

Index

- 1-round RC5, 251, 255
- 2-round MD4, 339
- 3DES, 228, 264
- 4-digit PIN, 390
- 4-round FEAL, 287
- 4-round IDEA, 239
- 6-round RC5, 246
- 8-bit computers, 339
- 8-bit processors, 271
- 8-bit smartcards, 261
- 8-byte shift register, 421
- 8-round DES, 162
- 12-round RC5, 247
- 14-round RC5P, 251
- 16-bit checksum, 356
- 16-bit microprocessor, 234
- 16-round DES, 162
- 32-bit processors, 258, 261
- 32-bit unit ID, 356
- 40-bit hash value, 350
- 48-byte header, 457
- 64-bit block, 391
- 64-bit seed, 372
- 128-bit keys, 393, 480
- 256-bit AES, 428
- 802.11 standard, 272
- 802.15.4/802.15.4b standard, 274
- 1984, Orwell, 473
- A3 algorithm, 323
- A5 algorithm, 283, 285
- A5/2, 286
- A8 algorithm, 323
- access privileges, 70, 445
- AccessData, 11, 90, 280
- active attackers, 212
- ActiveX controls, 367
- adaptive Ziv-Lempel algorithm, 105
- adaptive-chosen-plaintext attack, 63, 190
- Adleman, Len, 176, 202
- admission control, 397, 399
- Advanced Encryption Standard, 262
- AES, 167, 303, 305, 424, 449
- AES Initiative, 262
- AES requirements, 263
- AES shortlist, 265
- AES-128, 334
- air turbulences, 223, 298

- AIX, 446
Alberti, 35
algebraic methods, 312
algorithms, implementation, 205
Anderson, 286, 508, 509
anonymity, 386
anonymous remailers, 421, 431
ANSI standard X509.3, 431
ANSI standard X9.17, 221, 419
Arms Export Control Act, 412
ASCII characters, 102
Ascom Mail, 416
assembler commands, 453
assembler language, 480
associativity law, 236
asymmetric cipher, 348
asymmetric methods, 168, 428
AT&T Bell Laboratories, 356
Athlon PC, 24
Atkins, Derek, 422
ATM, 389
authentication key, 329, 439
authenticity, 436
automatic decryption, 22
automatic teller machine, 389
avalanche effect, 125, 138, 153, 311
AWT, 142
- Baldwin, Robert, 55, 513
bank computers, 165
banking applications, 264
base station, 282, 323
Bass-O-Matic, 411
BBS generator, 294
behavioral patterns, 384
Bellcore, 163
Benaloh, 382
benchmarks, 453
Benioff, 300
Bennett, 300
Biham, Elie, 116, 152, 163, 229, 508
binary files, 216
binary tree, 228
BioID, 397, 399
biometric authentication, 398
biometrics, 394
birthday attack, 209, 240, 350
Biruykov, 509
Biryukov, 229, 247
bit commitment, 376
bit-twiddling attack, 208
bitwise encryption, 81
bitwise processing, 124
bitwise Vigenère, 38
bitwise XOR, 38
Blaze, Matthew, 291, 356, 446, 513
Bleichenbacher, 509
Bleichenbacher attack, 443
Bleichenbacher, Daniel, 190
Bletchley Park, 34, 51
blind signatures, 378
blinded checks, 385
blinding factor, 379, 385
block algorithm, 211, 216, 221, 287, 289
block cipher, 126, 210
blockwise encryption, 216
Blowfish, 289, 424, 443, 449
Blowfish cryptanalysis, 290
Blowfish-128, 334
Blum numbers, 294
bomba (Enigma), 48
Bond, James, 214, 336, 445
Boneh, 163
Borst, 239
Bourne shell, 452
Bradford University, 283
Briceno, Marc, 325
British Telecom, 297
Brokat, 240, 482
brute force, 304
brute-force attack, 63, 140, 227
BSAFE, 231
Bühler, Hans, 402
byte order, 454

