

Stichwortverzeichnis (inkl. Abkürzungen)

- 3,5 Zoll Diskette 47
- 8080-Prozessor 49
- 8086-Prozessor 49

- A-Modus 257, 258, 259
- a-posteriori-Wahrscheinlichkeit 42
- a-priori-Wahrscheinlichkeit 42
- AA-20 52
- abelsche Gruppe 92, 95
- Abfragen
 - verteilt und anonymes 147, 150
- abgerundeten Mittelwert 132
- Abhören 5
- abhörsicher 5
- Ablauf
 - alternativer 147
- Abrechnung 190, 283, 288, 293
 - generelle 288
 - individuelle 288
- Abrechnungsdaten 288
- Abruf
 - anonymer 86, 219, 276
- Absenderadresse
 - explizite 76
 - öffentliche 76
- Absenderangabe 65
- absolute Mehrheit 225, 226, 235, 240, 291
- Abstrahlung 115
- Ada 128, 150
- adaptive chosen ciphertext attack 45, 87
- adaptiven aktiven Angriff mit gewähltem Schlüsseltext 87
- Adreßbuchdienst 116
- Adresse
 - explizite 74, 205
 - implizite 64, 277, 285, 298
 - öffentliche 65, 74, 118, 196
 - offene implizite 118
 - private 65, 118
- Adreßerkennung 65, 192
- Adreßerzeugung 192
- Adreßfolge 219
- Adressierung
 - implizite 118
 - offene 64, 65, 66
 - offene implizite 219
 - verdeckte 64, 65, 66, 196
 - verdeckte implizite 219
- Adressierungsart 66, 67
- Adreßvergleich 219
- Adreßverwaltung 66, 67
- Adreßverzeichnis 65, 221
- Adreßverzeichnis mit anonymen Rückadressen 77
- Ähnlichkeit 200
- aktive Angriff 82
- aktiver Angreifer 254, 269
- aktiver Angriff 20, 46, 217, 235, 267
- aktiver Treuhänder 293
- aktiver Verkettungsangriff über Betriebsmittelknappheit 112
- Alpern 65, 99
- Alphabet 173
- Alphabetgröße 174
- Alternative 111, 114
- alternativer Ablauf 147
- Alternativfolgen 147
- Angreifer 15, 16, 18, 41, 56, 57, 62, 143, 199, 235, 269
 - aktiver 269
 - Stärke eines 15
- Angreifermodell 62, 143, 144, 243
- Angreiferstation 143, 144, 145
- Angriff 213
 - aktiver 20, 46, 82, 86, 235, 267
 - adaptiver 87
 - nachrichtenbezogener 20
 - schlüsselbezogener 20
 - passiver 20
- Angriff auf die Dienstleistung 98

- Angriff mit gewähltem Klartext 87, 88
- Angriff mit gewähltem Schlüsseltext 87
- Angriffstyp 20
- anonym 14, 15
- anonym übertragbarer Standardwert 292
- anonyme Kommunikation 62
- anonyme Postlagerung 86
- anonyme Rückadresse 75, 77, 80, 84, 86, 219, 221
- anonyme Rückadresse mit langer Gültigkeit 86, 221
- anonymen Rückadresse 85
- anonymer Abruf 86, 219, 276
- anonymer Anruf 299
- anonymer Kanal 87, 217, 278
- anonymer Mehrfachzugriff 114
- anonymes Abfragen 103
- anonymes digitales Zahlungssystem 288
- Anonymität 16, 70, 110, 111, 112, 114, 115, 156, 183, 187, 210, 213, 220, 254, 271, 292, 293, 299
 - Grad an 16
- Anonymitäts-Beweis 143
- Anonymitäts-Modus 257
- Anonymitätseigenschaft 154
- Anonymitätserhaltung 111, 119
 - perfekte 119
- Anonymitätsklasse 195, 196, 202, 203, 209
- Anschluß
 - öffentlicher 59
- ANSI/IEEE Std 802.5-1985 179
- Apple Macintosh II 47, 49
- Apple Macintosh Plus 49
- ARRA 121, 136
- Assoziativspeicher 65, 219
- asymmetrische Stromchiffre 33, 38
- asymmetrische synchrone Stromchiffre 38
- asymmetrisches Kommunikationsnetz 191
- asymmetrisches Konzelationssystem 44, 75, 230
- asymmetrisches Kryptosystem 20, 41
- asymmetrisches Protokoll 260
- asynchroner Übertragungsmodus 117
- asynchrones Mehrfachzugriffsverfahren 298
- asynchronous transfer mode 117
- ATM 117
- Aufdeckforderung 268, 269
 - mögliche 268
 - tatsächliche 268
- Aufdeckrisiko 267, 268
- Aufdeckverfahren 267, 268, 269
- Aufdeckverfahren für das DC-Netz 268
- Ausbau 272
- Ausgabe-Nachricht 89
- Ausgabetakt 180
- Ausgabetaktgenerierung 179, 182
- Auslassen von MIXen 227, 241, 244, 246, 247, 249, 250, 251, 252, 253
- Auslassen von möglichst vielen MIXen 238, 239, 240
- Auslassen von möglichst wenig MIXen 234, 235, 238, 239, 240
- Ausschnittsbüro 61
- Authentifikation 20, 41, 53, 56, 299
- Authentikationsprotokolle 290
- authentifizieren 290
- autonome Zahlung 291
- Autorisationsprüfung 290

- B-ISDN 3
- Bank 289, 291
- batch 68
- Baum 92, 111, 186, 270
- BAUM-Netz 102, 107, 108, 110, 111, 114, 116, 142, 181, 182, 192, 193, 195, 198, 199, 201, 205, 264, 265, 267, 269, 270, 271, 278, 282, 286, 287, 288, 299
- BAUM- ν DC-/Verteilnetz 202
- Baumann 8
- Baumnetz 278
- Baumtopologie 204
- bedeutungslose Nachricht 67, 90, 187, 268, 269
- bedeutungsloser Zeitscheibenkanal 276
- begrenzte Rechenkapazität 41
- Benutzergruppe
 - geschlossene 57

