

Tárgymutató

- adaptív kód, 51
 ADPCM, 106, 115
 ADSL, 134
 a posteriori valószínűség, 153
 a priori valószínűség, 153
 aritmetikai kódolás, 29, 129, 133
 ARJ, 52
 ARQ, 223
 átlagos kódszóhossz, 14
 betűnkénti, 21
 átviteli függvény, 92

 Bayes-döntés, 154, 168
 bázis, 189
 BCH-kód, 197, 231
 becslés, 152
 belső kód, 241
 beszéd-tömörítés, 115
 betűnkénti hűségkritérium, 142
 betűnkénti torzítás, 141
 Bhattacharyya
 felső becslés, 291
 távolság, 276
 bináris entrópiafüggvény, 44, 61
 bináris szimmetrikus csatorna,
 → BSC
 bináris törléses csatorna, 165
 bináris véletlen átkulcsolás,
 → one-time-pad
 bináris z-csatorna, 164
 bitallokáció, 99
 blokkhossz, 259

 blokk-kód, 19, 182
 BSC, 155, 164, 270

 Caesar-titkosító, 315
 CBC, 346, 348
 CD, 211
 CD-minőségű hang, 119
 CDMA, 278
 frekvenciaugratásos, FH, 278
 időugratásos, TH, 278
 közvetlen sorozatú, DS, 278
 rádiótelefonía, 284
 CELP, 118
 ciklikus eltolás, 217
 ciklikus kód, 217
 ciklikus konvolúció, 252
 COMPRESS, 56
 CRC, 223, 231, 347
 csatornkapacitás, 165, 320
 csatornakód, 167
 csatornakódolási tétel, 172
 megfordítása, 170
 csomós hibázás, 212, 237

 DAT, 211
 DBS, 197
 DCT, 100, 121, 131
 dekódolás, 167, 183
 delta moduláció, 108
 DES, 357
 digitális aláírás, 323
 digitális moduláció, 159

- Dirichlet-partíció, 89
 diszkrét korrelációs detektor, 162
 diszkrét memóriamentes csatorna,
 → DMC
 DMC, 50, 164, 271, 272
 döntés, 152
 döntési tartomány, 153
 DPCM, 105
 DST, 100
 DWHT, 100
- ECB, 348
 egyértelmű dekódolhatóság,
 11, 13, 17
 egyirányú függvény, 332
 egyszerű hibázás, 182, 186
 elem rendje, 200
 entrópia, 14, 31
 feltételes, 33, 34
 ε -hibával dekódolhatóság, 65
 euklidészi algoritmus, 325
 euklidészi osztás polinomokra, 204
- fa-kód, 259
 Fano-egyenlőtlenség, 170
 fax-szabványok, 44
 Fermat-tanú, 334
 Fermat-tétel, 328
 Fleischer-tétel, 83
 folytonos tónusú tárolás, 125
 formáns beszédkódoló, 116
 forrásábécé, 10, 182
 forrásentrópia, 38
 forráskódolási tétel, 147
 megfordítása, 146
 Fourier-transzformáció, 91, 95,
 116, 120, 126, 250
 főpolinom, 216
 FSK, 159, 281
 futamhossz kódolás, 44, 132
- G.711, 115
 G.721, 115
 generátormátrix, 190, 202
 generátorpolinom, 219
 GIF, 56, 127
 globális kockázat, 152
 Golay-kód, 197, 226
 GSM, 119, 279
- Hamming-kód, 232
 bináris, 195
 nembináris, 202
 Hamming-korlát, 187
 Hamming-korreláció, 280
 Hamming-távolság, 156, 182, 271
 Hamming-torzítás, 141, 147
 HDTV, 135
 hibacsomó, 224, 237
 hibahelylokátor, 244
 hibahelypolinom, 245
 hibajavítás, 186
 hibajelzés, 185
 hibavalószínűség, 153
 hibavektor, 194
 hitelesség, 318
 Hölder-egyenlőtlenség, 86
 Huffman-kód, 23, 45, 60
 adaptív, 25
- indexelt tárolás, 126
 információforrás, 36
 emlékezetnélküli, 37
 memóriamentes, 37
 stacionárius, 37
 ergodik, 37
 információs divergencia, 59
 információstabilitás, 67
 irreducibilis polinom, 214
- javítható hibaminta, 195
 Jayant-kvantáló, 106