- C-network, 282
- cache hits, 308
- Caesar addition, 18, 94
- Caesar cipher, 18, 75
- call records analysis, 463
- Cambridge University, 53
- Capstone chip, 291, 354
- card phones, 462
- Caro-Kahn, 195
- CAST5, 424
- cattach command, 446
- CBC mode, 207, 357
- CBW, 55
- cell phone networks, 323
- cell phones, 462
- CERT, 12
- certificate, 429
- certification hierarchy, 428
- CFB, 210, 215
- CFB mode, 358
- CFS, 212
- challenge-reply scenario, 380
- Chan, 388
- Chaos Computer Club, 325, 395, 507
- character pairs, 32
- characteristics, 154
- Chaum, 378, 383
- checksum, 208, 218, 225, 286, 456
- chess programs, 11
- Chinese Remainder Theorem, 192
- chosen-challenge attack, 325
- chosen-ciphertext attack, 64, 378, 439
- chosen-key attack, 64
- chosen-plaintext attack, 63, 188
- Chuang, Isaac, 302
- Churchill, 51
- Cipher Block Chaining Mode, 207
- Cipher Feedback Mode, 210
- ciphering cylinder, 39, 75
- ciphering error, 34, 123, 208
- ciphertext, 17
- ciphertext stealing, 217
- ciphertext-ciphertext attack, 63
- ciphertext-only attack, 63
- cleptographic attack, 406
- cleptography, 404
- Clipper chip, 291, 317, 354, 412
- Cochrane, 476, 511
- code book, 46
- code breaking, 17
- collision, 338
- columnar transposition, 29
- common hash function, 337
- COMP128, 325
- completely blind signatures, 378
- complexity theory, 65
- compress program, 103
- compression, 26, 102, 275, 420, 442
- compression function, 338
- compression permutation, 137
- compromised-ciphertext-ciphertext attack, 49
- computer algebra, 55
- computer crime, 389
- confusion, 124, 245, 311
- congruence arithmetic, 178
- congruencies, 177
- congruent modulo, 176
- Conrad, Peter, 280, 507
- consecutive encryption, 227
- conventional signatures, 353
- Copacobana, 143
- Coppersmith, 288
- Coppersmith, Don, 134
- count byte, 216
- counter mode, 448
- Courtois, Nicolas, 270
- Coventry, 51
- Crack*, 70
- cracking A5, 286
- Cray, 150, 285
- CRC, 286
- CRC polynomial, 275
- credit card numbers, 220, 480
- CRT, 192
- crypt, 55

- Crypt Breakers Workbench, 55
- cryptanalysis, 1, 17, 61
- cryptanalysis, Enigma, 45
- cryptanalysis, Skipjack, 292
- crypted file system, 212
- Crypto AG, 402
- Crypto Law Surveys, 477
- crypto-file systems, 445
- crypto-smartcard, 395
- cryptogram, 19, 23
- Cryptographic File System, 446
- cryptographic protocols, 313
- cryptography, 1, 17
- cryptology, 1
- CSP-642, 40
- Cuba crisis, 335
- cube transposition, 28
- cuckoo channel, 352
- Currer-Briggs, Noel, 33
- cypherpunks, 272

- Daemen, Joan, 264
- daemon, 418
- daemon, sshd, 438
- Data Encryption Standard, 133
- data espionage, 405
- data integrity, 208
- data privacy, 464, 475
- data repositories, 302
- data warehousing, 464
- data-dependent rotations, 249, 260
- database encryption, 212
- De Mare, 382
- DEC workstation, 280
- Deep Crack, 142
- Demillo, 163
- denial-of-service attack, 321, 332, 364
- DES, 133
- DES algorithm, 123
- DES chips, 226
- DES Crack machine, 448
- DES features, 139
- DES modifications, 225

