	350
10.2	Verschlüsselung.....	352
10.3	Literatur.....	355
11	Produkte, Standards.....	356
11.1	Kerberos.....	357
11.2	PGP („Pretty Good Privacy“).....	358
11.3	Sonstiges für Email.....	359
11.4	SSL („Secure Socket Layer“).....	360
11.5	IPSEC (für IPv6).....	361
11.6	SSH („Secure Shell“).....	362
11.7	Literatur.....	363
TEIL III Nichtkryptographische Sicherheit.....		364
12	Generelle Sicherheitsaspekte.....	364
12.1	Organisatorische Sicherheit.....	366
12.2	Physische Sicherheit.....	369
12.2.1	Allgemeine Betrachtung.....	370
12.2.2	Magnetkarten.....	376
12.2.3	Speicherkarten.....	378
12.2.4	Smartcards.....	378
12.2.5	Größere Geräte.....	384
12.2.6	Nichtdigitale Angriffe auf Kryptographie.....	385
12.2.7	Sonstige physische Maßnahmen.....	387
12.2.8	Standards.....	387
12.3	Kommunikation mit Benutzer.....	388
12.3.1	Benutzeridentifikation.....	389
12.3.2	Geräteidentifikation.....	401
12.3.3	Einbau in verteiltes Szenario.....	404
12.3.4	Einbau in Anwendung.....	406
12.3.5	Normale Kommunikation mit kleinem persönlichen Gerät.....	408
12.4	Literatur.....	411
13	Betriebssysteme.....	414
13.1	Typische heutige Probleme.....	414
13.1.1	Diebstahl.....	414
13.1.2	Viren.....	414
13.1.3	Paßwortprobleme.....	419
13.1.4	Allgemeine Superuser-Probleme.....	423
13.1.5	Setuid-Programme.....	425
13.1.6	Hostauthentikationsprobleme.....	428
13.1.7	X Windows.....	430
13.1.8	Capability-Probleme.....	431
13.1.9	Applets u.ä.....	432
13.1.10	Trojanische Pferde allgemeiner.....	434
13.1.11	Wichtige Typen von Werkzeugen.....	438
13.1.12	Literatur.....	439
13.2	Abgrenzungen.....	440

13.3 Abstrakte Zugriffskontrolle	441
13.3.1 Zugriffskontrollzustände	442
13.3.2 Kurze Spezifikation einzelner Zugriffskontrollzustände.....	445
A. Gruppenbildung	445
B. Hierarchien	446
C. Explizite Verbote.....	448
D. Konflikte und Defaultwerte.....	449
E. Prioritäten.....	452
F. Verlangen von Rechtekombinationen.....	453
G. Zusätzliche Bedingungen.....	457
H. Zusammenfassung	458
13.3.3 Rechtweitergaberegeln allgemein.....	461
A. Vorbemerkung: Weitergaberegeln gibt's nicht immer	461
B. Einführung Weitergaberegeln	462
C. Begriffe, Abgrenzungen	464
D. Klassische Sprache für Regelmengen: HRU	465
E. Erreichbarkeitsfragen.....	479
F. Das andere Extrem: Take-grant-Schemata	491
G. Ausblick: Zwischendinge.....	499
H. Rechteentzug.....	501
13.3.4 Spezielle Zugriffskontrollstrategien	511
A. Eigentümergesteuert.....	512
B. Clark-Wilson-Modell (kommerzielle Integrität).....	513
C. Chinesische Mauer	518
D. Einfache Sicherheitsstufen für Geheimhaltung.....	521
E. Abteilungen (Compartments).....	523
F. Allgemeine Sicherheitsstufen für Geheimhaltung (\approx Bell-LaPadula).....	525
G. Sicherheitsstufen für Integrität (\approx Biba-Modell).....	534
H. Workflow-Modelle.....	536
13.3.5 Literatur.....	539
13.4 Durchsetzung	541
13.4.1 Hardwareschutz	543
A. Abgrenzung	543
B. Überblick	544
C. Speicherschutz	545
D. Prozessorzustände.....	557
E. Zustandswechsel.....	560
13.4.2 Betriebssystemkern	562
A. Überblick	562
B. Subjekte.....	564
C. Objekte und Zugriffsarten	574
D. Implementierung der Rechte und ihrer Weitergabe	596
E. Allgemeines zu Rechteentzug bei Capabilities	616
F. Rechtweitergabe bei ACLs (Zugriffskontrolllisten)	620
H. Spezialfälle	621
13.4.3 Höhere Schichten, Skizze	626
13.4.4 Literatur.....	627
13.5 Protokollierung und Intrusion detection.....	631
13.5.1 Wann gebraucht?	631
13.5.2 Protokollierung	633
13.5.3 Intrusion detection.....	635

13.6 Informationsflußkontrolle.....	638
13.6.1 Informationsfluß in (deterministischen) sequentiellen Programmen	641
A. Spezifikation	641
B. Typen von Informationsflüssen in sequentiellen Programmen.....	646
C. Probleme mit exakter Datenflußentscheidung	647
D. Vergrößerte statische Analyse.....	652
F. Komplettes Beispiel	659
G. Erweiterungen	660
13.6.2 Informationsflußdefinition in reaktiven Systemen.....	665
A. Modell für Ein- und Ausgaben:	666
B. Modell analog zu „vom Programm berechneter Funktion“:	667
C. Modell für System (\approx Programm):	668
D. Geheimzuhaltendes und Beobachtungen.....	669
E. Informationsflußdefinition.....	672
F. Theorien in diesem Bereich.....	675
13.6.3 Versteckte Kanäle	676
A. Speicherkanäle	676
B. Zeitkanäle.....	681
13.6.4 Literatur zu Kap. 13.5, 13.6.....	683
14 Informationssysteme (Datenbanken)	685
14.1 Zugriffskontrolle	686
A. Zum großen Teil schon behandelt	686
B. Konkrete Objekte in relationalen Datenbanken.....	687
C. Sichten (Views).....	689
D. Probleme mit semantischen Bedingungen	691
14.2 Statistische Datenbanken	702
14.2.1 Problemstellung	702
14.2.2 Beschränkung der Anfragen	707
A. Erste echte Gegenmaßnahme.....	707
B. Problem jetzt: Kombination mehrerer Statistiken	708
C. Weitere heuristische Gegenmaßnahmen	714
D. Sichere Gegenmaßnahmen	715
14.2.3 Ungenaue Antworten	717
14.2.4 Verwandte Themen.....	720
14.3 Literatur	721
15 Netze.....	722
15.1 Firewalls	724
15.1.1 Allgemeines	724
15.1.2 Netzschichten	728
15.1.3 IP-Ebene.....	730
15.1.4 TCP-Ebene.....	735
15.1.5 Anwendungsebene	740
15.1.6 Physische Konfigurationen	742
15.1.7 Literatur.....	744
15.2 Allgemeinere Zugriffskontrolle in verteilten Systemen	745
15.2.1 Zugriffskontrolle über Netze im engeren Sinn.....	745
15.2.2 Weitergehende Fragen	752
15.2.3 Literatur.....	754