- Beobachtungsmöglichkeit 57
- Bereits-gemixt-Liste 86
- Besiedlungsstruktur 279
- Bestandsdaten 7
- bethlehemitischer Kindermord 195
- Betreiber 284
- Betreiberschaft 284
- Betriebsmittelknappheit 112
- Bewegtbild 1
- Bewegungsbilder 297
- Beweismethode 146
- BIGFON 2, 3, 157
- BIGFON-Pilotversuche 5
- Bildfernsprechen 2, 189, 191
- Bildschirmtext 1, 4, 5, 7, 166
- Bildschirmtext-Zentrale 56
- Bildschirmtextzentrale 8
- binäres überlagerndes Senden 93, 95
- bit pattern sensitive timing jitter 180
- bit string 71
- Bitkette 71, 76, 88
- Bitübertragungsschicht 109
- Block 78, 162
- block cipher 31
- Blockchiffre 31, 34, 48, 53, 82, 158, 218, 268, 269
 - deterministische 31, 34, 36
 - indeterministische 31
 - symmetrische 230
- Blockchiffre mit Blockverkettung 33, 38
- Blockchiffre mit Blockverkettung über Schlüssel- und Klartext 38, 39
- Blocklänge 31, 46, 78, 162
- Blocksystem 31
- Blockverkettung 32
- braided ring 261
- Brechen
 - nachrichtenbezogenes 25, 28, 46
 - partielles 46
- Breitband-ISDN 2, 3
- breitbandig 1
- Breitbandiges integriertes Glasfaser-Fernmeldeortsnetz 3
- Breitbandkabelverteilstnetz 1, 2, 3, 102, 181
- Brickell 142
- bridge 142
- Briefmarke
 - digitale 288, 289
- broadcast 63, 91, 110
- Broadcast-Medium 269
- Bruder
 - Großer 51
- büschelweise auftretender Verkehr 157
- büschelweise Vermittlung 117
- Burandt 99
- burst switching 117
- bursty traffic 157
- By-Pass-Einrichtung 261, 264
- bypass 261
- carrier sense multiple access 138
- CATV 181
- CCITT 173, 178
- channel switching 116
- Chaum 67, 88, 91, 92, 93, 100, 106, 137, 184, 185, 191, 268, 294
- Chiffrierfunktion 19
- Chiffrierschlüssel 45, 88
- chosen-ciphertext attack 20, 87
- chosen-plaintext attack 20
- cipher block chaining, abgekürzt CBC 32
- cipher feedback 32
- ciphertext-only attack 20
- Code
 - nichtlinearer 140
- coherent detection 156
- coherent optical fiber transmission 156
- collision resolution algorithm 124
- collision-avoidance circuit 107
- collision-avoidance switch 107
- Common Antenna Television 181
- Computer-Virus 7, 17
- confinement problem 297
- covert channel 18, 67, 298
- CRC 121, 257
- cryptographically strong pseudorandom bit generator 43
- CSMA 121, 138, 200

- CSMA/ARRA 121
- CSMA/CD 121, 138, 205
- CSMA/splitting algorithm 121
- cyclic redundancy check 121

- Data Encryption Standard 23, 45, 49
- data link layer 110
- Data Terminal Equipment 284
- datagram service 117
- Datagramdienst 117
- Datenexpansion 276
- Datenschutz 3, 18, 57, 112, 187, 213
 - überprüfbarer 57
- Datenschutz-Qualität 197
- Datenschutzproblem 273
- Datensicherheit 57
- Datensicherung 7
- Datum 243
- DBP 1, 3, 6, 8, 52, 53, 59, 181, 189
- DC-/DC-Netz
 - dynamisch adaptierbares 208
- DC-network 92
- DC-Netz 92, 97, 99, 103, 104, 108, 110, 111, 114, 116, 119, 142, 173, 176, 178, 183, 184, 185, 186, 192, 194, 199, 203, 204, 205, 206, 209, 214, 254, 255, 257, 259, 264, 267, 268, 269, 270, 271, 278, 282, 286, 287, 288, 298
 - dynamisch partitionierbares 204
 - senderpartitioniertes 254, 255
- DCE 284
- Dechiffrierschlüssel 45
- Deckung 291
- Demokratie 92
- denial of service 267
- DES 23, 45, 46, 49, 50, 51, 52, 163, 194, 268, 278, 301
 - Nachfolge von 50
 - verallgemeinertes 194, 301
- Determinismus
 - echter 132
- deterministisch 31
- deterministische Blockchiffre 31, 34, 36
- deterministisches Kryptosystem 76
- Deutsche Bundespost 1
- dezentrale Ansatz 19
- Diagnoseprogramm 284
- Dienst 112
- Dienstanbieter 190
- Diensteintegration 18
 - diensteintegrierend 1
 - diensteintegrierendes Digitalnetz 2, 300
 - diensteintegrierendes Netz 173
- Diensterbringung 267, 274
- dienstespezifische Netze 18
- Dienstqualität 283, 284, 287
- Dienstvorgabe 213, 214
- digital 2
 - digitale Briefmarke 288
 - digitale Signalregenerierung 92, 101, 102, 107, 108, 110, 111, 114, 180, 182, 183, 191, 199, 259, 261, 264, 286
- digitales Zahlungssystem 291
- digitalisieren 277
- Digitalisierung 2, 182
- Digitalisierung des Teilnehmeranschlusses 273
- Digitalnetz
 - diensteintegrierendes 2
- DIN 52
- Dining Cryptographers network 92
- direct detection 157
- directory service 116
- direkte Übertragung 121
- direktes Produkt 96
- direktes Umcodierungsschema 71
- disjunkte MIX-Folge 220, 222
- Diskette 47
- Dispersion 101, 295
- Dispute beim Aufdecken 269
- diversitär entworfen 273
- Dokument 293
- Dritte Partei
 - unbeteiligte 20
- DTE 284
- dummy traffic 90
- duplex channel 159, 161

