

ΕΥΡΕΤΗΡΙΟ

Αγγλικοί όροι

A

absolute rate, 73
adjudicated protocols, 314
Advanced Encryption Standard, AES, 196
anonymity of spending, 302
arbitrated protocols, 314
arbitrator, 305
attack
 adaptive chosen-ciphertext, 11
 adaptive chosen-plaintext, 11
 chosen-ciphertext, 11
 chosen-plaintext, 11
 ciphertext-only, 10
 exhaustive search, 11, 14
 known-key, 248
 man in the middle, 8
authentication, 9, 258
autocorrelation test, 113

B

bent functions, 144
Berlekamp, 120, 122
Biham, 169, 179, 182
bijection, 143
binary encoding, 63
birthday paradox, 127
bit commitment protocols, 317
bit length, 64
Burrows, Abadi & Needham, BAN, 314

C

Certificate Practice Statement, 273
certificate repository, 273
certificate revocation lists, 282
certificate revocation service, 273
Certification Authority, 272
chaining variables, 139
challenge-response, 253
Chaum, 304
cipher, 158
cipher block chaining, CBC, 158
cipher feedback, CFB, 158
ciphertext, 10
complexity profile, 122
conditional probability, 68
confidentiality, 9
Coppersmith, 188
cross-certification, 274

D

Data Encryption Standard, DES, 183
dictionary attack, 261
Diffie, 212, 220, 264, 265, 266, 267, 268
Digital Signature Algorithm, 300
Digital Signature Standard, DSS, 300
directory service, 273
distinguished name, 279

E

electronic codebook, ECB, 158
 ElGamal, 298, 301
 elliptic curve
 supersingular, 241
 encoding, 3
 Euler, 30, 50, 58, 59, 62, 221, 225
 exclusive OR, XOR, 75
 exhaustive search, 11, 14

F

Feistel, 141, 143, 146, 147, 148, 151, 152,
 181, 183, 184, 186, 196
 Fermat, 58, 62, 223, 224
 finite state machine, 115
 frequency test, 112

G

Geffe, 202, 203
 generator, 34, 108
 Golomb, 114, 117
 Guillou - Quisquater, 335, 336

H

hash function, 125, 126, 127, 128, 162, 257,
 267
 collision resistance, 126
 one-way, 126
 Hill, 81, 96, 97, 99, 100, 109, 123

I

index of coincidence, 91
 integrity, 9
 Interactive Proof, 331
 interlock protocol, 331
 irreducible polynomial, 46, 117

J

joint probability, 67

K

Kasiski, 91, 93
 Kerchoff, 11, 100, 104, 196, 245

key, 107, 108, 199, 200, 248, 249, 251, 256,
 258, 264, 271, 278
 master, 246
 session, 246
 short term, 247
 terminal, 246
 key derivation protocols, 256
 Key Distribution Centre, KDC, 248
 key establishment protocols, 248
 Key Translation Centre, KTC, 248
 knapsack, 214, 216, 220
 Koblitz, 230

L

Lagrange, 33, 35
 linear complexity, 119
 linear feedback shift register, LFSR, 116
 Lucifer, 184

M

Massey, 120, 122
 meet in the middle, 170
 mental poker, 315
 Merkle, 217, 218, 219
 Message Authentication Code, MAC, 129
 Miller, 230
 mixing transformations, 141
 modes of operation, 158
 Modification Detection Code, MDC, 129

N

NIST, 140, 196, 239, 300
 nonce, 253
 non-repudiation, 9
 of destination, 9
 of origin, 9

O

oblivious transfer, 321
 one pass protocol, 253
 online certificate status protocol, OCSP, 282
 oracle, 151
 output feedback, OFB, 158

P

perfect backward secrecy, 248

perfect forward secrecy, 248
 perfect secrecy, 71
 permuted choice, 190
 Personal Security Environment, 280
 piling-up lemma, 174
 plaintext, 10
 Pretty Good Privacy, 276
 primitive root, 59
 Principal, 272
 protocol failure, 3, 313
 Public key certificate, 273

R

randomization process, 229
 RC4, 207, 208
 recovery exponent, 227
 redundancy, 73
 Registration Authority, 272
 ring, 37
 Rivest, 2, 138, 220, 315, 331
 Rivest, Shamir, Adleman, RSA, 220
 RSA Laboratories, 192

S

S/Key, 328, 329
 salting, 328
 Schnorr, 336, 337
 Secure Hash Algorithm, SHA, 140
 security