16	Vertrauenswürdiger Entwurf.....	755
16.1	Methoden.....	756
16.2	Kriterienkataloge.....	757
16.3	Literatur	762
Index.....		Index.1
	(Mehr oder minder) deutsche Begriffe.....	Index.1
	Englische Begriffe.....	Index.12
	Symbole	Index.14

(Mehr oder minder) deutsche Begriffe und alle Abkürzungen

- 4-Augen-Prinzip; 456
- A-posteriori-Wahrscheinlichkeit; 125; 638; 645
- A-priori-Wahrscheinlichkeit; 125; 638; 645
- Abfangangriff; 33
- Abhörbarkeit; 353
- Ablauf; 666
- Ablehnung, Informationsfluß durch; 691
- Abstrahlung; 371
- abstrakte Zugriffskontrolle; 441
- abstrakter Datentyp; 340
- Abteilungen; 523
- ACL (access control list); 443; 614
- Active X; 432
- adaptiv; 58
- additive Statistik; 711
- Adreßraum; 564
- Adreßraum, teilweise Vererbung; 613
- aktiver Angriff; 57; 164; 186; 215; 232
- Aktualität; 322
- Alarm; 633
- algebraische Abstraktion; 340
- Algorithmen mit Restklassen; 79
- Algorithmen, Öffentlichkeit; 52
- All-Rechte; 472
- allgemeiner Tracker-Angriff; 710
- allozieren; 576; 594
- Amoeba; 570; 571; 591; 598; 606
- analoge Charakteristika; 371
- Anforderungsanalyse; 12
- Anfragebeschränkung; 707
- Angreifermodell; 15
- Angriffsmuster; 636
- Angriffsquellen; 16
- Angriffssimulation; 341
- Angriffstypen; 56
- Annahmen, kryptographische; 66
- anonyme Kommunikation; 723
- Anonymisierung (in Datenbank); 720
- Anonymität; 14
- Anweisungslabel; 653
- Anwenderschnittstelle; 278
- API; 28
- API-Standard; 356
- Append-only-Schutz; 633
- Applet; 432; 456; 624
- ASN.1 (Abstract Syntax Notation); 312; 329
- asymmetrisch; 27
- asymmetrische Authentikation; 37
- asymmetrische Verschlüsselung; 32; 159
- asymptotische Komplexität; 65
- Attribut (in Datenbank); 688
- Attributzertifikat; 299; 306; 316; 598; 753
- Ausdruckslabel; 653
- Ausgangsp permutation; 132
- Auslieferer; 16
- Auslieferung; 394
- Ausnahme; 448; 449
- Ausnahmeflag als versteckter Kanal; 678
- außen; 724
- Außenstehende; 16
- Ausweisprüfung; 293
- Authentikation aus schlüssellosen Hashfunktionen; 210
- Authentikation mit Schiedsrichter; 206
- Authentikation, beweisbar kryptographisch sicher; 207
- Authentikationsbetriebsarten von Blockchiffren; 208
- Authentikationscode; 36
- Authentikationscodes für lange Nachrichten; 205
- Authentizität; 14
- Average-case-Komplexität; 64
- azyklische Weitergaberegeln; 500
- BAN-Logik; 339
- bargeldartiges Zahlungssystem; 215
- Basisregister; 546
- Bayes'sche Formel; 127
- BBS (Blum-Blum-Shub-Generator); 268
- Bedingungen (bei Zugriffskontrolle); 457
- Bedrohung; 12; 15
- Bell-LaPadula-Modell; 525
- Benutzer; 16
- benutzergesteuerte Zugriffskontrolle; 511
- Benutzeridentifikation; 388; 389
- Benutzerkommunikation mit kleinem Gerät; 388; 408
- Benutzerrecht; 456
- benutzerverwaltete Capabilities; 597; 606
- Beobachtung; 671
- Beobachtung bei PIN-Eingabe; 390

- Beobachtungspunkt; 639; 670
- Beobachtungsrisiko; 407
- Beraterfirma; 518
- Beschränkung der Anfrageanzahl; 714
- Beschränkung der Anfragen; 707
- Beschränkung der Attributanzahl; 714
- Betreiber; 16
- Betriebsarten; 143; 208; 276
- Betriebsmittel; 544
- Betriebsmittel, statische Aufteilung; 678
- Betriebssystem, höhere Schichten; 626
- Betriebssysteme für Spezialfunktionen; 623
- Betriebssystemkern; 562
- Betroffene; 12
- Bevölkerungsdatenbank; 703
- beweisbar kryptographisch sicher; 66
- Beweislast; 350
- Beweismittel; 17; 331
- Bewerten physischer Angriffe; 374
- Biba-Modell; 534
- Bibliothek; 356
- Biometrik; 397; 637
- BirliX; 571; 573; 595; 599; 614
- Bitfolge; 48
- blinde Entschlüsselung; 165
- blinde Signaturen; 215; 238
- Blockchiffre; 131; 143
- Blockverkettung; 149
- Branche; 518
- Brewer-Nash-Modell; 518
- Bücher; 6
- CA (certification authority); 301
- Cache; 551
- Capabilities auf Ports; 610
- Capabilities, Implementierungsvarianten; 597
- Capabilities, signiert; 620
- Capabilities, Verschicken in Nachrichten bei kernverwalteten; 612
- Capability; 430; 503; 549; 556; 568
- Capability, Probleme in UNIX; 431
- Capability-Liste; 443; 601
- Capability-Parameter, formaler; 603
- Capability-Template; 603
- Capability-Ziel; 617
- CAST (Blockchiffre); 158
- CBC (Betriebsart); 149
- CBC-Auth; 208
- CERT-Advisories; 439
- CFB (Betriebsart); 151
- CFB-Auth; 209
- Challenge-Response; 324
- Chiffretext; 31
- Chiffrierschlüssel; 32
- Chinesische Mauer; 518
- Chinesischer Restalgorithmus; 92
- Chinesischer Restsatz; 89
- Chipkarte; 378
- chmod; 425; 444
- chrootuid; 438
- Clark-Wilson-Modell; 513; 536
- Client-Server-Struktur (bei Betriebssystemkern); 591
- Common Criteria; 758
- Compiler; 663
- COPS; 438
- Copytex; 377
- CORBA; 752
- CRA (Chinesischer Restalgorithmus); 92
- Crossover-Punkt; 398
- DAC (discretionary access control); 511
- Data Encryption Standard; 131
- Datei; 574
- Dateisystem; 626
- Dateisystem (Realisierung auf einfachem Kern); 582
- Dateiverschlüsselung; 358
- Dechiffrierschlüssel; 32
- Default Pager (bei Mach); 593
- Defaultwert (für Rechte); 451
- Delegation; 462; 536; 620
- DES (Blockchiffre); 131
- DES in Software; 137
- DES, Verallgemeinerungen; 140
- Diebstahl; 414
- Diebstahl verhindern; 368
- Dienstziele; 13
- Dienstzielverletzung; 21
- differentielle Kryptoanalyse; 139
- Diffie-Hellman-Annahme; 177
- Diffie-Hellman-Schlüsselaustausch; 176; 178
- Diffusion; 131; 137
- Dirichletscher Primzahlsatz; 98
- diskret (falscher Begriff); 511
- diskreter Logarithmus; 100

