

Index

- abelian group, 63
- AES, 314, 317
- Agence Nationale de la Sécurité des Systèmes d'Information, *see* ANSSI
- algebraic number, 58
- ANSSI, 315
- application-specific integrated circuit, *see* ASIC
- approximation regime, 22, 30
- arithmetic
 - double-word, 255
 - floating-point, 255
 - long-integer, 254
- ASIC, 318
- baby-step–giant-step, *see* BSGS
- Barreto–Naehrig curves, 327, 329
- birthday
 - paradox, 43, 54
 - search, 186
- birthday bound, 295
- bit-slicing, 232
- Bitcoin, 175–180, 316, 318
- BKZ, 15, 18, 19, 24, 26, 27, 30–34, 38, 39, 330
 - BKZ 2.0, 20
 - pressed, 24
- Bleichenbacher
 - biased nonce, 180
 - oracle attack, 151
 - signature forgery, 145, 152
- Boneh–Durfee attack, 96
- bounded distance decoding, 29
- Brainpool, 172
 - curves, 172
- BSGS, 108, 294
- BSI, 315
- Bundesamt für Sicherheit in der Informationstechnik, *see* BSI
- Certicom ECC challenge, 325
- certificate
 - pinning, 192
- certification authority
 - rogue, 191
- CFRAC, 53–54, 56, 75, 76, 319, 323
- Chinese remainder theorem, 49, 71, 107, 161, 294
- closest-vector problem, 330
- CN11 simulator, 23
- Coen brothers, 8
- collision
 - chosen-prefix, 184, 186
 - collision attack, 182
 - collision resistance, 182
 - identical-prefix, 184
 - meaningful, 190
 - near-collision, 184
- complexity
 - of AKS primality test, 47
 - of BPSW primality test, 46
 - of CFRAC, 53
 - of elliptic-curve method, 66
 - of number field sieve, 62
 - of Pollard rho, 43
 - of quadratic sieve, 57
- constant-time implementations, 223
- continued fraction, 50
- continued fraction factoring algorithm, *see* CFRAC
- contractions, 257
- COPACOBANA, 316
- Coppersmith method, 15, 79, 143
- Crandall

384

number, 239, 242, 244
 curve
 anomalous, 121, 326
 curve25519, 242–243
 invalid, 172
 replacement attack, 176
 singular, 119
 standard, 172
 CWI, 321
 cyclotomic subgroup, 296
 Darmstadt lattice challenge, 330
 Data Encryption Standard, *see* DES
 Deep Crack, 316
 DES, 47, 316, 317
 DH
 alphabet soup explosion, 298
 computational problem, 294
 decisional problem, 162, 295
 in the wild, 154–170
 key exchange, 294, 298, 318
 differential
 characteristic, 185
 cryptanalysis, 184
 Diffie–Hellman, *see* DH
 digital signature, 48
 algorithm, *see* DSA
 discrete logarithm problem, *see* DLP
 DLP, 106, 294
 descent and cover methods, 117
 generic algorithm, 107
 weak curves, 117
 double rounding, 257
 DROWN attack, 151
 DSA
 in the wild, 174–181
 ECC, 237, 325
 arithmetic, 237–243
 ECDH
 in the wild, 170–173
 ECDSA
 in the wild, 174–181
 ECM, 64, 75, 76, 325
 second stage of, 66
 ECRYPT, 313, 315
 ECSTR, *see* XTR
 EdDSA, 242
 efficient compact subgroup trace
 representation, *see* ECSTR
 Electronic Frontier Foundation, 316
 ElGamal encryption, 155, 162, 295, 298
 elliptic curve, 110, 295