- Duplex-Kanal 140, 149, 159, 161
- Durchmesser 186
- Durchsatz 125, 195, 238, 252
- dynamisch adaptierbares DC-/DC-Netz 208
- dynamisch adaptierbares Vermittlungs-/DC-Netz 206
- dynamisch aktivierte Redundanz 220
- dynamisch erzeugte Redundanz 223
- dynamisch erzeugte, dynamisch aktivierte Redundanz 221
- dynamisch erzeugte, statisch aktivierte Redundanz 222
- dynamisch partitionierbares DC-Netz 204, 205
- dynamisch partitionierbares RING-Netz 206

- Echtle 132, 254
- ECMA-89 179
- Effizienz 189, 280
- Einfehlerannahme 257, 258
- Eingabe-Nachricht 89
- Einschränkungsproblem 297
- Einwegfunktion 230, 231, 232, 240
- Einzelgebührennachweis 289
- elastic buffer 180
- elastischer Puffer 180, 182
- electronic mail 221
- electronic wallet 292
- elektronische Post 170, 194, 221, 278
- elektronisches Postfach 1
- Empfängeranonymitätsschema 74
- Empfangen
 - globales überlagerndes 125, 135, 298
 - paarweises überlagerndes 135, 140, 141, 298
 - überlagerndes 95
- Empfangsbestätigung 226, 243
- end-to-end encryption 54
- Ende-zu-Ende-Fehlerbehebung 213, 215, 217, 222, 250
- Ende-zu-Ende-Protokoll 217, 220, 222, 260
- Ende-zu-Ende-Verschlüsselung 53, 54, 55, 56, 57, 58, 108, 109, 141, 149, 217, 218, 272, 273, 285, 300
- Ende-zu-„Ende“-Verschlüsselung 282
- endliche abelsche Gruppe 96
- Entkopplungsalgorithmus 125
- Entropie 42, 43, 230, 231
- Entwurf 284
- Entwurfshilfsmittel 284
- Entwurfskosten 203
- Erasable-Laser-Optical-Disk 47
- Erdarbeiten 281
- Ereignis 15, 16
- Erfassungsmöglichkeit 19
- Erfolgswahrscheinlichkeit 43
- Ergebnisrückführung 36, 37, 163
- Erschließungszustand 279
- Ersetzen von MIXen 222, 240
- etappenweiser Ausbau 272
- explizite Absenderadresse 76
- explizite Adresse 64, 74, 195, 196, 197, 199, 205
- explizite Adressierung
 - verdeckte 196

- F-Modus 257, 258
- fail-stop Betrieb 220
- fair 107
- Faktor 88
- Faktorisierung 46
- Falle 268
- FCFS 125
- Fehler 86, 213, 217, 235, 267
- Fehlerbehandlung 213
- Fehlerdiagnose 255, 256
- fehlererkennender Code 217
- Fehlererkennung 257
- Fehlererweiterung 36
- Fehlerlokalisierung 257
- Fehlermodell 213, 226, 244
- fehlertolerant 189
- fehlertolerante anonyme Rückadresse 231, 232
- fehlertolerante Verschlüsselungsstruktur 271
- Fehlertoleranz 116, 210, 271
- Fehlertoleranz-Maßnahme 183
- Fehlertoleranz-Modus 257

- Fehlertoleranzverfahren 213
- Fehlerüberdeckung 256
- Fehlerursache 213, 214
- Fehlervorgabe 213, 219, 232, 244, 254, 256, 266
- fein 205
- Fernabfrage 284
- Fernablesen 297
- Fernkopieren 1
- Fernmeldegeheimnis 16
- Fernmeldemonopol 188, 300
- Fernmeldenetz 274
- Fernnetz 276, 278
- Fernsehen 1, 4, 56, 189
- Fernsehen mit Bezahlung gesehener Sendungen 190
- Fernsprechen 1
- Fernsprechnetzt 1, 2
 - analoges 1
 - digitales 1
- Fernvermittlungsstelle 274, 275, 277, 279
- Fernvermittlungstechnik 2
- Fernwartung 7, 18, 109, 284
- Fernwirken 1, 297
- fest speicherprogrammiert 17, 18, 273
- First Come First Serve 125
- flooding 110
- Flußregelungsmechanismen 178
- frame 137
- frei speicherprogrammierbar 273
- freie Speicherprogrammierbarkeit 197
- Führerschein 294
- Funk
 - öffentlicher mobiler 214, 295
- Funknetz 3, 190, 214, 295, 296

- GaAs 181
- gateway 201, 206, 208, 266
- Gebäude 272
- Gebührendaten 7
- geflochtener Baum 265
- geflochtener Ring 261, 263, 264
- Geheimdienst 56
- geheimes „Know-how“ 18

- Geheimhaltung 19
- Gemeinschaftsantennenanlagen 2
- generelle Abrechnung 288
- Generierung eines Schlüsselpaares 48
- Gerät
 - ausforschungssicheres 51
 - sicheres 41
- geschlossene Benutzergruppe 57
- Gesprächswunsch 276
- gewählter Klartext-Schlüsseltext-Angriff 20
- gewählter Schlüsseltext-Klartext-Angriff 20
- GF(2) 95
- Glasfaser 2, 53, 54, 156, 279
- gleichmäßiger Zeichenstrom 53, 55
- globale Sicht 210
- globale Überlagerung 176, 288
- globales überlagerndes Empfangen 98, 119, 125, 135, 200, 298
- grob 205
- Großer Bruder 51, 293
- Großstadtnetz 102
- Grundrecht 192
- Grundverfahren zum Schutz der Verkehrs- und Interessensdaten 111, 188, 193
- Gruppe
 - abelsche 92, 95
 - endliche 96
 - zyklische 95

- Hacker 290
- Häufigkeitsanalyse 31
- Haftfehler 258
- Hash-Funktion 86, 240
- HDTV 3, 54, 183
- Herkunftsadresse 59
- Hersteller 284
- heterogen 287
- heterogenes Kommunikationsnetz 189, 202, 209
- hidden channel 67
- Hierarchiegrenze 195, 202, 203, 209
 - statisch feste 196
- hierarchisch 115
- hierarchische Adresse 196, 199