- diskreter Logarithmus, Berechnen; 113
- Diskreter-Log-Annahme; 100; 110
- Disput; 37; 331
- DNS-Server; 428
- Domain; 522
- DORIS-Datenbanksystem; 453
- Dritte; 37
- DSA (Signatursystem); 222
- DSS (Signatursystem); 222
- Durchsetzung; 541
- e-te Wurzel; 161
- EC-Karten; 377; 392; 394
- ECB (Betriebsart); 147
- effektive User-ID; 425
- eigene Geräte; 366
- eigenhändige Unterschrift; 350
- eigentümergesteuerte Zugriffskontrolle; 511; 512
- Ein-/Ausgabeverhalten bei reaktivem System; 667
- Einbahn-; 42
- einelementige Menge, Statistik; 704; 707
- Einflußnahme auf ehrliche Benutzer; 19; 56
- einfrieren; 371
- Einfügeangriff; 715
- Eingabegenerieralgorithmus; 71
- Eingangsp permutation; 132
- eingeschränkte Umgebung; 438
- Einmal-Signaturen; 236
- einweg; 70
- einweg bei Hashfunktionen; 245
- Einwegfunktion; 41; 70
- Einwegpermutation; 41
- Einzelüberwachung; 354
- elektrische Schnittstellen; 371
- elektronische Briefftasche; 367
- Elektronisches Codebuch; 147
- Elementordnung; 103
- ElGamal-Signaturen, Angriffe; 226
- ElGamal-Signaturen, naiv; 224
- ElGamal-Signatursystem; 222
- ElGamal-Verschlüsselung; 176
- ElGamal-Verschlüsselung, Angriffe; 183
- ElGamal-Verschlüsselung, naiv; 181
- elliptische Kurven; 113; 115; 189
- Email-Rückruf; 294
- Email-Verschlüsselung; 358; 359; 363
- entdecken; 21
- Entwerfer; 16
- Ergebnisrückführung; 153
- Erkennen physischer Angriffe; 373
- erlaubter Zugriffskontrollzustand; 479
- Erreichbarkeit; 479
- Erreichbarkeit einer Rechteart; 480
- Erreichbarkeit eines konkreten Rechts; 481
- Erreichbarkeit, unentscheidbar; 480
- erweiterter Euklidischer Algorithmus; 82
- Euklidischer Algorithmus; 83
- Eulersche Phi-Funktion; 85
- Executerecht bei Dateien; 574
- existentielle Fälschung; 54; 214; 226; 232
- Expansionspermutation; 136
- explizit spezifiziertes Recht; 452
- explizites Verbot; 448
- Explizitheit; 326
- Exponentiation; 80
- exponentiell klein; 64
- Export; 352
- Fail-stop-Signatursysteme; 238
- Fake-Terminal-Angriff; 401
- Faktorisierungsannahme; 95
- Falltür-Einwegfunktion; 45
- fast überall schwer; 64
- FEAL (Blockchiffre); 158
- Fehler 1. Art; 398
- Fehler 2. Art; 398
- Fehlerausbreitung; 146
- Fehlerfinden; 339
- Fehlerquellen; 16
- Fehlertoleranz; 16; 330
- Feistelprinzip; 131; 133
- Fenster; 626
- feste Zerlegung einer statistischen Datenbank; 715
- Fiat-Shamir-Identifikationssystem; 231
- File Handle bei NFS; 431
- Fileserver; 583; 593
- Filter-Operation; 533
- finanziell beschränkt; 19
- Fingerprint; 295
- FIPS (amer. Standards); 222
- FIPS 140-1; 387
- Firewall; 438; 724
- Firewall mit Authentikation; 736

- Flußaspekt; 515; 536
- FORK; 569
- formal; 339
- Framework; 356; 752
- freie Beweiswürdigung; 350
- freiwillige Zugriffskontrolle; 511
- Freshness; 321
- frisch; 321
- funktionale Abhängigkeit; 698
- Funktionalitätsklassen; 760
- Funktionstrennung; 424
- Gate (Firewalltyp); 743
- Geburtstagsangriff; 260
- Gedächtnis; 50
- geheimer Schlüssel; 34
- Geheimhaltung, hinreichendes Kriterium; 126
- Geheimhaltungsformel; 125; 638; 644; 673
- Geheimhaltungsziele; 13
- Geheimzuhaltendes in reaktivem System; 669
- gemeinsamer Münzwurf; 179
- Generator; 105; 108; 116
- Generator in Untergruppe erzeugen; 119
- Geräte, eigene; 366
- Geräte, portable; 366
- Geräteidentifikation; 388; 401
- geringstmögliche Privilegien; 416
- Gesamtcapability; 607
- Geschäftsbedingung; 300
- getypte Zugriffskontrolle; 455
- gewählte Nachricht; 54; 58
- gewählter Klartext; 57
- gewählter MAC; 58
- gewählter Schlüsseltext; 57
- ggT (größter gemeinsamer Teiler); 83
- Glaubenslogik; 342
- globale Zeit; 323
- GMR (Signaturssystem); 237
- Grantrecht; 462
- Grantrecht bei konkreten Capabilities; 605
- größte untere Schranke; 526
- Grundschutzhandbuch; 761
- Gruppe; 445
- Gruppenordnung; 102
- Gruppensignaturen; 238
- GSM-Mobiltelefonkarten; 379
- Guillou-Quisquater-Identifikationssystem; 231
- Gültigkeitsdauer; 297
- Haftung; 297
- halbkaskadierter Rechteentzug; 509
- Halteproblem; 484
- Handelnde in HRU; 475
- Handlungsfolge; 536
- Hardware-Reset-Mechanismen; 401
- Hashfunktionen; 46; 243
- Hashfunktionen aus Blockchiffren; 259
- Hashfunktionen für lange Nachrichten; 255
- Hashfunktionen in Signatursystemen; 216; 275
- Hashfunktionen, beweisbar kollisionsfrei; 252
- Hashfunktionen, direkt konstruierte; 262
- Häufungsverfahren; 398
- herunterstufen; 529
- Hierarchie; 446; 686
- Hilfsvariablen in
 - Informationsflußuntersuchung; 652; 660
- HMAC (Authentikationssystem); 210
- Hochschreiben; 529
- höhere Betriebssystemschichten; 626
- höhere Programmiersprachen,
 - Schutzfunktionen; 625
- Hostauthentikationsprobleme; 428
- HRU (Sprache für Rechteweitergaberegeln); 465
- hybride Verschlüsselung; 168; 273
- Hydra; 570; 585; 601
- I/O-Gerät; 576
- iAPX432; 556
- IDEA (Blockchiffre); 141; 158
- Identifikation; 333
- Identifikation, Einbau in Anwendung; 388; 406
- Identifikation, Einbau in verteiltes Szenario; 388; 404
- Identifikationssystem; 231
- Identitätsprüfung; 291; 293
- Import; 352
- Individualdaten; 703
- Inferenzkontrolle; 702
- Informationsfluß durch Abbruch; 649
- Informationsfluß durch Kontrollfluß; 646
- Informationsfluß in sequentiellen Programmen; 641
- Informationsfluß, direkt; 646
- Informationsfluß, dynamische Entscheidung; 649