- DES operating modes, 206
- DES round, 139
- DESX, 231
- DFA, 163
- diagonal board, 51
- dictionary attack, 67, 224, 226, 390, 451
- difference, blocks, 154
- differential cryptanalysis, 116, 125, 152, 247, 288
- differential fault analysis, 163
- differential linear cryptanalysis, 162, 288
- Differential Power Analysis, 309
- Diffie-Hellman key exchange, 198
- Diffie-Hellman patent, 196
- Diffie-Hellman key exchange, 316
- diffusion, 124, 238, 244, 311
- digital signatures, 336, 344, 482
- digital watermark, 16
- digitized speech, 15
- digram, 22
- digram substitution, 32
- Dippold, Ron, 85
- direction flag, 329
- discrete logarithm, 178, 196, 236, 301
- distinguished pairs, 30
- distributive law, 235
- DOS, 280
- DOS computer, 68
- double encryption, 227
- Double-DES encryption, 226
- doubtful cryptography, 401
- DPA, 309
- DRAMs, 165
- DSA, 424
- DSA signature algorithm, 352

- e-mail security, 410
- eBay, 373
- ECB, 215
- ECB mode, 206, 357
- Echelon, 465
- EEPROM, 163
- EES, 291, 354

- EFF, 142
- electromagnetic radiation, 305, 310
- Electronic Codebook Mode, 206
- Electronic Frontier Foundation, 142
- electronic money, 383
- electronic signatures, 345
- ElGamal, 424
- ElGamal method, 196, 197
- encrypted checksum, 209
- encryption, pkzip, 275
- encryption, WordPerfect, 82
- ENIAC, 54, 303
- Enigma, 5, 42, 43
- Erathostene sieve, 185
- error probability, 186
- error propagation, 214
- error-correcting codes, 331
- Escher knot, 129
- Escrowed Encryption Standard, 291, 354
- ETH Zurich, 232
- EU Echelon Committee, 469
- Euler's function, 179
- Euler's generalization, 179
- exclusive OR, 57
- expansion permutation, 138
- extended Euclidean algorithm, 182, 189
- Extended Sparse Linearization, 270

- face recognition, 472, 475
- FaceVACS, 396
- facial recognition, 395
- factoring, 180
- fail-stop signatures, 381
- false accept rate, 399
- false reject rate, 399
- FAR, 399
- fast password check, 218
- fcrypt, 59
- fcrypt encryption, 115
- FDI chip, 470
- FEAL, 287, 339
- FEAL-NX, 288
- federal principle, 176

- federated ID, 373
- Feistel network, 132, 241, 287, 289, 292
- Feistel, Horst, 132, 134
- Ferguson, Niels, 269
- Fermat's little theorem, 179, 419
- Feynman, 300
- Fiat, 383
- fifth-order equations, 128
- filler bytes, 216
- FinCEN, 473
- finger command, 432
- fingerprint, 395, 414
- fingerprint recognition, 399
- firewall, 212
- FireWire standard, 251
- FolderBolt, 289
- forbidden pairs, 22
- Fortezza, 291
- Frankel, 388
- FreeBSD, 444
- frequency analysis, 21
- frequency hopping, 282
- frequency profile, 101
- FRR, 399
- functional analysis, 10

- gait, 397
- Galois fields, 267, 268
- garbled blocks, 214
- Gardner, 176
- Garfinkel, 412
- Gartenpflege (Enigma), 49
- Geiger counters, 223
- generalized Euclidean algorithm, 197
- generating keys for RSA, 187
- generatrix, 78
- Givierge, 78
- global family key, 355
- GNU Privacy Guard, 423
- GnuPG, 224, 481
- Gold Bug, 21
- Goldberg, 325
- Goldberg, Ian, 219

- Goldwasser, 294
- Golic, Jovan D., 283, 327
- goodpasswd, 73
- GOST, 339
- graphics tablet, 396
- graphologist, 353, 397
- grep, 74
- group, 31, 226
- group property, 226
- Grover algorithm, 302
- GSM handsets, 286
- GSM standard, 282, 323
- gzip program, 104, 420