Index

discrete logarithm problem, 66
 discriminant, 111
 divisor, 113
 factoring method, *see* ECM
 group law, 112
 method, 57, 64, 68
 principal divisor, 115
 supersingular, 67
 Weierstrass form, 110, 295, 308
 elliptic-curve
 cryptography, *see* ECC
 Diffie–Hellman, *see* ECDH
 digital signature algorithm, *see* ECDSA
 Eratosthenes, 41
 error correction, 236
 exponent
 re-use, 161
 short, 160
 factor base, 53, 54, 109
 factoring
 known bits, 89
 fast exponentiation algorithm, 71
 Fermat
 factoring method, 42
 little theorem, 43, 49
 number, 45, 58, 75
 FFLAS, 288
 Fibonacci number, 46
 FLAME, 198, 219, 317
 floating-point, 242
 Floyd’s cycle-finding, 108
 Flynn’s taxonomy, 230
 footnote, xii, 18, 22, 26, 68, 123, 124, 131,
 132, 186–188, 198, 209, 211, 255, 257,
 258, 268, 270, 271, 278, 315, 318, 321,
 322
 FPGA, 316, 318
 FPLLL, 20
 FPyLLL, 24
 function field sieve, 328
 fused multiply and add, 257
 Gaussian heuristic, 20–22, 24, 27, 28, 31
 genus 1, *see* elliptic curve
 genus 2, 238
 geometric series assumption, 21
 tail-adapted, 21
 GHS attack, 326
 GLV, 301
 GMP, 251
 GNU multiple precision arithmetic library, *see*
 GMP

- GnuTLS, 160
- Gram–Schmidt
 - basis, 18
 - length, 19, 32
 - orthogonalisation, 17
 - vector, 23, 26, 27, 31, 33, 39
- graphics processing unit, 324
- hash function
 - chaining value, 183
 - compression function, 183
 - cryptographic hash function, 182
 - dilemma, 183
 - MD5, *see* MD5
 - Merkle–Damgård framework, 183
 - SHA-1, *see* SHA-1
 - SHA-2, *see* SHA-2
 - SHA-3, *see* SHA-3
 - standards, 183
- Hasse
 - interval, 65, 68
 - theorem, 64
- Hensel lifting, 108, 121
- Hermite
 - constant, 17
 - factor, 19, 22
 - normal form, 25
 - regime, 22, 30
 - root factor, 34
- HKZ, 18, 21, 26
- hybrid encryption, 149
- ICM, 109, 312
- identity based encryption, 327
- IKE, 154, 156–158, 160, 173, 202
- index calculus method, *see* ICM
- Internet key-exchange, *see* IKE
- Internet protocol security, *see* IPsec
- IPsec, 140, 154, 155, 157, 162, 165, 170, 202
 - handshake, 160
 - IKE, 152, 156
- keccak, *see* SHA-3
- L-function, 53, 57, 66, 69, 107
- Lamport signatures, 332
- Las Vegas algorithm, 68
- lattice, 72
 - full rank, 72
- law of quadratic reciprocity, 42
- lazy butterfly, 266
- Learning-With-Errors problem, 330
- Legendre symbol, 56, 63
- Lenstra–Lenstra–Lovász reduction, *see* LLL
- Libreswan, 165
- linear algebra, 109
- LIP, 251
- LLL, 15, 20, 25, 26, 30, 31, 38, 78, 82, 330
- LUC, 122, 298
- McEliece cryptosystem, 331
- MD5, 183, 212, 317
 - collision attack, 212
- Menezes–Okamoto–Vanstone attack, *see* MOV attack
- Merkle trees, 332
- Mersenne number
 - generalised, 238–242
 - special arithmetic, 247–250
- mesh sorting, 324
- meta-reduction non-sense, 78
- MIMD, 230
- Mingle Instruction Single Data, *see* SISD
- MISD, 230
- modular multiplication, 223–250
 - Montgomery multiplication, *see* Montgomery multiplication
 - parallelism, 229–234
 - Quisquater multiplication, *see* Quisquater multiplication
 - scaled modulus, *see* scaled modulus
 - tail tailoring, *see* tail tailoring
- modulus
 - composite, 163
- Monte Carlo algorithm, 43
- Montgomery
 - μ , 224
 - form, 224
 - interleaved multiplication, 225
 - multiplication, 224–225
 - reduction, 224
 - special, 241
- Moore’s law, 230
- MOV attack, 116
- MPC-in-the-Head, 332
- MPQS, 319, 320, 332
- MQ-based cryptography, 331
- Multiple Instruction Multiple Data, *see* MIMD
- Multiple Instruction Single Data, *see* MISD
- multiplication
 - FFT, 271
 - FFT, truncated, 267
 - Karatsuba, 235, 247, 271
 - multi-modular, 272
 - Schönhage–Strassen, 271
 - schoolbook, 271