- Informationsfluß, indirekt; 646
- Informationsfluß, statische Entscheidung; 651
- Informationsflußentscheidungsproblem; 647
- Informationsflußkontrolle; 440; 638
- Informationsflußspezifikation; 532; 578
- Informationssystem; 685; 686
- informationstheoretisch; 60
- Initialisierungsvektor; 149
- Inklusionsabhängigkeit; 701
- innen; 724
- Instanzenrecht; 453
- Integrität; 13
- Intel-Prozessoren; 551
- Interaktion; 50
- Interessensgruppe; 12
- Interleaving; 59
- Internet-Aufbau; 728
- Internet-Kiosk; 405
- Interprozeßkommunikation; 576
- Intervalle bei Benutzeridentifikation; 406
- Intrusion detection; 631; 635
- Invertieren von Restklassen; 82
- IP; 729
- IP-Adressen, Fälschung; 428
- IPSEC; 361; 363
- IPv6; 361
- ISO 9000; 761
- ISO-Standard 7816; 380
- ISO-Standard 9594-8; 312
- ISS; 438
- ist Teil von (Hierarchie); 448
- Iteration bei Blockchiffren; 131
- iterierte Hashfunktion; 261
- ITSEC; 757
- Jacobi-Symbol; 164
- Java; 432
- Java-Card; 622
- Java-Virtual-Machine; 624
- Judy Moore's Angriff; 215
- juristische Aspekte; 350
- juristische Maßnahmen; 22
- k-aus-n; 18
- kanonische Abbildung; 90
- kaskadierter Rechteentzug; 502
- Kerberos; 357; 363
- Kernobjekte bei großen Betriebssystemkernen; 574
- Kernobjekte bei kleinen Betriebssystemkernen; 580
- Kernsubjekt; 564; 571
- kernverwaltete Capability; 597
- Kindprozeß; 609; 613
- Klartext; 29
- Klartext-Schlüsseltext-Angriff; 56
- Klassenrecht; 453
- kleiner Fermatscher Satz; 107
- kleinste obere Schranke; 526
- Kollision; 46
- kollisionsfrei; 47; 219; 245
- Kombinationen kryptographischer Systeme; 273
- Kombinationen, Anwenderschnittstelle; 278
- Kombinationsmöglichkeiten; 716
- kombinierte Sicherheitsstufen; 527
- kommerzielle Integrität; 513
- kommerzielle Zugriffskontrolle; 512
- komplexitätstheoretisch; 60
- komplexitätstheoretisch beschränkt; 19
- Komplexitätstheorie; 64
- Konfigurationsdateien; 420
- Konfigurationsprüfer; 422; 438
- Konflikt; 449
- Konfusion; 131; 137
- Kongruenz; 75
- Kongruenzeigenschaft; 76
- Konsole; 456
- Konzelation; 28
- Krawczyk's System; 205
- Kreditkarten; 377
- kritischer Schritt; 406
- Kryptobibliothek; 278
- Kryptogesetze; 353
- Kryptographie; 2; 25
- Kryptographie, nichtdigitale Angriffe; 385
- kryptographisch; 60
- Kryptologie; 25
- L3; 593; 610
- Längenregister; 546
- leicht; 65
- LFSR; 267
- lineare Adresse; 554
- lineare Algebra; 87
- lineare Gleichungssysteme; 87
- lineare Kryptoanalyse; 139

- Logdatei; 423; 438; 633
- Logdatei, Auswertung; 635
- logische Adresse; 547
- lokaler Namensraum; 588
- löschen; 374
- Lucas-Funktionen; 189
- Lüfter; 282
- MAC; 35; 36; 196
- MAC (mandatory access control); 511
- Mach; 571; 593; 610
- Magnetkarten; 376
- Mail-Gateway; 740
- Makrostatistik; 720
- Manipulationsschutz; 370
- MAP; 581
- maschinenunabhängig; 65
- Masterschlüssel; 287
- Maximalstufe; 529
- McEliece; 189
- MD4 (Hashfunktion); 262
- MD5 (Hashfunktion); 262
- medizinische Datenbank; 703
- mehrseitige Sicherheit; 17; 366
- Menschenkenntnis; 307
- Metarechteart; 462; 493
- Methoden (Rechte auf); 514
- Microprobe; 382
- Mikrokern; 570
- Mikrostatistik; 720
- militärischer Ansatz; 511
- MIME, Viren in; 416
- MM-Merkmal; 377
- mobile Agenten; 456
- Mobile-Virus-Modell; 19
- Mobiltelefon; 408
- MOD-Operator; 77
- Modi von Blockchiffren; 143; 208; 276
- modular; 424
- Modularisierung; 427
- modulo; 75
- Modus; 557
- monotone Logik; 346
- monotone Weitergaberegeln; 499
- Multifunktionalität; 622
- Multi-Policy; 464; 615
- Multi-Policy-Kern; 600
- Multicast; 174
- Multics; 558; 570
- Multilevel-System; 511
- Mustererkennung; 397
- Nachrichtenformate; 329
- Nachrichtenlänge; 50
- Nachrichtenummer; 327
- Nachrichtensemantik; 329
- Name; 296; 314
- Namensverwaltung; 626
- Nebenklassen; 102
- negatives Recht; 448; 450
- Netscape; 360
- Netze; 722
- News-Gruppen; 10
- nichtdigitale Angriffe; 385
- nichtkaskadierter Rechteentzug; 508
- Nichtlinearität; 137
- nichtnumerische Daten; 709
- Nonce; 324
- Notfallzugriff; 632
- NP-leicht; 63
- Nullstellen; 87
- Objekt; 442
- Objekte auf Hardwareebene; 556
- objektorientierte Betriebssysteme; 573; 580; 595
- objektorientierte Rechte; 601; 686
- Objektorientierung bei Zugriffskontrolle; 446
- OFB (Betriebsart); 153; 264
- öffentlicher Exponent, kleiner; 173
- öffentlicher Schlüssel; 34
- One-time-Pad; 122; 128
- Ong-Schnorr-Shamir-Signatursystem; 231
- Oracle; 503; 688
- Orakel; 67
- Orange Book; 757
- Ordnung; 102; 103
- organisatorische Sicherheit; 364; 366
- Paketfilter; 730; 742
- Papierverzeichnis; 290; 302
- Parameterprüfung, fehlende; 426
- partielle Information; 42; 54; 164
- partielle Ordnung; 525
- passiver Angriff; 56
- Passphrase; 390
- Paßwort; 390; 391
- Paßwortdatei; 393