- complexity theoretic, 14
- computational, 13
- provable, 14
- unconditional, 13, 313

 self enforcing protocols, 314
 self recovery, 290
 serial test, 113
 Shamir, 179, 182, 219, 220, 262, 263, 266,
 315, 331, 333, 334, 335, 336
 Shannon, 12, 13, 67, 68, 72, 74, 95, 106, 141,
 143, 158, 163
 shift register, 115
 strict avalanche criterion, 143
 substitution, 80, 142
 substitution boxes, 142
 Substitution Permutation Networks, SPNs,
 141

T

timestamp, 253

transposition, 80
 trapdoor, 192

U

unicity distance, 73, 74

V

Vernam, 93, 95, 166
 Vigenère, 87, 88, 89, 93, 94, 132, 201

W

web of trust, 275
 whitening, 146

Z

zero knowledge protocols, 331

Ελληνικοί όροι

A

- αβεβαιότητα, 68, 70, 71, 74, 325
 από κοινού, 69
 υπό συνθήκη, 69
 αδύναμα κλειδιά, 195
 ακέραια περιοχή, 39, 41
 ακέραιος Blum, 205
 ακεραιότητα, 9
 ακολουθία, 16, 34, 35, 36, 57, 60, 61, 63, 76, 89, 90, 94, 107, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 125, 140, 153, 157, 164, 166, 167, 186, 199, 201, 203, 206, 207, 215, 216, 217, 218, 219, γνησίως αυξουσα, 215, 217
 διαδρομή, 114
 πραγματικά τυχαία, 112
 ρολογιού, 203
 υπεραύξουσα, 215
 ψευδοτυχαία, 111, 112
 γεννήτριες, 115
 αλατισμός, 328
 αλγόριθμος
 Berlekamp και Massey, 120
 επαναλαμβανόμενου τετραγωνισμού - και - πολλαπλασιασμού, 64, 222, 240
 του Ευκλείδη, 23, 24, 25, 35, 53, 224
 αμοιβαία πληροφορία, 70
 αναγνώριση, 324
 αναγνώριση εκτός ζώνης, 276
 ανάγωγο πολυώνυμο, 46, 48, 49, 50, 66, 117, 119, 198
 αναδιάταξη, 80, 81, 144, 219, 315
 ανάκληση πιστοποιητικού, 273, 283
 αντικατάσταση, 80, 81, 86, 87, 96, 102, 141, 144, 247
 μονοαλφαβητική, 80, 82, 86, 104
 πολυαλφαβητική, 80, 86, 87
 αντίπαλος, 2, 3, 8, 10, 11, 83, 85, 99, 123, 150, 153, 154, 181, 212, 213, 227, 229, 243, 247, 251, 262, 263, 264, 265, 266, 270, 274, 281, 297, 299, 306, 312, 313, 330, 338
 πλεονέκτημα, 150
 ανωνυμία ξοδέματος, 302
 απλό κείμενο, 3
 από κοινού πιθανότητα, 67, 69
 Αποθήκη πιστοποιητικών, 273
 αποκρυπτογράφηση, 3
 Αρχή Εγγραφής, 272, 276, 280
 Αρχή Πιστοποίησης, 272, 273, 274, 275, 276, 277, 278, 279, 280, 282, 283, 337
 ασφάλεια
 άνευ όρων, 13, 70, 71, 73, 76, 87, 94, 95, 270, 313
 αποδείξιμη, 14, 146, 148, 152, 313
 θεωρητική πολυπλοκότητα, 14
 υπολογιστική, 13
 Ασφαλές Προσωπικό Περιβάλλον, 280
 ασφαλής πρώτος, 228
 αυθεντικοποίηση, 9, 129, 134, 286, 287, 326, 327, 329
 Fiat και Shamir, 333
 Guillou και Quisquater, 335, 336
 S/Key, 328, 329
 Schnorr, 336
 αμοιβαία, 330
 απλού κειμένου, 134
 κρυπτοκειμένου, 134
 ταυτότητας, 324
 αυτοεπιβαλλόμενα πρωτόκολλα, 314
- ### Γ
- γεννήτορας, 34, 50, 59, 207, 228, 237, 266, 298, 301, 318
 γεννήτρια Blum Micali, 206
 γεννήτρια Blum, Blum και Shub, 204
 γεννήτρια Geffe, 202, 203
 γεννήτρια εναλλασσομένου βήματος, 203, 204
 γεννήτρια καταφλίου, 203
 γραμμική κρυπτανάλυση, 144, 173, 174, 175, 176, 195
 λήμμα συσσωρεύσεως, 174, 175
 γραμμική πολυπλοκότητα, 119, 120, 202, 203, 204
 προφίλ πολυπλοκότητας, 119, 120, 202, 203, 204
- ### Δ
- δακτύλιος, 37, 38
 αντιμεταθετικός, 38