- hierarchische Gliederung des Kommunikationsnetzes 187
 hierarchisches Kommunikationsnetz 195
 High Definition TV 3, 54
 hochauflösendes Fernsehen 3, 54, 56, 183, 191
 Höckel 181
 Hörfunk 1
 homogenes Kommunikationsnetz 189
 hybrides Konzelationssystem 302
- I-Kanal 156
 IBFN 2, 3, 4, 157
 ideal secrecy 42
 Identifikation 294
 identifizieren 290
 implizite Adresse 64, 110, 118, 135, 192, 194, 196, 199, 201, 218, 221, 277, 285, 296, 298
 implizite Adressierung 67, 111, 115, 116, 118
 indeterministisch verschlüsselnd 90
 indeterministische Blockchiffre 31
 indeterministisches Protokoll 260
 indirektes längentreues Umcodierungsschema 77, 162, 163
 indirektes Umcodierungsschema 71, 77, 82, 227, 233
 indirektes Umcodierungsschema für Empfängeranonymität 75
 individuelle Abrechnung 288
 Information 41
 informationelles Selbstbestimmungsrecht 300
 Informationsdienst 293
 Informationseinheit 112
 Informationsgehalt 42, 230
 Informationsgesellschaft 189
 Informationspluralismus 293
 informationstheoretisch 41, 100
 informationstheoretische Anonymität 99
 informationstheoretische Integrität 42
 informationstheoretische Konzelation 42
 informationstheoretische Modellwelt 41, 147, 269
 informationstheoretische Senderanonymität 70
 Inhaltsdaten 4, 190, 295
 injektiv 19
 Installation 284
 Integrated Services Digital Network 2
 Integriertes Breitbandfernmeldenetz 2, 3
 integriertes Text- und Datennetz 2
 Integrität 19, 42, 43, 53
 informationstheoretische 42
 perfekte informationstheoretische 42
 perfekte komplexitätstheoretische 43
 Interessensdaten 4, 54, 56, 57, 59, 61, 62, 115, 190, 192, 285, 295, 299
 invertierbar 19
 IS 8802/5 179
 ISDN 2, 6, 57, 76, 274
 ISO 52, 108
 Isolation 297
 I'm alive message 220, 243
- jitter 114
- K-Kanal 156
 Kabel 272
 Kabelfernsehen 1
 Kabelfernsehnetz 181
 Kabelkanal 183, 272, 279
 Kabelkeller 214
 Kabellänge 281
 Kabeltext 1
 Kabelverlegung 281
 Kanal 117, 119, 140, 147, 148, 159, 165, 183
 anonymer 87, 217, 278
 verborgener 7, 18, 67, 298
 virtueller 157, 159
 Kanalaufbau 87, 196
 Kanalnummer 116
 Kanalselektion 110, 111, 156
 Kanalvermittlung 55, 112, 116, 117, 118, 143, 170

- Katastrophe 214, 273, 275
- Katastrophenmodell 214
- Katastrophentoleranz 296
- Katastrophentoleranzverfahren 214
- key expansion 301
- Kindermord
 - bethlehemitischer 195
- Klartext 42
- Klartext-Schlüsseltext-Angriff 20
 - adaptiv gewählter 20
 - gewählter 20
- Klasseneinteilung 16, 187
- Kleeblatt-Ringe 205
- knapsack problem 46
- known-plaintext attack 20
- Koaxialkabel 53
- Koaxialkabelbaumnetz 182, 277, 278
- Körpereigenschaften 95
- körperliches Merkmal 294
- kohärente optische Nachrichtentechnik 156, 183
- Kollisionen verhindernder Schalter 107, 108, 182
- Kollisionen verhinderndes Baumnetz 107, 181
- Kollisionsauflösung 121, 123, 136, 298
- Kollisionsauflösungsalgorithmus 125, 127, 135, 140
- Kollisionsergebnis 93
- Kommunikation
 - anonyme 62
- Kommunikationsbeziehung 62, 73, 76, 77
- Kommunikationsleibwächter 290
- Kommunikationsnetz 1
 - asymmetrisches 191
 - heterogenes 189
 - hierarchisches 195
 - homogenes 189
 - öffentliches 1
- Kommunikationsnetzmodell 164, 165
- Kommunikationspartner 56, 57, 61
- komplexitätstheoretisch 41, 100
- komplexitätstheoretische Modellwelt 41
- Konferenzschaltung 119, 135, 141, 142, 143, 149, 173, 204
- kontinuierliche Chiffre 31
- Konzelation 19, 42, 53
 - informationstheoretische 42
 - perfekte informationstheoretische 42
 - perfekte komplexitätstheoretische 43
- Konzelations-Protokoll 65
- Konzelationssystem
 - asymmetrisches 230
 - perfektes komplexitätstheoretisches 44
 - hybrides 302
- Koordinations-Problem 222, 223, 227
- Koordinations-Protokoll 224, 226, 227, 228, 229, 233, 234, 235, 236, 238, 239, 240, 241, 244, 245, 252
- Kosten 280
- Kryptographie 19, 231
- kryptographisch stark 43
- Kryptosystem 19, 31
 - asymmetrisches 20, 41
 - deterministisches 76
 - symmetrisches 20, 75, 291
- Kubicek 17
- Kupferdoppelader 53
- Längentreue 79
- längentreues Umcodierungsschema 77, 78, 84
- Lampson 297
- Lebenssignal 220, 243
- Lee 142
- Leitung 53, 54
- Leitungstopologie 92
- Leuze 6
- link-by-link encryption 53
- lokale Auswahl 61
- lokale Sicht 210
- LUCIFER 46, 51
- MAN 102
- manipulationssicher 291, 292
- manipulationssicherer autonomer Zähler 292
- Mann 266