- Paßwortprobleme bei UNIX; 419
- PCBC (Betriebsart); 156
- PEM; 359
- Pentium; 551
- Personalkontrolle; 366
- persönliches Wissen; 396
- Petrinetz; 537
- Pfadangriffe; 421
- PGP; 295; 358; 363
- PGP, Zertifikate; 311
- Phi-Funktion; 85
- physiognomische Merkmale; 397
- physische Adresse; 547
- physische Angriffsklassen; 371
- physische Sicherheit; 364; 369
- physischer Zugriff; 371
- PIN; 390
- PINs, zentral gewählte; 393
- PKI (public-key infrastructure); 290
- policy; 300
- Policy Manager; 600
- Polyinstantiierung; 692; 696
- polynomial; 65
- Port; 576; 592; 606; 611
- portable Geräte; 366
- POS-Terminal; 367
- postfixfrei; 258
- Postscript, Viren in; 416
- Primitivwurzel; 109
- Primzahlerzeugung; 98
- Primzahlsatz; 98
- Priorität; 452
- Privaturkunde; 350
- privilegierte Befehle; 559
- privilegiertes Zustand; 557
- PRNG; 49
- probabilistische Algorithmen; 64; 68
- probabilistische Turingmaschine; 69
- probabilistische Verschlüsselung; 33
- Probierangriff; 33
- Produkte, kryptographische; 356
- Produzenten; 16
- Programmfehler; 441
- Programmierschnittstelle; 356
- Programmtextrecht; 456
- Protokolle, einfache; 320
- Protokollierung; 631
- Protokollspezifikation; 330
- Protokollstandard; 356
- Proxy; 457; 735; 741
- Prozeßdeskriptor; 564
- Prozessorkarte; 378
- Prozessormodus; 557; 563
- Prozessorzustand; 557
- Prozessorzustand (im allg. Sinn); 564
- Prozeß; 564; 572
- Prozeßsteuerrechner; 623
- prüfen; 40
- Prüfsummen über Programme; 422
- Pseudo-one-time-Pad; 145; 153; 158
- Pseudonym; 296; 316
- Pseudonymität; 14
- Pseudozufallsbitfolgenerator; 49
- Pseudozufallsgenerator; 48; 153; 264
- Pseudozufallsgenerator, Sicherheitsdefinition; 270
- Pseudozufallsgeneratoren aus Blockchiffren; 264
- Pseudozufallsgeneratoren, beweisbar sicher; 268
- Pseudozufallsgeneratoren, direkte Konstruktionen; 267
- Pseudozufallsgeneratoren, Einsatz; 277
- Pseudozufallspermutationen; 276
- Pseudozufallszahlengenerator; 49
- puffern; 373
- quadratisches Sieb; 97
- Qualitätsverbesserung; 284
- Quantenkryptographie; 387
- Rabin-Miller-Test; 99; 107
- Rabin-System; 189
- Rateangriffe; 391
- räumliche Sicherung; 366
- Rauschdioden; 282
- RC5 (Blockchiffre); 158
- reaktives System; 640; 665
- reaktives System, Ein-/Ausgabeverhalten; 667
- reaktives System, Zustand; 668
- Rechenfähigkeiten; 60
- Rechteamplifikation; 601
- Rechteart; 442; 444
- Rechtearten, anwendungsbezogen; 491
- Rechteentzug; 501
- Rechteentzug bei Capabilities; 616

- Rechteentzug, halbkaskadiert; 509
- Rechteentzug, kaskadiert; 502
- Rechteentzug, nichtkaskadiert; 508
- Rechteimplementierung; 596
- Rechtekombination; 453; 614
- Rechteweitergabe; 461
- Rechteweitergabe als Methode; 615
- Rechteweitergabe bei Zugriffskontrolllisten;
620
- Rechteweitergabe, Implementierung; 596
- Reduktion; 67
- Redundanz; 166; 220
- Regelschema; 466
- Register; 564
- Registrierung; 291
- rein beobachtend; 19; 56
- reiner Schlüsseltext-Angriff; 56
- Relation (in Datenbank); 687
- relationale Datenbank; 687
- Replay; 59
- Replayvermeidung; 321
- Repräsentantensystem; 77
- Restklasse; 76
- Restklassenring; 75
- rigoros; 339
- RIPMD-160 (Hashfunktion); 262
- Risikoanalyse; 18
- Risikoklassen; 407
- risikoscheu; 19
- rlogin; 420; 429
- Rolle; 445; 446; 508
- Rollentrennung; 514; 536; 756
- Rotormaschinen; 158
- Router; 729; 742
- RPC (Remote Procedure Call); 607
- RSA (Trapdoor-Einwegpermutationen); 159
- RSA, Effizienzverbesserungen; 172
- RSA, Homomorphie; 164; 214
- RSA-Annahme(n); 163
- RSA-Signatursystem; 213
- RSA-Signatursystem, Angriffe; 214
- RSA-Signatursystem, naiv; 213
- RSA-Verschlüsselung; 159
- RSA-Verschlüsselung, Angriffe; 164
- RSA-Verschlüsselung, naiv; 164
- Rückkopplungsfunktion; 267
- Rückruf; 310
- Rucksacksysteme; 189; 231
- Rückwärts-Verzeigerung; 616
- Runde; 131; 132
- Rundung; 717
- Rundung der Einzelwerte; 719
- Rundung in Ausgabe; 718
- Runterschreiben; 529
- S/MIME; 359
- Sandbox; 416; 432
- SATAN; 438
- Satz vom primitiven Element; 109
- Satz von Lagrange; 102
- Satz von Rice; 647
- Schadensfunktion; 414
- Schatten-Paßwortdatei; 393
- Schemainformation; 688
- Schicht; 541; 582
- Schieberegister; 267
- schirmen; 374
- Schlüssel; 27
- Schlüssel ohne Personenzuordnung; 316
- Schlüssel, Verwendungsbeschränkung; 297;
312
- Schlüsselattribut; 694
- Schlüsselerzeugung; 31
- Schlüsselerzeugung für Diskreter-Log-
Systeme; 116
- Schlüsselgenerierung; 31
- Schlüsselgenerierung, kompliziertere; 50
- schlüssellose Hashfunktion; 47
- Schlüsseltext; 29
- Schlüsseltextrückführung; 151
- Schlüsselverteilung; 280; 286
- Schlüsselverteilung über Massenmedien; 294
- Schlüsselverteilung, persönlich; 287; 290; 292
- Schlüsselverteiltzentrale(n); 288
- Schlüsselzertifikat; 291; 299
- Schnittstellenablauf; 666
- Schnorr-Signatursystem; 222; 230
- Schreibrechte auf fremde Objekte, Problem;
435
- Schreibrechte auf Konfigurationsdateien; 420
- Schreibrechte, unnötige; 416; 435
- Schriftform; 350
- Schulmethoden; 79
- Schutzdomäne; 568
- Schutzschicht; 373