με μοναδιαίο στοιχείο, 38
 πολωνυμικός, 45
 δείκτης σύμπτωσης, 91, 93
 Δήλωση Χρήσης Πιστοποιητικού, 273, 277
 διαιρέτης, 15, 20, 21, 33, 35, 39, 46, 47, 225, 228
 διαιτητής, 305, 307, 308, 309, 314
 διακεκριμένο όνομα, 279
 διαμοιρασμός μυστικών, 268
 διάλυσμα αρχικοποίησης, 137, 162, 165
 διαπιστοποίηση, 274
 διαρροή πληροφορίας, 71, 73
 διαφορική κρυπτανάλυση, 173, 179, 180, 184
 διαφορικό χαρακτηριστικό, 180, 181
 διάχυση, 12, 13, 77, 78, 141, 158, 163
 Δίκτυα Feistel, 146
 Δίκτυα Αντικατάστασης-Μετάθεσης, 141
 με κλειδί, 144
 Δίκτυο Feistel, 152
 ισορροπημένο, 147
 σημαίνοντος στόχου, 147, 148
 σημαίνουσας προέλευσης, 147, 148
 συνάρτηση γύρου, 146, 147, 152, 184, 187, 190, 193
 δυαδική κωδικοποίηση, 63
 δυαδικό μήκος, 64, 65

E

εκθέτης ανάκτησης, 227
 εκθετική συνάρτηση, 138
 εκθετοποίηση, 33, 62, 65, 138
 έλεγχος
 Kasiski, 89, 90
 Κάπα, 104
 τυχαιότητα, 112
 αυτοσυσχέτισης, 113
 σειριακός, 113
 συχνότητα, 112, 113
 Χι, 105
 έλεγχος προσπέλασης, 324
 ελλειπτική καμπύλη, 230, 231, 232, 233, 236, 237, 238, 239, 241, 242, 243, 265, 284
 ElGamal, 242
 ιδιάζουσα, 232
 πρόβλημα διακριτού λογάριθμου, 239, 241
 πρόσθεση σημείων, 233
 σε $GF(2^n)$, 239
 σε modulo p , 236
 εμπιστευτικότητα, 9, 214
 ενδομορφικό κρυπτοσύστημα, 106

Εντολέας, 272
 εξουσιοδότηση, 324, 326
 επίθεση
 γνωστού απλού κειμένου, 10
 γνωστού κλειδιού, 248
 ενδιάμεσου ατόμου, 8, 214, 262, 263, 264, 266, 267, 268, 271, 330, 331
 εξαντλητική αναζήτηση, 11, 14, 82, 103, 108, 133, 138, 170, 172, 192, 196, 201, 241, 261, 264, 323, 328
 επιλεγμένου απλού κειμένου, 11
 προσαρμόσιμου, 11
 επιλεγμένου κρυπτοκειμένου, 11
 προσαρμόσιμου, 11
 κρυπτοκείμενο, 10
 πιθανού μηνύματος, 213
 πλαστογραφίας, 131, 132, 299, 300, 312
 συνάντησης στο ενδιάμεσο, 170, 171
 επιλεκτική πλαστογραφία, 293
 Ευκλείδης, 24

H

ηλεκτρονικό χρήμα, 2, 302, 303
 ημιαδύναμα κλειδιά, 194, 195

Θ

Θεώρημα της Διαίρεσης, 16, 21

I

ισομορφισμός, 40
 ισότιμος, 18, 54, 320

K

κατάλοιπο, 17, 318
 κλάση modulo n , 19, 49
 καταχωρητής ολίσθησης, 79, 115, 116, 117, 119, 120, 124, 165, 190, 201
 με ανάδραση, 115
 με γραμμική ανάδραση, 116, 117, 119
 με μη γραμμική ανάδραση, 124
 κεκαμμένες συναρτήσεις, 144
 Κέντρο Διανομής Κλειδιών, 248, 249
 Κέντρο Μετάφρασης Κλειδιών, 248, 250
 Κινέζικο θεώρημα υπολοίπων, 51
 κλειδί, 3
 απαιτούμενο μήκος, 12
 δημόσιο, 7, 246