- Massenkommunikation 189
 Massenkommunikationsdienst 190
 Massey 123
 Maxi-Datensatz 294
 MDES 301
 Medium 110, 114
 Mehrfachfehler 190
 Mehrfachzugriff 93, 110, 115, 116, 298
 anonymer 111
 Mehrfachzugriffsprotokoll 199, 200, 205
 Mehrfachzugriffsverfahren 257, 267, 269
 asynchrones 298
 Mehrheit
 absolute 225, 226, 235, 240, 291
 Merkmal 15
 körperliches 294
 message switching 116
 Metropolitan Area Network 102
 Mini-Datensatz 294
 Mittelwertbildung 135
 Mittelwertvergleich 132, 173
 mittlerer MIX 87
 MIX 67, 70, 71, 72, 74, 77, 89, 114, 164,
 187, 223, 274, 275, 277, 278, 282
 MIX-Betreiber 193
 MIX-Kaskade 193, 197, 274, 275, 276,
 279
 MIX-Netz 67, 73, 110, 111, 114, 157,
 183, 192, 193, 194, 214, 219, 254,
 267, 269, 270, 271, 285, 286
 MIX-zu-MIX-Protokoll 220, 225
 MIX-zu-MIX-Verschlüsselung 240, 243,
 267, 270
 MIXe mit bedeutungslosen Zeitscheiben-
 kanälen und Verteilung der Gesprächs-
 wünsche 276, 277, 278, 285
 MIXe mit Reserve-MIXen 241, 244, 245,
 247, 250, 251, 252, 253, 271
 Modellwelt
 informationstheoretische 269
 modified DES 301
 modulo-Addierer 108, 175, 254, 257
 Modulus 88
 mögliche Aufdeckforderung 268
 Monomode-Glasfaser 156, 180, 183, 186
 multicast 91, 189, 195
 Multiplexbildung 180, 184, 186

n-anonym 144, 145
 schwach 144
n-identifizierbar 144
n-testbar 144
 partiell 144
 Nachbar 57
 Nachfolge von DES 50
 Nachricht 117, 119, 140, 147, 159, 165
 bedeutungslose 268
 Nachrichten(fragmente) 53
 nachrichtenbezogener aktiver Angriff 20
 nachrichtenbezogenes Brechen 25, 28, 46
 Nachrichteninhaltsteil 75, 80, 231
 Nachrichtenkombination 96, 97
 nachrichtentechnik
 kohärente optische 183
 Nachrichtenvermittlung 116, 117
 National Bureau of Standards 23, 45, 52
 National Security Agency 50
 NBS 23, 45, 52
 Nebengeräusch 141
 network layer 110
 Network Termination 284
 Netzabschluß 284, 285, 286, 287, 288, 289
 Netzanschluß 286
 Netzbetreiber 61, 284, 288
 Netzbetreiberschaft 283
 Netzinvestition 272
 Netzmanagement 283
 anarchisch-liberales 283
 nicht manipulierbarer Zähler 288
 nichtlinear gebildetes Prüfzeichen 121
 nichtlinearer Code 140
 Norm 57
 Normung 56, 57, 111
 Notruf 296
 NSA 50, 51, 52, 57
 NT 284
 Nutzdaten 4, 56, 59, 199, 273, 295, 299
 Nutzleistung 187, 252

- öffentliche Absenderadresse 76
- öffentliche Adresse 65, 74, 118, 192, 196
- öffentliche offene Adresse 66
- öffentlicher Anschluß 59
- öffentlicher mobiler Funk 214, 295
- öffentliches Kommunikationsnetz 1
- offene Adresse 66
- offene Adressierung 64, 65, 66
- offene implizite Adresse 118, 192, 282, 298
- offene implizite Adressierung 118, 219
- offenes System 57
- ω -anonym 144, 145
- ω -identifizierbar 144
- ω -testbar 144
- one time pad 42
- One-Time-Tapes 42
- one-way function 230
- Open Systems Interconnection 108
- optische Verstärkung 183, 191
- optischen Überlagerungsempfang 191
- optischer Überlagerungsempfang 181
- Ortsgespräch 275, 276
- Ortsnetz 279
- Ortsvermittlungsstelle 214, 274, 276, 277, 279, 281
- Ortsvermittlungstechnik 2
- OSI 108
- OSI Referenzmodell 111
- OSI Referenzmodell 108, 109
- output feedback 36

- paarweises überlagerndes Empfangen 98, 101, 108, 119, 135, 140, 141, 204, 298
- packet switching 116
- Paket 117, 119, 140, 147, 159, 165
- Paketvermittlung 116, 117, 172, 276
- PAL 54
- PAL Fernsehbild 47
- Parallel-Redundanz 225
- Parallel-Serien-System 245
- paralleler Ring 261
- partiell n -testbar 144
- partiell ω -testbar 144
- partielle Verteilung 91, 195
- partiell Brechen eines Kryptosystems 46
- Partitionierung 205
- passiver Angriff 20, 46
- pattern sensitive timing jitter 114
- Pauschale 289
- Pay-per-View-TV 190
- Peilung 295
- perfect secrecy 42
- perfekt anonym 15
- perfekt unbeobachtbar 15, 16, 53
- perfekt unverkettbar 15
- perfekte Anonymitätserhaltung 119
- perfekte informationstheoretische Anonymität 63, 119
- perfekte informationstheoretische Integrität 42, 99
- perfekte informationstheoretische Konzelation 42
- perfekte informationstheoretische Unbeobachtbarkeit des Empfangens 63
- perfekte informationstheoretische Unverkettbarkeit 63, 120
- perfekte komplexitätstheoretische Integrität 43
- perfekte komplexitätstheoretische Konzelation 43, 48
- perfekte komplexitätstheoretische symmetrische deterministische Blockchiffre 44
- perfekte Unverkettbarkeit 213
- perfekte Unverkettbarkeitserhaltung 120
- perfektes komplexitätstheoretisches asymmetrisches Konzelationssystem 44
- perfektes komplexitätstheoretisches Signatursystem 44
- Permutation 45, 46
- Permutationsbox 45, 301
- Persönlichkeitsbild 5, 61
- personenbezogene Information 191
- physical layer 109
- physische Unbeobachtbarkeit 114
- plaintext-ciphertext feedback 36
- Post
 - elektronische 170