- Hager, Nicky, 466
- hairspray attack, 390
- Halder, 299
- hand geometry, 397
- hand-writing recognition, 471
- Handschuh, Helena, 254
- hardware keylogger, 472
- Harris, 45
- hash function, 337
- hash table, 337
- hash value, 337
- Hawkes, Philip, 239
- Hellman, 509
- Hellman tables, 147
- Hellman tradeoff, 145
- helper programs, 436, 453
- hide information, 352
- High-Order DPA, 310
- high-security tract, 391, 399
- Hilbert problems, 10
- hill-climbing method, 55
- Hinsley, Harry, 53
- HMAC, 343, 373
- home banking, 362, 364
- homophone substitution, 25
- homophony, 77
- HOTP algorithm, 373
- HP-UX UNIX, 220
- HP/UX, 446

- Huffmann method, 115
- Hughes, Richard, 298
- Hummelt, 7
- hybrid methods, 171

- IAO, 464
- IBM P960, 342
- IDEAS, 232, 424, 470
- IDEA in PGP, 411
- IDEA method, 233
- IDEA patent, 233
- IDEA round, 236
- IEEE standard 802.15.4, 448
- IETF SSH, 443
- illusory complication, 81
- image transformation, 129
- impossible differentials, 292
- IMSI catcher, 286
- index of coincidence, 91
- industrial espionage, 469, 472
- Information Awareness Office, 464
- information harvesting, 462
- information hiding, 14
- initialization block, 211
- initialization vector, 208, 218, 274, 275, 277, 355, 419, 447, 456
- Inode number, 448
- insertion attack, 213, 272, 275, 311, 420
- integers, 178
- integrity, 335
- integrity key, 329
- Intel processors, 244, 454
- intellectual property, 15
- Intelligence agencies, 466
- Intelsat, 467
- interception activities, 465
- interleaved CBC mode, 215
- interlock protocol, 173
- Internet Protocol, 208
- interpolation attack, 269
- interrupt vectors, 223
- intranet, 212, 436
- invisible ink, 12

- IP protocol, 442
- IP spoofing, 8
- IP-spoofing attack, 437
- IPsec, 317
- iris scan, 396
- Irix, 446
- isotopy, 236
- Itanium2 processor, 341
- IV, 208

- Jaffe, 309
- Java applets, 367
- Jun, 309

- Kahn, Codebreakers, 53
- Kahn, David, 512
- Kahn, Enigma, 5
- Kahn, semagram, 12
- Kaliski, 373
- kappa, 91
- Karn, Philipp, 505
- Kasiski method, 93
- KEA, 292, 317
- KEK, 169
- Kerberos, 215, 321, 401
- key crunching, 225
- key distribution, 171, 314
- key encryption key, 169
- key escrow, 291, 354, 406, 423, 477
- key generation, 219, 239
- key revocation, 430, 434
- key servers, 171, 416
- key tags, 369
- key transformation, 137
- key-dependent S-box, 229
- key-detection algorithm, 247
- keyboard sniffers, 8
- keybox, 255
- keyrings, 428
- keystrokes, 223, 398
- KGB, 58
- kiss (Enigma), 49
- Kleine Signaltuch, 50

- Kmail, 434
- knapsack algorithm, 199
- knapsack method, 201
- Knoppix, 445
- known-plaintext attack, 63, 227
- Knudsen, 239, 247
- Koch, Werner, 423
- Kocher, 309, 508
- Kocher, Paul, 307
- Koops, Bert-Jaap, 477, 511
- Korn shell, 452
- Korn, Willi, 43
- Kuhn, 163, 508
- Kushilevitz, 247

- Lai, 232
- Lamport, Leslie, 362
- LAN, 401, 436
- Lange, David, 468
- Langford, 509
- laser microphones, 475
- Latin square, 80
- Law Enforcement Access Field, 355
- LBS, 463
- LEAF, 355
- LEAF feedback, 357
- letter distribution, 54
- letter repeat pattern, 23
- LFSR, 284
- libcrypto library, 334
- linear combination, 120
- linear cryptanalysis, 157, 248
- linear dependencies, 190
- Linear Feedback Shift Register, 284
- linear function, 284
- linear methods, 159
- linear relationship, 160
- Linux, 223, 280, 424, 428, 434, 435, 444, 445
- Lipton, 163
- locally based services, 463
- Lockerbie, 403