- Schutzsubjekt bei großem Betriebssystemkern; 567
- Schutzsubjekt bei kleinem Betriebssystemkern; 571
- Schutzziele; 13
- schwer; 65
- Scramblen des Chipdesigns; 375
- SDL (Protokollspezifikationsprache); 330
- SDSI (Zertifizierungsvorschlag); 315
- Segment; 550; 580
- Segmentdeskriptor; 553
- Segmentregister; 551
- Seite; 549
- Seitentabelle; 549
- selbstsynchronisierend; 146
- selektive Fälschung; 54
- Semantik; 451
- semantische Bedingung; 686; 691
- semantische Sicherheit; 190
- Sensoren; 373
- Separierbarkeit; 663
- Sequenznummern; 323
- Servicecode; 437
- Setgid; 566
- Setuid; 566
- Setuid-Bit; 566
- Setuid-Programme; 425
- Setuid-Shell; 425
- SHA-1 (Hashfunktion); 262
- Shannon-Theorie; 122
- Shell; 626
- Shell-Escape; 425
- Sicherheit; 1; 12
- Sicherheit, generelle Aspekte; 364
- Sicherheit, nichtkryptographische; 364
- Sicherheit, Zusammenhang kryptographische und nichtkryptographische; 365
- Sicherheitsbegriffe; 12
- Sicherheitsbeweise; 66
- Sicherheitsgrad; 27; 52
- Sicherheitskriterien; 755; 757
- Sicherheitsmodul; 368; 369
- Sicherheitsparameter; 29
- Sicherheitsstufen; 511
- Sicherheitsstufen für Integrität; 534
- Sicherheitsstufen, allgemein; 525
- Sicherheitsstufen, einfach; 521
- Sicht; 689
- Sichtbarkeit; 625
- Signal; 576
- Signatur; 40
- Signaturgesetz; 314; 351
- Signaturssysteme; 37; 213
- Signaturssysteme, beweisbar sicher; 236
- Signaturssysteme, Sicherheitsdefinition; 232
- signieren; 40
- Signierschlüssel; 37
- Single-step-Modus; 373
- Sitzung; 529
- Sitzungsschlüssel; 287; 336
- smap; 438
- Smartcard; 378
- Smartcardbetriebssystem; 621
- Smartcardprozessor; 545; 621
- Smartcards, Schwächen; 380
- Socket-Funktionen; 739
- SOCKS; 737
- socksifizieren; 739
- Software-Fehlertoleranz; 756
- Softwareinterrupt; 560
- Sorgfalt; 307
- Spannungsversorgung, Wichtigkeit; 375
- Speicherkanal; 436; 676
- Speicherobjekt (bei Mach); 594
- Speicherschutz; 545
- Speicherschutzbit; 555; 558
- Spezifikation erlaubter Informationsflüsse; 642
- Spezifikation von Zugriffskontrollzustand; 445
- SPKI (Zertifizierungsvorschlag); 315
- Spur; 666
- Spürhund; 710
- SQL; 503
- SQL-Notation; 689; 690
- SRL (Subjekt-Restriktionsliste); 614
- SSH; 746
- SSH (Secure Shell); 362; 363
- SSL (Secure Socket Layer); 360; 363
- SSLeay; 360
- Standards, kryptographische; 356
- Standards, physische Sicherheit; 387
- Startwert; 48
- Statistik; 533
- Statistiken, Kombination; 708
- statistische Datenbank; 702

- statistische Datenbanken, Ziel; 703
- statistische Operation; 690
- Steganographie; 353
- Steuerprogramm (Beispiel); 664; 679
- Stimmerkennung; 293
- Strahlung; 371
- Stromchiffre; 145
- Stromversorgung; 373
- strongly universal2; 200
- Struktur; 50
- strukturierter Entwurf; 756
- subexponentiell; 97
- Subjekt; 442
- Subjekt-Restriktionsliste; 614
- subjektseitige Weitergabe; 599
- Substitutionen; 158
- Substitutions-Permutations-Prinzip; 131; 137
- Substitutionsbox; 136
- Superencryption; 353
- Superuser; 423
- Supervisor-Modus; 557
- swatch; 438
- Sybase; 688
- symmetrisch; 27
- symmetrische Authentikation; 35; 195
- symmetrische Repräsentation; 78
- symmetrische Verschlüsselung; 29; 122
- synchron; 146
- Syntaxbaum; 652
- System R; 503
- Systemaufruf; 576
- Systemauslastung (als versteckter Kanal); 677
- Systemschichten; 541
- Systemtypen; 28
- Tabelle (in Datenbank); 687
- Take-Grant in konkreter Implementierung; 605
- Take-Grant-Schema; 491
- Takerecht; 477
- Taktversorgung; 373
- TAN; 335
- Tätigkeiten, bei Biometrik; 397
- TCP; 729
- tcpwrapper; 438
- technische Maßnahmen; 22
- Teilmengenverband; 526
- Teilrecht; 453; 579
- Teilrecht, Weitergabe bei benutzerverwalteten Capabilities; 608
- Teilschlüssel; 132
- Teilschlüsselerzeugung; 137
- Telefonkarten; 378
- Telefonrückruf; 293
- Test; 35
- Testalgorithmen; 270
- Tests ausspezifizieren; 330
- Testschlüssel; 37
- Thread; 571
- Tiger; 438
- TMach; 571
- Token; 400
- Top-level-Spezifikation; 517; 532
- totale Ordnung; 526
- Tracker; 710
- Trägermenge; 123
- Transaktions-ID; 325
- Transaktionsnummer; 327
- transitives trojanisches Pferd; 437
- Trap; 560; 565
- Trapdoor-Einwegpermutationen; 44
- Tresor; 366
- Trial Division; 99
- Tripel in Zugriffskontrollzustand; 442
- Tripel-DES; 131; 140
- tripwire; 438
- trojanisches Pferd; 434; 441; 757
- trojanisches Pferd, Nutzung von verstecktem Kanal; 679
- trojanisches Pferd, transitiv; 437
- trojanisches Pferd, universell; 437
- Tsudiks System; 210
- Tupel (in Datenbank); 688
- Turing-Reduktion; 67
- Turingmaschine; 484
- Türzugang; 322; 333
- Typ bei Zugriffskontrolle; 445
- Typ, Implementierung in Hydra; 586
- Typ-Tag; 555
- Typen auf Hardwareebene; 555
- Überblicksartikel; 6
- UCLA Secure UNIX; 570; 581; 600
- Umgebungsbedingung; 371
- unäre Prädikate (in HRU); 472
- Unbeobachtbarkeit; 14