- Postfach
 - elektronisches 1
- Priorität 155
- private Adresse 65, 66, 118
- private implizite Adresse 116
- private offene Adresse 66
- Produktion 284
- PROMETHEUS 296
- Protokoll
 - asymmetrisches 260
- Protokollumsetzer 199, 201, 206, 208, 260, 266
- Prüfzeichen 257
 - nichtlinear gebildetes 121
- Pseudonym 112
- pseudozufällig 31
- Pseudozufallsbitfolge 43
- Pseudozufallsbitfolgengenerator 43, 44, 48, 100
- Pseudozufallszahl 105
- Pseudozufallszahlengenerator 175, 254, 278
- Puffer
 - elastischer 180, 182
- Punkt-zu-Punkt-Duplex-Kanal 98, 101, 103
- Punkt-zu-Punkt-Leitung 269
- Punkt-zu-Punkt-Leitungen 53
- PZG 254, 257, 258, 259, 267

- R-ALOHA 121, 136
- R-CSMA 121
- Rahmen 137
- Randell 297
- Rauschen 141
- Realisierbarkeit
 - technisch-ökonomische 272
- Realzeitanforderung 87
- Rechner des Netzbetreibers 56
- Recht auf informationelle Selbstbestimmung 57
- Rechtssicherheit 57, 291
- recovery point 257
- Redundanz 42, 230, 243
 - dynamisch aktivierte 221
 - dynamisch erzeugte 223
 - statisch aktivierte 222
 - statisch erzeugte 223
- Redundanzprädikat 88, 90
- Redundanzreduktion 54
- Redundanzverengung 266
- Referenzuhr 180
- Reidentifikation 294
- reliability 244
- Reproduktionskosten 203
- Reserve-MIX 225, 226, 227, 245
- Reservierung 137
- Reservierungskanal 173
- Reservierungsschema 121, 137
- Reservierungstechnik 93
- Reservierungsverfahren 138, 267
- Restklassenring 88
- Richtfunkstrecken 53
- Ring 92, 100, 106, 111, 186, 270
 - geflochtener 261, 264
- Ring mit umlaufendem Senderecht 147, 148
- Ring mit umlaufenden Übertragungsrahmen 147, 148
- RING-2-b-Empfangsprotokoll 151
- RING-2-b-Sendeprotokoll 151, 152, 153
- RING-2-f-Netz 104, 105, 108, 110, 119, 120, 150, 199, 264, 288
- RING-Netz 101, 102, 107, 110, 111, 114, 116, 142, 146, 148, 149, 178, 179, 182, 186, 191, 193, 195, 198, 199, 201, 205, 259, 261, 262, 265, 266, 267, 269, 270, 271, 279, 281, 282, 286, 287, 288, 299
 - dynamisch partitionierbares 206
- Ring-Verkabelungs-Konzentrator 261
- RING- ν DC-/Verteilnetz 202
- Ringrekonfigurierung 260, 261
- Ringstruktur 95
- Ringzugriffsverfahren 143, 154
- Roberts' scheme 121, 137
- Rolf 17
- Rolle 15
- ROM 18
- Routing 205
- routing 110

- RSA 25, 46, 48, 49, 88, 89, 230, 292, 294
- RSA Implementierung 49
- Rucksackproblem 46
- Rückadresse 75, 90, 194, 244
 - anonyme 75, 86, 219, 221
 - mit langer Gültigkeit 86, 221
 - fehlertolerante anonyme 231
- Rückadreßteil 75, 76, 231, 232
- rückgekoppeltes Schieberegister 46
- Rückmeldung
 - ternäre 125
- Rücksetzpunkt 257
- Rundfunksendernetz 1
- Rushby 297

- Sabotage 183
- Sabotageakt 214
- Satellitenstrecke 53
- Schalten anonymer Kanäle 276
- Schalten von Kanälen 243
- Schichtenmodell 108
- Schieberegister 46, 194
 - nichtlinear rückgekoppeltes 194
 - rückgekoppeltes 46
- Schlüssel 19
- Schlüssel zum Testen 44
- Schlüsselaustausch 56, 66, 70, 302
- Schlüsselaustauschgraph 105, 258
- schlüsselbezogener aktiver Angriff 20
- schlüsselbezogenes Brechen 46
- Schlüsselexpansion 301
- Schlüsselgenerierung 45, 48
- Schlüsselgenerierungsalgorithmus 50, 51
- Schlüsselkombination 96, 97
- Schlüssellänge 46
- Schlüsseltext 42
- Schlüsseltext- und Ergebnisrückführung 40
- Schlüsseltext-Angriff 20
- Schlüsseltext-Klartext-Angriff
 - adaptiv gewählter 20
 - gewählter 20
- Schlüsseltextrückführung 34, 35
- Schlüsseltopologie 204
- schmalbandig 1
 - schmalbandiges ISDN 274
 - Schneider 65, 99
 - Schub 68, 71, 86, 89, 243, 245
 - Schubgröße 89
 - Schutz 189
 - Schutz der Kommunikationsbeziehung 67, 187, 192, 194, 274, 276
 - Schutz des Empfängers 63, 86, 114, 189, 190, 194, 221, 277
 - Schutz des Senders 90, 189, 194, 298, 299
 - schwach koordinierte MIXe 252
 - schwach n -anonym 144, 145
 - schwache Koordinierung 243
 - Schwellwertschema 218, 225, 226, 227
 - SCSI-Festplatte 47
 - secrecy
 - ideal 42
 - perfect 42
 - security 244
 - seed 43
 - Selbstbestimmungsrecht
 - informationelles 300
 - Selbstdiagnose 257
 - Selbstidentifikation 299
 - selbstsynchronisierende Stromchiffre 32, 33, 35, 54, 82, 158, 160, 161, 218
 - self-synchronous stream cipher 32
 - Sendeereignis 112
 - Senden durch Ersetzen 106, 142, 146, 149, 154
 - Senden durch Überlagern 106, 149
 - Senderanonymität 92, 95, 136
 - informationstheoretische 70
 - Senderanonymitätsschema 74
 - Senderechtszeichen 148, 193, 260
 - Senderechtszeichen mit umlaufzeitabhängiger Nutzungsbegrenzung 155
 - senderpartitioniertes DC-Netz 254, 255, 271
 - Sensitivität 189, 191, 192
 - Sensitivitätsklasse 192
 - Sequenznummer 178, 217
 - Serien-Parallel-System 245
 - Seriensysteme im Sinne der Zuverlässigkeit 210