- Lofoten Islands, 49
- Logdaemon, 449
- long-term validities, 349
- Los Alamos, 298
- Lotus Notes, 271
- LSH, 444
- Lucifer project, 134

- M4 project, 55
- M6 algorithm, 251
- MA transformation, 238
- MAC, 338
- Mac software, 85
- Magdeburg cruiser, 4
- Magenta method, 263
- magic numbers, 26
- mail encryption, 433
- Mailsafe, 231
- malicious software, 343
- man-in-the-middle attack, 173, 371, 430
- mantra, 224
- Markoff, 163
- Markov cipher, 247
- Massey, 232
- matrix, 78
- Matsui, 157, 288
- Matui, 328
- MD2, 338, 339
- MD4, 339
- MD5, 339, 424
- MD5 collision, 342
- MD5-HMAC, 344
- meet-in-the-middle attack, 227
- Meier, 247
- Merkle, Ralph, 322, 338
- message authentication code, 338
- message digest, 338
- message exchange, 169
- message integrity check, 338
- message key, 46
- Meyer, 134
- MIC, 338
- Micali, 294

- microdots, 12
- microphones, 475
- Microsoft Excel, 274
- Microsoft Internet Explorer, 367
- Microsoft Word, 68, 274, 401
- Midway Islands, 5
- militaries, 39, 459
- military cryptography, 285
- MIME, 431
- MIPS, 193
- MISTY1 algorithm, 328
- mix servers, 464
- MM protection method, 391
- mod-3 cryptanalysis, 250
- modem, 442
- modular arithmetic, 178
- monoids, 236
- Morgenstern, Christian, 24
- Morse code, 12
- mouse movements, 223
- movement patterns, 462
- Mozilla, 434
- MS-DOS, 216, 420
- Muffett, Alec, 70
- multiple encryption, 31, 226
- Murphy, 288
- Mutt, 431, 434, 435
- M-94, 39

- N-gram analysis, 465
- N-Hash, 339
- NAI, 423
- Naor, 383
- NASA, 14
- National Institute of Standards and Technology, 134
- Nautilus, 289
- negative pattern search, 45, 75
- Netscape Navigator, 220, 271, 479
- Netscape story, 219
- Network File System, 436
- NeuroMetric, 475
- newwpcrack, 9, 85

- NFS, 194, 436
- NIST, 134, 262, 340
- non-interactive zero-knowledge proof, 380
- notebook, 342, 445
- Novell NetWare, 363
- NSA, 5, 54, 65, 285, 291, 301, 317, 340, 403, 411, 465
- NSA, VENONA, 59
- nuclear magnetic resonance, 302
- nuclear weapons, 335
- number theory, 179, 188
- number-field sieve, 194

- Oasis, 513
- Oasis program, 471
- OATH, 372
- OCR software, 471
- OFB, 211
- OFB mode, 358
- offline-payment protocols, 384
- Olson, Edwin, 23
- one-letter password, 222
- one-time pad, 56, 294
- one-time passwords, 362, 452
- one-way accumulators, 382
- one-way hash function, 336, 337, 347
- online encryption, 212
- online-payment protocols, 384
- Open Authentication Initiative, 372
- OpenPGP, 423, 432
- OpenSSH, 444
- operating modes, 206
- OPIE, 449
- OPIE program, 363
- Oracle Secure SQL, 271
- Ostholm, Stig, 505
- Output Feedback Mode, 211
- overhead, 456

- P-box, 137
- pack program, 115
- padding, 216, 420, 457

- parabola, 332
- parallelism, 215
- parity check, 164
- parity error, 165
- partial differential cryptanalysis, 247
- passphrase, 224, 442, 450, 455
- passphrase-s, 417
- password entry, 222
- password program, 72
- password token, 372
- path of trust, 415
- pay-TV, 163
- PCBC, 215
- PEM, 175, 428
- period, 37
- permutation, 20
- permutet alphabet, 33
- personal identification number, 3
- perturbation vector, 447
- PES, 232
- Pfitzmann, Birgit, 16, 381
- PGP, 176
 - algorithms, 417
 - classic, 409
 - digital signatures, 352
 - fingerprint, 414
 - functions, 413
 - implementation, 417
 - key generation, 419
 - key servers, 416
 - motivation, 410
 - passphrases, 417
 - patent, 411
 - PEM, 428
 - portability, 416
 - prime-number generation, 419
 - random generation, 418
 - Release 2.6, 411
 - Release 2.6.3, 422
 - release numbers, 423
 - security, 418
 - Version 5.0, 422
 - Web of Trust, 414