- Unentscheidbarkeit bei Informationsfluß; 647
- Unentscheidbarkeit bei
 - Informationsflußkontrolle; 647
- Unentscheidbarkeit bei Zugriffskontrolle; 480
- universelles trojanisches Pferd; 437
- UNIX-Paßwörter; 392
- unsichtbare Signaturen; 238
- Untergruppen zyklischer Gruppen; 108
- unterschreiben; 40
- Unterschrift; 40
- unterzeichnen; 40
- Ununterscheidbarkeit; 190
- Urbild; 41
- User-Modus; 557
- Verantwortungszuweisung; 20; 435; 634; 757
- Verband; 525; 532
- Verbot; 448
- Verfolgung aller Kombinationsmöglichkeiten;
 - 716
- Verfügbarkeit; 13
- Verhaltensmuster; 636
- verhindern; 21
- Verifikation; 756
- verifizieren; 40
- Verlust verhindern; 368
- vernachlässigbar; 64; 68
- Vernam-Chiffre; 122; 128
- Vernam-Chiffre, Optimalität; 130
- Verschlüsselung, Sicherheitsdefinition; 190
- versteckter Kanal; 436; 440; 676
- versteckter Kanal, Kapazität; 680
- Vertrauen; 12; 15
- Vertrauensgrad; 18
- Vertrauensmodell; 17; 18; 291; 304
- Vertrauensstruktur; 18
- vertrauenswürdige Kommunikation mit
 - Benutzer; 364
- vertrauenswürdiger Entwurf; 364
- Vertraulichkeit; 13
- Vertraulichkeitsverletzung; 21
- Vertretersystem; 77
- Verwürfeln des Chipdesigns; 375
- Verzeichnis; 574
- Verzögern physischer Angriffe; 373
- Virenerkennung; 417
- virtuelle Adressierung; 548
- virtuelle Maschine; 624
- virtueller Speicher; 593
- Virus; 414; 434
- visuelle Verschlüsselung; 410
- vollständige Suche; 61; 62
- Voreinstellungen; 422
- vorgeschriebene Zugriffskontrolle; 511
- Vorwegberechnung; 229
- Vorwissen; 124
- W'keit (Abk. f. Wahrscheinlichkeit); 68
- Wartungsdienst; 16
- Wegman-Carter-Basissystem; 201
- Weitergabe bei benutzerverwalteten
 - Capabilities; 608
- Weitergabe von Rechten; 461
- Werkzeuge für UNIX-Sicherheit; 438; 439
- Willenserklärung; 350
- Wirtsprogramm; 414
- Wissen; 390
- wohlgeformte Transaktion; 514; 536; 686; 693
- Word, Viren in; 415
- Worst-case-Komplexität; 64
- Wörterbuchangriff; 391
- Wrapper; 438; 457
- X Windows; 430
- X.509; 312
- X.509v3; 312
- x^2 -mod- n -Generator; 268
- Zeichensynchronisation; 146
- Zeitkanal; 436; 676; 681
- Zeitschranken bei Capabilities; 617
- Zeitstempel; 323
- Zertifikat; 299
- Zertifikat, genauer Inhalt; 300
- Zertifikat, Haftung; 301
- Zertifikat, Rückruf; 310
- Zertifikate persönlicher Bekannter; 304
- Zertifikate staatlicher Stellen; 304
- Zertifikate, mehrere; 304
- Zertifikate, Verteilung; 302
- Zertifikatskette; 305
- Zertifizierung, hierarchisch; 313
- Zertifizierungsrechner; 623
- Ziel; 12
- Ziele, genauere; 50
- zufällige Fehler in Ausgabe; 717
- zufällige Fehler in Einzelwerten; 719

Zufallspermutationen, Modellierung von
 Blockchiffren; 144
Zufallszahlen; 284
Zufallszahlen aus Rechner; 283
Zufallszahlen vom Benutzer; 283
Zufallszahlen, echte; 280
Zufallszahlen, physikalisch; 282
Zugangsschutz; 389
Zugangsstruktur; 18
Zugriff aus der Ferne; 722; 745
Zugriffsart; 442
Zugriffsbedingungen, nicht maschinell
 prüfbare; 632
Zugriffskontrolle; 364; 441
Zugriffskontrolle, Semantik; 442
Zugriffskontrollentscheidung; 451
Zugriffskontrollliste; 420; 443
Zugriffskontrollliste als konkrete
 Implementierung; 596
Zugriffskontrollliste bei Speicherschutz; 555
Zugriffskontrolllisten in objektorientierten
 Betriebssystemen; 614
Zugriffskontrollmatrix; 442
Zugriffskontrollsprachen, Kriterien; 458
Zugriffskontrollstrategien; 440
Zugriffskontrollzustand; 442
Zugriffskontrollzustand als Graph; 494
Zugriffskontrollzustand, Spezifikation; 445
Zuordnung Person-Schlüssel; 291
Zuordnung Person-Schlüssel, genauer Inhalt;
 297
Zurechenbarkeit; 20
Zusatzwissen; 703
Zustandswechsel (Prozessor); 560
Zweck; 27
zyklisch; 105
zyklische Gruppe; 102

Englische Begriffe

*-property; 528
access control; 441
access control list; 420; 443
access control policy; 479
access structure; 18
accountability; 20
acyclic MTAM (Regelschema); 499
adversary; 15
aggregation; 690
arbiter; 206
assurance; 758
attribute certificate; 299
authorization; 441
authorization scheme; 466
availability; 13
badge; 333
birthday attack; 260
brute-force search; 61
certification authority; 301
certified discrete log; 113
challenge-response; 324
chinese remainder theorem; 89
Chinese wall; 518
chosen-ciphertext; 57
chosen-message; 58
chosen-plaintext; 57
cipher feedback; 151
cipher-block chaining; 149
ciphertext; 31
ciphertext-only; 56
classification; 521
clearance; 522
cleartext; 31
compartment; 446; 523
computational; 60
confidentiality; 13
covert channel; 436; 676
credential; 299
decipher; 31
declassify; 529
decrypt; 31
decryption key; 34
Digital Signature Standard; 222
directory; 291; 302
discretionary access control; 511