- Shannon 41, 45, 97
- sicheres Gerät 41
- Sicherheit 3, 18, 41, 244, 245
- Sicherheitsmodell 244
- Sicherheitsparameter 41
- Sicherheitsproblem 16, 273
- Sicherungsschicht 110
- Signalisierungskanal 118, 276, 277, 278
- Signalregenerierung
 - digitale 92, 101, 102, 110, 114, 182, 183, 259, 264, 286
- Signatursystem 20, 44, 48, 291, 292, 294
 - perfektes komplexitätstheoretisches 44
- Signierschlüssel 41
- simplex channel 159
- Simplex-Kanal 149, 159, 160, 161, 244
- slotted ALOHA 93, 121, 123, 136
- slotted ring 147
- Softwareschutz 293
- Speicherprogrammierbarkeit
 - freie 197
- splitting algorithm 121, 123
- sporadisches Fehlerauftreten 213
- Spracherkennung 300
- Sprechererkennung 300
- Stärke eines Angreifers 15
- Standard 57
- Standardisierung 56, 57
- Startwert 43, 48, 267
- statisch erzeugte Redundanz 221, 223
- statisch feste Hierarchiegrenze 196, 197
- statistische Erhebung 294
- Stern 186
- stochastisches Modell 244
- Störer 268
- stream cipher 31
 - self-synchronous 32
 - synchronous 32
- Stromchiffre 31, 53, 55, 117, 157, 218
 - asymmetrische 33, 38
 - asymmetrische synchrone 38
 - asynchrone 82
 - selbstsynchronisierende 32, 33, 35, 54, 158, 160, 161
 - symmetrische 34, 36
 - synchrone 32, 37, 39, 82, 158, 161
- Stromsystem 31
- stuck at 258
- sublayer 110
- Substitutionsbox 45, 46, 302
- symmetrische Stromchiffre 34, 36
- symmetrisches Kryptosystem 20, 54, 291
- synchrone Stromchiffre 32, 37, 39, 42, 82, 158, 161, 218
- Synchronisation 32, 177, 257, 278
- Synchronität 298
- synchronous stream cipher 32
- Szenario 165
- Taktverschiebung
 - zeichenfolgensensitive 114
- tamper responding container 18
- TASI 112
- tatsächliche Aufdeckforderung 268
- TDM 156
- TE 284
- Team 224, 225, 226, 227, 236, 241
- technisch-ökonomische Realisierbarkeit 272
- teilnehmerüberprüfbarer Datenschutz 272, 281
- Teilnehmeranschluß 272
- Teilnehmeranschlußbereich 1, 18, 189, 191
- Teilnehmerendgerät 284, 285, 289
- Teilnehmerstation 283, 284, 285
- Teilschicht 110
- Teilungsalgorithmus 125
- TELEBOX 1
- TELEFAX 1
- Telefonbuch 65
- Telefongespräch 166, 172
- Telefonzelle 59, 60, 273
- Telekommunikationsordnung 7
- TELETEX 1
- Teletransaktion 291
- TELEX 1
- TEMEX 1, 297
- TEMPEST 10
- Terminal Equipment 284

- ternäre Rückmeldung 121, 125
- time assignment speech interpolation 112
- time division multiplexing 156
- timed token access 155
- timed token rotation protocol 155
- timing jitter 114
 - bit pattern sensitive 180
- TKO 7, 16
- TNIU 297
- token ring 147
- Topologie 176, 299
- Transaktionsnummer 116
- transitives Trojanisches Pferd 8, 17
- transport layer 109
- Transportschicht 109, 114
- trap 268
- Treuhänder
 - aktiver 293
- Trojanisches Pferd 7, 8, 9, 17, 67, 187, 197, 201, 273, 274, 283, 284, 285, 286, 287, 297
 - transitives 8
- Trustworthy Network Interface Unit 297

- Überflutung 110
- Überlagern 93
- überlagerndes Empfangen 95, 106, 108
 - globales 98, 119, 125, 135, 200, 298
 - paarweises 98, 101, 108, 119, 135, 140, 141, 298
- überlagerndes Senden 92, 93, 102, 108, 114, 136, 195, 199, 264, 278
 - binäres 93, 95
 - verallgemeinertes 92, 95, 137
- Überlagerung 136, 141
- Überlagerungs-Kollision 93, 95, 97, 98
- Überlagerungsempfang
 - optischer 156, 181, 191
- Überlagerungstopologie 108, 176, 177, 185, 204
- Überlagerungszeit 186
- Überlebenswahrscheinlichkeit 244
- Übermittlungszeit 166
- überprüfbarer Datenschutz 57, 192

- Übertragungs-Kollision 93
- Übertragungsaufwand 238
- Übertragungsfehlern 110
- Übertragungsleitung 183
- Übertragungsmodus
 - asynchroner 117
- Übertragungsrahmen 148, 181, 193, 199, 260
- Übertragungsstrecke 53, 57
- Übertragungstopologie 108, 176, 177, 184, 185, 204, 259, 264, 287
- Übertragungszeit 186
- ÜR 199
- Uhrzeit 243
- umcodierender MIX 67
- Umcodierungsschema 70, 71
 - direktes 71, 89
 - indirektes 71, 82, 89, 227
 - indirektes längentreues 162, 163
 - längentreues 77, 78, 84
- Umcodierungsschema für Empfängeranonymität 76, 77, 80, 81, 84
- Umcodierungsschema für Senderanonymität 74, 76, 77, 79, 80, 84
- unbeobachtbar 14, 15, 16
- Unbeobachtbarkeit 16, 112, 210, 213, 220, 254, 292, 299
 - Grad an 16
- Unbeobachtbarkeit angrenzender Leitungen und Stationen 110
- unbeteiligte Dritte Partei 20
- unmanipulierbares Gehäuse 18, 51
- Unterschrift 44
 - digitale 19
- untraceable return address 75
- unverkettbar 14, 15
- Unverkettbarkeit 16, 110, 111, 112, 114, 115, 156, 183, 210, 212, 220, 254, 292, 299
- Unverkettbarkeitserhaltung 111, 119
 - perfekte 120
- Urheberrechtsproblem 293