- PGP/MIME, 434
- PGP/MIME standard, 431
- PGPfone, 289
- PGPPASS, 417
- phishing attacks, 371
- phone banking, 362
- picklock keys, 423
- Pieprzyk, Josef, 270
- PIN, 3, 309, 325, 369, 389, 391, 399
- PIN key, 391
- Pine, 434
- piracy, 15
- pkcrack program, 280
- PKCS#1, 190
- PKI, 429
- PKP, 195, 411, 482
- pkzip, 115, 275
- plaintext, 17
- plaintext attack, 17, 277
- playfair method, 34
- plugboard, 43
- Plumb, Colin, 422
- PnuPG, 423
- pocket calculators, 369
- Poe, Edgar Allan, 21
- polarization of light, 295
- polyalphabetic substitution, 35
- polynomial method, 332
- pool keys, 391
- poor passwords, 73
- Porta, 32
- portability, 449
- position-finding information, 463
- possible keys, 66
- possible weak keys, 157
- power attack, 309
- power consumption, 309
- PPP, 442
- Pretty Good Privacy, 409
- prime numbers, 179
- prime-number theorem, 188
- Privacy Enhanced Mail, 175, 428
- private key, 168, 427
- probabilistic algorithm, 293
- probabilistic cryptography, 381
- probable values, 154
- probable word, 68, 76
- product algorithm, 127, 161, 247, 268, 292
- Progress database, 372
- Promis, 8
- Propagating Cipher Block Chaining, 215
- Proposed Encryption Standard, 232
- ps command, 456
- pseudo collisions, 344
- pseudo-random events, 222
- public domain, 444
- public key, 168
- Public Key Infrastructure, 429
- Public Key Partners, 195
- public-key distribution, 174
- public-key methods, 168
- Putty, 438
- Python, 23, 334

- quadratic sieve, 193
- quantity kappa, 91
- quantum computer, 194, 299
- quantum cryptography, 295, 304
- quantum entanglement, 300
- Quantum Information Science, 301
- quantum mechanics, 295, 299
- qubit, 300
- Quicken, 368
- quintets, 329

- Rabin-Miller method, 419
- Rabin-Miller text, 186
- RACE Initiative, 401
- Radio Network Controller, 329
- random number generation, 188
- random-number generator, 220, 294
- randomness, 222, 293, 418, 424
- RC4, 271
- RC4/5/6, 449