- jelsebesség,
→ kódolási sebesség
- Jensen-egyenlőtlenség, 15
- JPEG, 100, 128
- kaszvád kód, 241
- katasztrofális kód, 264
- kényszerhossz, 258
- kínai maradéktétel, 240, 336, 358
- kompanderes kvantáló, 83, 115
- konvolúciós kód, 259, 288
 állapotátmenet gráf, 261
 bináris fa reprezentáció, 260
 szuperortogonális, 289
 trellis reprezentáció, 261
- kód, 10, 182
- kódábécé, 10, 182
- kódátfűzés, 212, 236, 288
- kódolás, 167, 182
- kódolási nyereség, 267
- kódolási sebesség, 70, 142, 169, 234, 258
- kódosztásos többszörös hozzáférés,
→ CDMA
- kódsebesség,
→ kódolási sebesség
- kódszó, 10, 182
- kódszókeret, 258
- kódszópolinom, 218
- kódtávolság, 185
- konvolúciós tétel, 251
- kovarianciafüggvény, 91, 111, 162
- kölcsönös információ, 139, 319
- költségfüggvény, 152
- közelítő hálózati videozás, 134
- Kraft-egyenlőtlenség, 12, 57
- kriptoanalízis, 313
- kriptográfia, 313
- kriptográfiai ellenőrző összeg,
→ MAC
- kriptográfiai protokoll, 319, 337
 digitális aláírás, 349
- kulcskiosztás, 341
 konvencionális, 342
 nyilvános kulcsú, 344
- partnerhitelesítés
 jelszavas, 338
 kihívás és válaszvárás, 340
- titok megosztása, 354
- üzenethitelesítés, 346
 digitális aláírás, 348
 hash függvény, 348
 MAC, 346
 rejtjelezés, 347
- krominancia-együttható, 125
- kulcs, 314
- Kullback-Leibler-távolság, 59
- különbségi kódolás, 103
- külső kód, 241
- kvantáló, 72
 egyenletes, 75
 entrópiája, 78
 torzítása, 75
 vektorkvantáló, 87, 98, 116, 126, 142
- láncszabály, 34
- legközelebbi szomszéd feltétel, 81
- Lempel–Ziv-kódok, 51
- léptetőregiszteres kódoló, 258
- LFSR, 228, 255
- Linde–Buzo–Gray-algoritmus, 89
- lineáris becslés, 110
- lineáris függetlenség, 189
- lineáris kód, 188, 202
- lineáris prediktív kódolás, 116
- lineáris prediktorfüggvény, 111
- lineáris szűrés, 92
- Lloyd–Max-algoritmus, 81
- Lloyd–Max-feltétel, 82

- LPC, 116
 luminancia-együtthető, 125
 LZ77, 51
 LZ78, 53, 62
 LZW, 54, 127
- MAC, 346
 Markov-forrás, 47
 Markov-lánc, 41
 homogén, 41
 stacionárius, 41
 maximális távolságú kód,
 → MDS kód
 maximum-likelihood
 dekódolás, 156, 180, 270
 döntés, 155
 McMillan-egyenlőtlenség, 12
 MDC, 347
 MDS kód, 187
 megszemélyesítés, 318
 minimális súly, 193
 mintavételezés, 93
 mintavételi idő, 93
 mintavételi tétel, 94
 modulo p aritmetika, 199
 MPE, 118
 MPEG, 100, 120, 133
 legális bitfolyam, 135
- négyzetes torzítás, 72, 88, 142
- nyílt üzenet, 314
- one-time-pad, 287, 316, 320, 321
- PAM, 159
 paritásellenőrző mátrix, 191
 paritásellenőrző polinom, 222
 paritáskód
 egydimenziós, 177, 185, 197,
 242
 kétdimenziós, 240
 paritásmátrix, 191, 202
 paritásszegmens, 190
 PCM, 114
 perfekt kód, 188
 Peterson–Gorenstein–Zierler-
 dekódoló, 247
 PKZIP, 52
 polinom, 204
 prediktív kódolás, 103
 prediktor, 105
 prefix kód, 11, 13
 primitív elem, 201
 PSK, 159, 267
- R–D függvény, 143
 redundancia, 190
 Reed–Solomon-kód, 208, 222, 232,
 243, 250, 354
 Reiger-optimális, 238
 részsávós kódolás, 101
 (R, G, B) színkoordináták, 125
 rövidítés, 224, 242
 RPE, 119
 RSA-algoritmus, 329, 340
- salting, 359
 sávszűrő, 92
 Shannon–Fano-kód, 18, 60
 shiftregiszter, 227
 Singleton-korlát, 186
 spektrális sűrűségfüggvény, 91
 spektrum, 250
 spektrumpolinom, 252
 standard elrendezési táblázat, 194
 súly, 193
 súlyfüggvény, 92
 súlypont feltétel, 82
- szabad távolság, 266
 szindróma, 193

- szindróma dekódolás, 194
szinuszos beszédkódoló, 117
szisztematikus generálás, 220
szisztematikus kód, 190
szorzatkód, 238
- táblázatos dekódolás, 183, 195
támadás
 aktív, 318
 ismert nyílt szövegű, 317
 passzív, 317
 rejtett szövegű, 317
 választható nyílt szövegű, 317
 választható szövegű, 318
támadó, 316
támadó közepén támadás, 344
távolságprofil, 266
telefon-minőségű hang, 114
teletext, 197
test, 197
testvérpár tulajdonság, 26
titkosítás, 318
 konvencionális, 316
 nyilvános kulcsú, 319, 322
 rejtett kulcsú, 316
titkosítási algoritmus, 319
titkosított üzenet, 314
titkosság
 feltétel nélküli, 322, 333
 gyakorlati, 322, 333
Toeplitz-lemma, 39
torzítási mérték, 141
tökéletes titkosítás, 319
törléses hiba, 186
transzformációs kódolás, 98, 120,
 253
trellis-kód, 259
túlélő, 271
- Ungerboeck-kód, 266
- üzenet, 10, 182
üzenetkeret, 258
üzenetmódosítás, 318
üzenetszegmens, 190
- V.32bis, 270
V.42bis, 56
változó szóhosszúságú kódolás, 11
véges test, 199
Vernam-titkosító,
 → one-time-pad
Viterbi-algoritmus, 271
Voronoi-tartomány, 89
- Walsh–Hadamard-
 kód, 285
 transzformáció, 100
Wiener–Hopf-egyenletrendszer, 112
- (Y, C_b, C_r) séma, 125