- V-Kanal 156

- Varianz der Nutzungszeit 159
- verallgemeinertes überlagerndes Senden 92, 95, 137
- Verallgemeinerungen von DES 301
- Verbindung 159
- Verbindungs-Verschlüsselung 53, 54, 55, 56, 57, 58, 101, 108, 109, 145, 218, 270
 - virtuelle 74, 77, 86
- Verbindungsadresse 118
- Verbindungsaufbauzeit 166
- Verbindungsdaten 7
- verbindungsorientiert 117
- Verbindungswunsch 159
- verborgener Kanal 7, 18, 67, 298
- verdeckte Adressierung 64, 65, 66
- verdeckte explizite Adressierung 196
- verdeckte implizite Adressierung 118, 219
- Verfahren zum anonymen Mehrfachzugriff 259
- Verfügbarkeit 244
- Verhinderung der Dienstbringung 243
- Verkehr
 - büschelweise auftretender 157
- Verkehrsanalyse 191
- Verkehrscharakteristik 192
- Verkehrsdaten 5, 56, 57, 62, 115, 190, 192, 199, 285, 295, 299
- Verkehrereignis 14
- Verkehrsklasse 115
- Verkehrsklassen 187, 189
 - verschieden geschützte 187
- Verkehrslast 166
- Verkehrsleitsystem 296
- verkettbar 64
- Verkettung 61, 117, 213
- Verkettungsangriff
 - aktiver 112
- Verkettungsangriff über Betriebsmittelknappheit 112
- Verklemmung 161
- Vermittlung
 - büschelweise 117
- Vermittlungs-/DC-Netz 207
- Vermittlungs-/Verteilnetz 195, 197, 198, 199, 200, 266, 278, 279
- Vermittlungsart 117
- Vermittlungsdaten 4, 5, 56, 59, 62, 295, 297
- Vermittlungsnetz 1, 2, 57, 142, 197, 300
- Vermittlungsschicht 110, 114
- Vermittlungsstellen 272
- Vermittlungszentrale 16, 18, 56, 57, 58, 108, 273, 285
- VermittlungsvMIX-/Verteilnetz 202
- Vernam 42
- Vernam-Chiffre 42, 47, 48
- verschieden geschützte Verkehrsklassen 187
- Verschiedene MIX-Folgen 244, 245, 247, 248, 250, 252
- Verschlüsselung 19, 53, 57, 114, 217, 273
- Verschlüsselungsleistung 47
- Verstärker 272
- Verstärkung
 - optische 183, 191
- versteckte Automorphismen 147
- Verteil-/Verteilnetz 200, 201, 208
- Verteil-Simplex-Kanal 98
- Verteilnetz 1, 2, 183, 197, 209, 269, 279
- Verteilnetzzentrale 199
- verteilt und anonymes Abfragen 147, 150
- Verteilung 63, 64, 67, 86, 90, 110, 111, 114, 116, 147, 156, 183, 187, 192, 194, 218, 221, 277, 285, 298
- Verteilvermittlung 157
- vertrauenswürdige Netzschnittstelle 297
- Vertrauenswürdigkeit 16
- vertraulich 4
- Vertreter 226, 227
- Verzögerung 276
- Verzögerungszeit 125, 141, 173, 178, 184, 189, 195, 238, 252
- Videokonferenznetz 2
- Videotext 1
- virtual circuit 157
- virtuelle Verbindungs-Verschlüsselung 74, 77, 85, 86, 114
- virtueller Kanal 157, 159

- virtueller Ring 270
- Virus-Eigenschaft 17
- Visitenkarte 47
- Volkszählungsurteil 300
- Volladdierer 174
- vollständige Verteilung 91

- Wahlwiederholung 277, 278
- WANGNET 182
- wavelength division multiplexing 156
- WDM 156, 181
- Wegeermittlung 110, 114
- Wellenlängenmultiplex 156, 181, 183

- X.25 284
- XOR 42, 47

- Yacobi 142

- Z-80-Prozessor 49
- Zähler
 - nicht manipulierbarer 288
- Zahlungssystem
 - anonymes digitales 288
 - digitales 291
- Zahlungssystembetreiber 291, 292
- Zeichen 31
- zeichenfolgensensitive Taktverschiebung 114
- Zeichenkette 71
- Zeichenstrom
 - gleichmäßiger 53
- Zeitintervall 68
- Zeitintervallverfahren 125
- zeitlich entkoppelte Verarbeitung 60, 125
- Zeitmultiplex 156, 181
- Zeitscheibenkanal
 - bedeutungsloser 276
- Zeitschranke 220, 222
- Zeitstempel 85, 103, 178, 217
- Zeitung 293
- Zellularfunksystem 296
- zentralistische Ansatz 16
- Zentralstelle für das Chiffrierwesen 51
- Zeuge 16, 19
- ZfCh 51, 52, 57
- Zieladresse 59
- zufällige Bitkette 88, 90
- Zufallszahl 48
 - echte 31
 - pseudozufällige 31
- Zugriffsverfahren 93, 99, 101
- zusammenhängend 95, 96
- Zuverlässigkeit 244, 245, 246
- Zuverlässigkeitsengpaß 266
- Zweckbindungsgebot 294
- Zwei-Phasen-Konzept 221
- Zwischenregenerator 5
- zyklische Gruppe 95