- RC5, 455
 - AES requirements, 258
 - algorithm, 241
 - cryptanalysis, 244
 - description, 241
 - design goals, 240
 - differential cryptanalysis, 246
 - linear cryptanalysis, 248
 - new attacks, 251
 - one-round, 252
 - patent, 258
 - rotations, 246
 - round, 241
 - security, 245, 257
 - timing attack, 254
 - versus RC6, 260
 - weak keys, 248
- RC5a, 219, 247, 249, 255, 258, 452
- RC5P, 250
- RC6, 258, 260
- reduced key space, 47, 67, 219, 222
- redundancy, 208
- reflector, 43
- Rejewski, Marian, 47
- related keys, 156
- relative frequency, 101
- relatively prime, 179
- remailer, 6
- remainders, 178
- replay attacks, 320, 328, 363
- replay daemon, 450
- residual classes, 332
- retinal scan, 396
- reversing drum, 43
- right pairs, 154, 247
- Rijmen, 239
- Rijmen, Vincent, 264
- Rijndael, 264, 266, 424
- Ring of Steel, 475
- Riordan, Mark, 37, 432
- RIPE project, 340
- RIPE-MD160, 340
- RIPEM, 432
- RIPEMD-160, 424
- Rivest, Ron, 173, 176, 231, 240, 271, 339
- roaming contracts, 324
- robust secret-sharing protocols, 332
- Rogaway, 288
- Roman army, 18
- root computer, 176
- root server, 429
- ROT13, 20
- rotor drum, 42
- rotor machine, 40
- round, 127
- round, Feistel, 132
- RSA, 424
- RSA cards, 309
- RSA Challenge, 141
- RSA Data Security, 195
- RSA for signatures, 345
- RSA Laboratories, 245, 258, 339, 373, 482
- RSA method, 176, 184, 378, 410
- RSA patent, 195, 317
- RSA SecurID, 369
- RSA security, 187
- RSADSI, 272, 274, 411
- RSAREF, 411
- Rubik's cube, 10
- S-box, 137, 153
- S/Key, 449
- S/MIME, 431
- SafeGuard Private Crypt, 271
- SAFER-SK128, 447
- salt, 72
- Sandia National Laboratories, 291
- SATAN program, 223
- Scherbius, Arthur, 42
- Schlafly, Roger, 276
- Schneier, Bruce, 2, 38, 59, 135, 156, 159, 205, 226, 229, 274, 289, 303, 313, 379, 398, 430, 435, 473, 508
- Schroepfel, Richard, 269
- Schwartz, 462, 510

- sci-crypt newsgroup, 401
- sci.crypt, 53
- sci.crypt newsgroup, 272, 283
- Scientology, 6
- screen saver, 396
- screen-lock program, 222
- SDA, 325
- SEAL, 288
- secret key, 352
- secret sharing, 331
- secret splitting, 330
- secret-key distribution, 169
- Secure Hash Algorithm, 340
- SecurID, 369
- seed, 370, 450
- seismometers, 223
- self-extracting archives, 343
- SELinux, 418
- semagram, 12
- semiconductor technology, 303
- semiweak keys, 157
- Serpent, 270
- server, 319, 370
- server hierarchy, 430
- SESAME, 401
- session key, 168, 169, 221, 286, 315, 318, 323, 419
- session-key distribution, 438
- SETUP systems, 405
- Shamir, Adi, 116, 148, 152, 163, 173, 176, 192, 194, 509
- Shannon, C. E., 124
- shareware, 281, 481
- SHA-1, 340, 424
- SHA-1-HMAC, 373
- SHA-256, 341, 344, 424
- Shepherd, Simon, 283
- shift register, 211, 284, 421
- shifted distributions, 94
- Shor algorithm, 300, 301
- short key length, 225
- short passwords, 224
- sieving numbers, 185
- signaling messages, 329
- signature algorithm, 352
- signature recognition, 396
- SIM card, 323
- Simmons, 352
- Simple Power Attack, 309
- simple substitution, 20
- simple XOR, 38
- Sinkov, 29
- SKIP, 317
- Skipjack, 291, 305, 354
- Skytale, 28
- Smartcard Developer Association, 325
- smartcards, 309, 399
- Smartpen, 396, 400
- snake oil, 402
- Snefru, 338
- Softpro, 396
- Solaris, 220, 446
- solarization effect, 148
- Someren, Nicko van, 192
- SONET OC-48, 470
- speech input, 223
- spoofing attack, 437
- square polynomial, 332
- squeezing attack, 360
- Squirrel Mail, 435
- SRAMs, 165
- SSH, 191
- ssh command, 440
- ssh daemon, 441
- SSH installation, 440
- SSH Secure Shell, 436
- ssh-agent, 442
- SSH1, 438
- SSH2, 443
- SSL server, 191
- SSL version, 191
- statistical analysis, 32
- steganography, 12, 352, 404
- Steganos, 15, 271
- STOA report, 469

- stream cipher, 126, 213, 214, 216, 271, 275, 283, 288, 360
- stroboscopic cameras, 475
- strong SETUP systems, 405
- subliminal channel, 352, 378
- substitution box, 138
- sum of the digits, 337
- Sun-4 workstation, 246
- super-PIN, 326
- superincreasing knapsack, 199
- superuser, 70, 417, 438, 445, 450
- Surety Technologies, 376
- symmetric methods, 167, 205, 314
- symmetric RC4, 220
- synchronization, 289, 363
- synchronization error, 215
- system time, 223