εδραίωση, 248, 256, 259, 263, 311
 ενεργό, 171, 201
 ιδιωτικό, 7, 246
 κρυπτοπερίοδος, 245
 κύκλος ζωής, 246
 κύριο, 246, 247, 327
 μυστικό, 246
 πραγματικό, 93, 171, 201
 σκιά ή μερίδιο, 269
 συνόδου, 246, 247, 248, 249, 250, 251, 252, 255, 256, 257, 258, 259, 260, 262, 264, 265, 267, 268, 293
 τέλεια μυστικότητα, 248
 τεμαχισμός, 268
 τερματικού, 246

κλειδοροή
 γεννήτρια κλειδοροής, 76, 78, 79, 112, 164, 167

κουτί αντικατάστασης, 142, 143, 144, 145, 174, 176, 177, 181, 182, 187, 188, 189, 190, 193, 197, 198

κριτήριο της αυστηρής χιονοστοιβάδας, 143

κρυπταλγόριθμος, 3
 AES, 196
 DES, 183, 186
 Hill, 96
 RC4, 207
 Vernam, 94, 95, 96
 Vigenère, 87, 88, 89, 93, 94, 132, 201
 γραμμικός, 84, 85
 μετατόπισης, 81
 ροής, 76
 σημειωματάριο μιας χρήσης, 93, 94, 96
 τμήματος, 157

κρυπτανάλυση, 3
 κρυπτογράφηση, 3
 κρυπτογραφία
 συμμετρική, 5, 6, 157, 211, 214, 246, 251, 292, 305, 306, 317, 330
 συμμετρικός κρυπταλγόριθμος, 157, 181, 214

κρυπτογραφικές πράξεις, 311
 κρυπτογραφική σύνθεση, 106
 κρυπτογραφικό γινόμενο, 106, 107, 108, 157, 158, 170, 171, 181, 183, 194, 196
 κρυπτογραφικό πρωτόκολλο, 10
 κρυπτοκείμενο, 3
 κρυπτοσύστημα, 3
 ElGamal, 228, 229, 242, 298
 knapsack, 214
 Merkle και Hellman, 217

RSA, 220, 221, 226, 293, 294, 296, 316, 335
 άνευ όρων ασφαλές, 73
 ασύμμετρο, 6
 ελλειπτικής καμπύλης, 230, 242
 συμμετρικό, 4
 κώδικας ανίχνευσης τροποποίησης, MDC, 129
 κώδικας αυθεντικοποίησης μηνύματος, MAC, 129

Λ

λεύκανση, 146

Μ

μαντείο, 148, 151, 152, 154, 155
 μέγιστος κοινός διαιρέτης, 20
 μετάθεση
 ψευδοτυχαία, 151
 μη-απόρνηση, 9
 μοναδικός αριθμός, 253, 254, 255, 260
 μονοειδές πολυώνυμο, 44, 47
 μοντέλο εμπιστοσύνης, 273, 275
 επίπεδο, 275, 276
 ιεραρχικό, 276
 μοντέλο επικοινωνίας, 4, 7, 242, 248, 249, 251, 263, 266, 267
 μυστική πόρτα, 211, 212, 216, 217
 μυστικό απόδειξης, 332, 336

Ο

ομάδα, 27
 αντιμεταθετική ή αβελιανή, 27
 πεπερασμένη, 28, 34
 πολλαπλασιαστική modulo n , 31
 προσθετική modulo n , 29
 τάξη, 28
 ομομορφισμός, 40

Π

παράδοξο των γενεθλίων, 127, 128, 373
 πεπερασμένο σώμα, 42, 43, 49, 50, 240, 241
 τάξεως p , 42
 της μορφής $GF(2^n)$, 47
 περίσσεια, 73, 74, 104, 129, 167, 290, 291, 316
 πιστοποιητικό δημόσιου κλειδιού, 273