domain; 446
dual-ported host; 742
effective uid; 566
electronic codebook; 147
encipher; 31
encrypt; 31
encryption key; 34
enemy; 15
evidence; 17
execution; 666
execution environment; 568
existential break; 54
extensible systems; 433
extension header; 361
fault-based cryptanalysis; 385
file descriptor; 575
freshness; 321
guardian; 367
header, IP; 361
high-water-mark; 532; 660
infeasible; 65
initial belief; 344; 347
integrity; 13
key; 31
key certificate; 299
key recovery; 354
key server; 291; 302
keyed hash function; 36
knapsack; 189
known-plaintext; 56
labeling; 525
lattice; 525
least privilege; 416; 424; 427; 598
lightweight process; 571
linear feedback shift register; 267
logic of belief; 342
mafia fraud; 334
magic cookie (bei X Windows); 430
man-in-the-middle; 334
mandatory access control; 511
maximum-order control; 714
meet-in-the-middle; 140
memory channel; 676
memory object; 594
message authentication code; 35
middle-person; 334
middle-person attack; 33
mounten; 429
multi-level; 511
multi-party security; 17
multi-policy; 464
network computing; 405
nonce; 324
nondeducibility; 673
noninterference; 672
number field sieve; 97; 114
one-time pad; 122
one-way; 42
open file descriptor; 575
output feedback; 153
payload; 361
perturbation; 717
plaintext; 31
policy; 479; 515
precomputation; 229
private key; 34
private-key; 31
privileged mode; 557
protection domain; 568
protection ring; 558
protection system; 466
pseudo-random number generator; 49
public key; 34
public key agreement; 178
public-key infrastructure; 290
query restriction; 707
real group id; 564
real uid; 564
replay; 59
revocation (von Schlüsselzertifikat); 310
revocation (von Recht); 501
run; 666
salt; 393
secret key; 34
secret-key exchange; 178
security association; 361
security level; 521
selective break; 54
separation of duty; 514
simple security property; 528
sniffing; 419
spread spectrum; 387
square-and-multiply; 80
strongly universal₂; 200

stub; 565
 superencryption; 353
 tamper-proof; 370
 tamper-resistance; 370
 task; 571
 threat; 15
 ticket; 357
 timeliness; 322
 timing attack; 385
 timing channel; 676
 total break; 53
 totient function; 85
 trace; 666
 transport mode; 361
 trust center; 17; 366
 trust domain; 456
 trust model; 291
 trusted path; 401
 trusted process; 563; 579; 600
 trusted subject; 529
 tunnel mode; 361
 typed access control; 455
 unconditional; 60
 undeniable signatures; 238
 universal break; 53
 universal one-way; 246
 unwinding; 675
 user identification; 389
 view; 689
 wallet; 367; 408
 web of trust; 311
 well-formed transaction; 514
 workflow; 514; 536
 wrapper; 438

Symbole

.login; 421; 434
 .rhosts; 420
 :: (in W'keiten); 68
 ; (Hintereinanderausführung); 68
 <•> (erzeugte Untergruppe); 105
 \cong (isomorph); 89
 $\rightarrow_{\alpha(x_1, \dots, x_k)}$ (in HRU); 470
 \rightarrow_{op} (in HRU); 468
 \Rightarrow (in HRU); 471
 \Rightarrow^* (in HRU); 471
 $\Rightarrow_{S_{trust}}$ (zu HRU); 478
 $\Rightarrow_{S_{trust}}^*$ (zu HRU); 478
 \lceil (Viewoperator); 671
 $\lfloor \bullet \rfloor$ (Trägermenge); 123
 $\bar{\quad}$ (Restklasse); 76
 $\{X^P\}_K$; 343
 $|$ (Teiler); 75
 $|\bullet|$ (Ordnung); 102
 \leftarrow (probabilistische Zuweisung); 68
 ∞ (unendlich); 103
 \pm (Variable bei Rechten); 452
 \leq (auf Sicherheitsstufen); 526
 \leq (Untergruppe); 102
 \times (kartesisches Produkt); 89
 \equiv (kongruent); 75
abrech; 664
Aut_{B,X}; 306
auth; 35
believes; 344
c (Schlüsseltext); 29
Cert_{X,Y}; 306
 CHANGED; 653
 Char; 710
C_l (Schlüsseltextraum); 124
 COMMAND; 466
controls; 344
 COUNT; 705
 CREATE; 465
create_with_accessmode; 492
d (bei RSA); 160
 DELETE; 465
 DESTROY; 465
 Digital Signature Algorithm; 222
DPL (bei Intel-Prozessoren); 552
e (bei RSA); 160

- ent*; 29
- ENTER; 465
- erklärung*; 664
- EXEC; 565
- exp_g*; 106
- Φ (verbotene Auswahl); 710
- f* (oft Einwegfunktion); 41
- ϕ (oft Phi-Funktion); 85
- falsch*; 35
- fd* (file descriptor); 574
- fresh*; 343
- FROM (in SQL); 689
- geheim*; 522
- gen*; 29
- grant*; 462; 491; 689
- grant_r*; 492; 503
- grant_{read}*; 471
- grant_{rg}*; 503
- guS; 527
- hash*; 46
- High*; 669
- hosts.equiv; 420
- Ind*; 710
- init* (bei UNIX); 568
- IP; 132
- is_a* (Hierarchie); 448
- k* (bei statistischer Datenbank); 707
- κ (kanonische Abbildung); 90
- k* (Schlüssel); 29
- kill*; 575
- K_l (Schlüsselraum); 124
- koS; 527
- L* (Menge von Sicherheitsstufen); 526
- l* (labeling); 526
- l* (Sicherheitsparameter); 29
- L(n)*; 97
- l** (zweiter Sicherheitsparameter); 111
- LABEL; 642
- l_{akt}* (aktuelle Stufe); 530
- len_p*; 111
- L_i (bei DES); 133
- log_g*; 100
- Low*; 670
- m* (Klartext); 29
- MAC; 35
- M_j*; Klartextrraum; 124
- mod; 75
- O* (Objektmenge); 442
- offen*; 522
- ok*; 35
- ord(g)*.; 103
- own_n*; 462
- $P \xleftrightarrow{K} Q$; 343
- $\pi(\bullet)$ (Anzahl Primzahlen); 98
- P(E)*; 68
- P_D ; 124
- pk* (öffentlicher Schlüssel); 32; 37
- poly; 68
- PZG; 48
- R* (Rechtearten); 442
- r* (read); 463
- R** (anwendungsbezogene Rechtearten); 491
- $Rec_{X,Y,i}$; 306
- revoke*_{rg}*; 506
- revoke*; 689
- revoke_{read}*; 472; 502
- revoke_{rg}*; 506
- rg* (read-grant); 463
- R_i (bei DES); 133
- RPL* (bei Intel-Prozessoren); 550
- rt*; 477
- S* (Subjektmenge); 442
- salt*; 393
- seed*; 48; 264
- SELECT (in SQL); 689
- SELECT AVERAGE; 690
- send-once*; 612
- sig*; 37
- sign*; 37
- sk* (geheimer Schlüssel); 32; 37
- streng_{geheim}*; 522
- su (bei UNIX); 421, 434, 568
- T* (Trackerformel); 710
- take*; 491
- take_r*; 492
- take_{read}*; 477
- test*; 35
- text*; 37
- $Trust_{B,X,i}$; 306
- Users*; 666
- ver*; 29
- vertraulich*; 522
- view*; 671
- w* (write); 463

Ω : (oft Ordnung); 103
wg (write-grant); 463
WHERE (in SQL); 689
x (execute); 463
xg (execute-grant); 463
z (Zufallszahl); 29
z' (Zufallszahl); 32
 Z_n^* ; 82
 Z_n ; 75
 Z_p^* ; 87