- tamperproof chips, 163, 323
- TAN, 364
- Tangram, 464
- tap sequence, 285
- TCP/IP, 436
- telephone surveillance, 475
- teleshopping, 383
- telnet program, 371
- text integrity, 215
- TIA, 464
- time-memory tradeoff, 145
- timesharing, 282
- timestamp, 221, 320, 375, 431
- timing attack, 191, 254, 307–309
- token, 369
- topic analysis, 465
- Toshiba, 299
- Total Information Awareness, 464
- traffic analysis, 431, 462
- trail mapper, 470
- transaction number, 364
- transmission error, 214
- transposition cipher, 28
- trap command, 452
- tree search, 23
- tree structure, 27, 431
- Triple-DES, 226, 228, 424, 447
- triplets, 324
- Tripwire program, 344
- Trojan cryptography, 400
- Trojan horse, 71, 400
- trustworthy computer, 176
- trustworthy key, 414
- trustworthy server, 320
- trustworthy timestamp service, 375
- Tsiounis, 388
- Tuchman, 134, 228
- turbulences, 298
- Turing, 48
- Twinkle, 194
- two-letter passwords, 222
- Twofish, 270, 424, 449

- UKUSA alliance, 466
- Ultra project, 52
- ultracomputer, 305
- UMTS, 328, 448
- unit key, 355
- universal key, 427
- UNIX, 436, 445
- UNIX DES encryption, 211
- UNIX login, 70
- UNIX pipeline, 422
- UNIX systems, 70, 222
- US export laws, 479
- US Naval Research Laboratories, 449

- value of information, 4
- variable biometrics, 399
- Vaudenay, 290
- vein patterns, 397
- Venema, Wietse, 223, 449
- VENONA project, 58
- VeriSign, 373
- VeriSign Identity Protection, 373
- Vernam cipher, 38, 268, 447
- ViaCrypt, 411
- Viaris method, 78

- video conferences, 15
- vigc_crk program, 105
- vigcrack, 95
- Vigenère cipher, 36
- Vigenère method, 91
- vim editor, 435
- VIP, 373
- virus infection, 338
- visual cryptanalysis, 148
- VLSI Technology, 147
- voice recognition, 397, 471
- vulnerabilities*, 68
- vulnerabilities, Enigma, 52
- vulnerabilities, general, 69

- Wagner, 325
- Wagner, David, 219
- Waidner, Michael, 381
- Wal-Mart, 464
- Wassenaar, 480
- Wayner, 14
- weak cryptography, 401
- weak keys, 157, 239, 247, 312
- weak passwords, 70
- weak SETUP systems, 405
- weather key, 49
- Web of Trust, 176, 414
- Web servers, 480
- Webcams, 472
- Welchman, Gordon, 51
- WEP standard, 274
- Westfeld, 15
- Wheatstone, 33
- whitening, 230, 394, 447
- Whiting, Doug, 269
- wide-mouth frog protocol, 320

- Windows, 445
- Windows computer, 68, 222
- Windows NT, 258
- Windows programs, 440
- Winkler, Ira, 461
- WinPT, 434
- Winterbotham, 53
- wireless sensor networks, 274
- Wood, 462, 510
- WordPerfect, 9
- WordPerfect encryption, 82
- WordPerfect styles, 85

- X-protocol, 442
- X-terminal, 444
- X.509 protocol, 429
- X509.3, 431
- X9.17, 221, 419
- Xilinx chips, 286
- XSL method, 270
- Xtra Secure, 465

- Yamagishi, 288
- Yamamoto, 5
- Ylönen, Tatu, 437
- Young, Adam, 401
- Yung, Moti, 401

- zero-knowledge proof, 332, 380
- ZigBEE, 448
- ZigBEE standard, 274
- zigzag method, 57
- Zimmermann, Phil, 410
- Ziv-Lempel algorithm, 104
- Ziv-Lempel-Welch compression, 27