πληροφορία, 67
 Shannon, 68
 δυαδική πηγή, 68
 πολλαπλάσιο, 15, 59, 97, 162
 πολώνυμο παρεμβολής, 269, 270, 271
 πρόβλημα
 αθροίσματος των γραμματοσήμων, 214, 215
 διακριτού λογάριθμου, 50, 206, 229, 239, 241, 243, 262, 264, 265, 299, 318, 336
 παραγοντοποίησης σύνθετου ακεραίου, 220, 226, 336
 τετραγώνου, 5, 6, 247, 263
 πρόγραμμα κλειδιών, 107, 108, 144, 147, 157, 169, 171, 172, 186, 190, 191, 194, 195, 199, 200
 απλές σχέσεις, 172
 ασθενές, 172
 γεννήτρια, 108
 καθολικά δυνατό, 172
 πρωτεύουσα ρίζα, 59, 60, 61
 πρωτόκολλο
 bit δέσμευσης, 317
 ανταλλαγής κλειδιού με αυθεντικοποίηση, 258
 ανταλλαγής κλειδιών Diffie και Hellman, 212, 220, 264, 265, 266, 267, 268
 απλή ανταλλαγή κλειδιών, 10
 αποτυχία πρωτοκόλλου, 3, 313
 εδραίωση κλειδιών, 253
 κατάσταση πιστοποιητικού, 282
 Κέρβερους, 258, 259, 260, 261
 μεταφορά εν αγνοία, 320
 μηδενικής γνώσης, 331, 338
 μίας φορές, 254
 νοερό πόκερ, 315
 παραγωγής κλειδιών, 256
 πρόκλησης-απόκρισης, 254
 ρίγη κέρματος, 319
 Σταθμού-σε-Σταθμό, 267
 συναρμογής, 331
 πρώτος αριθμός, 16
 σχετικά πρώτοι, 21, 22, 29, 30, 40, 42, 51, 52

P

ρίγη κέρματος, 319, 320, 321, 340

Σ

συγκεντρωτική διαχείριση κλειδιών, 249

σύγχυση, 12, 13, 78, 124, 141, 158, 163
 συμπληρωματική μεταβλητή, 193
 συνάρτηση ϕ του Euler, 30
 συνάρτηση Carmichael, 225
 συνάρτηση hash, 125, 126, 127, 128, 162, 257, 267
 MD4 και MD5, 138, 140
 SHA, 140
 ανθεκτικότητα σε συγκρούσεις, 126
 επαναληπτική, 136
 κρυπτογραφική, 126
 μονόδρομη, 126, 132, 136, 138
 συνάρτηση ανάδρασης, 116, 117, 120, 123, 124
 συνάρτηση συμπίεσης, 136, 139
 σύνθετος αριθμός, 16
 σύνοψη
 μέγεθος, 127
 μηνύματος, 125, 291, 292, 308, 309
 σύστημα ψηφιακής υπογραφής, 288, 289, 290, 291, 292, 294, 305, 307, 308
 ElGamal, 298, 299
 Fiege-Fiat-Shamir, 296
 με αυτοανάκτηση, 290
 με παράρτημα, 292, 293, 296
 Πρότυπο Ψηφιακής Υπογραφής, DSS, 300
 σφάλμα, 12, 77, 78, 79
 διάδοση σφαλμάτων, 12
 στη λειτουργία CBC, 163
 στη λειτουργία CFB, 166
 στη λειτουργία OFB, 167
 σχέδιο (m, n)-κατωφλίου, 269

T

τέλεια μυστικότητα, 71, 72
 τετριμμένος διαρέτης, 15
 τρίτη οντότητα, 266, 267, 268, 272, 314, 322
 τρόποι λειτουργίας, 158, 160, 168, 169
 ανάδραση εξόδου, 158
 ανάδραση κρυπταλγόριθμου, 158
 ηλεκτρονικό κωδικοβιβλίο, 158
 κρυπταλγόριθμος αλυσιδωτού τμήματος, 158
 μη τυποποιημένοι, 167
 τυχαία συνάρτηση, 151, 153, 154
 τυχαιότητας, δημιουργία συνθηκών, 229

Υ

υπό συνθήκη αβεβαιότητας, 69

υπό συνθήκη πιθανότητα, 68, 69
υποδομή δημόσιου κλειδιού, PKI, 271
υποομάδα, 32, 33, 34, 35, 58, 237
 γήσια, 32, 33
 που δημιουργείται από στοιχείο, 33

X

χαρακτηριστικό πολυώνυμο, 117, 120, 121,
 122, 123
 πρωτεύον, 117
χρονοσφραγίδα, 253, 256, 257, 258, 260

Ψ

ψευδοτυχαία γεννήτρια, 153
ψηφιακή υπογραφή, 135, 136, 266, 268, 273,
 277, 278, 286, 287, 289, 292, 293, 294,
 295, 296, 297, 298, 300, 301, 305, 307,
 308, 309, 332, 337
 πράξη επαλήθευσης, 288, 294
 πράξη υπογραφής, 287, 288, 294
 τυφλή, 302
ψηφιακό πιστοποιητικό, 273, 274, 275, 276,
 277, 278, 279, 280, 281, 282, 329, 337
 διακεκριμένο όνομα, 279
 X.509, 277