- National Institute of Standards and Technology, *see* NIST
 National Security Agency, *see* NSA
 NFS, 57, 58, 75, 76, 169, 311, 312, 321, 322, 328
 general, 61, 332
 tower, 329
 NIST, 142, 143, 145, 157, 162, 172, 238, 313, 315, 317, 318, 330–332
 curves, 172, 173
 P-256, 172, 175
 primes, 239
 SP800-56A, 162
 nonce
 predicted, 177
 repeated, 178
 Nostradamus attack, 203, 205
 NSA, 153, 171, 176
 suite B, 171
 NTL, 251
 number field sieve, *see* NFS
 number theory library, *see* NTL, *see* NTL
 oil-and-vinegar systems, 332
 OpenSSH, 158
 OpenSSL, 142, 146–148, 151, 153, 160, 161, 166
 Openswan, 165
 pairing, 67
 cryptography, 326
 embedding degree, 116
 PGP, 201
 pigeon-hole principle, 183
 Pohlig–Hellman algorithm, 107, 161, 294
 Pollard
 $p - 1$ method, 43, 62, 64, 66, 76
 rho method, 43, 75, 76, 108, 294, 295
 polynomial
 time, 53, 69, 70, 74, 77
 PRAC algorithm, 300
 pre-image resistance, 182
 second pre-image resistance, 182
 prime
 distinct, 175
 fixed, 159
 generation, 141
 hard-coded, 158
 length, 157
 nearby, 168
 probable, 46
 probable, strong, 46
 proving, 46
 pseudo, 46, 70, 76
 pseudo, strong, 46, 70, 76
 safe, 161
 size, 143
 standardised, 158
 structure, 142
 testing, 45
 protocol
 cross attack, 167
 public key, 47
 cipher, 48, 50
 repeated, 175
 quadratic
 form, 68
 polynomial, 56
 residue, 42, 49, 51, 53
 sieve, 56–58, 76
 quantum computer, 77, 329
 Quentin Tarantino, 8
 Quisquater multiplication, 229
 radix-2^w representation, 223
 random number generator, *see* RNG
 reduction
 Hermite–Korkine–Zolotarev, *see* HKZ
 slide, 19, 20
 sloppy, 244–247
 relation generation, 109
 representation
 redundant, 243
 Riemann hypothesis
 extended, 68
 Rijndael, 317
 Rivest–Shamir–Adleman, *see* RSA
 RNG
 vulnerabilities, 146
 RSA, 41–43, 45, 47–49, 66, 67, 69–72, 74, 140, 314, 318, 325
 arithmetic, 225–237
 Boneh–Durfee attack, *see* Boneh–Durfee attack
 broadcast attack, 86
 certifying, 91
 challenge, 320, 325
 challenge numbers, 62
 common factors, 147
 in the wild, 141–154
 key generation, 141
 predictable bits, 148
 problem, 73
 repeated moduli, 145
 RSA-129, 320, 321

- security, 79
- shared bits, 148
- small secret exponent, 95
- Wiener's attack, *see* Wiener's attack
- Sage, 20, 24
- SAT problem, 331
- scaled modulus, 228
- Schnorr subgroups, 294
- Schoof–Elkies–Atkin method, 112
- SEA, *see* Schoof–Elkies–Atkin method
- secret key
 - predictable, 177
 - small, 176
- secure shell, *see* SSH
- secure sockets layer, *see* SSL
- SHA-1, 183, 317, 318
- SHA-2, 183, 318
- SHA-256, 318
- SHA-3, 183, 318
- SHARK, 324
- Shor's algorithm, 329
- shortest-vector problem, 330
- sieve of Eratosthenes, 56
- signature padding, 152
- SIMD, 230
- Single Instruction Multiple Data, *see* SIMD
- SISD, 230
- size of an elliptic curve modulo p , 63
- smooth integer, 51, 53, 66, 76
- SNFS
 - trapdoor, 169
- SPHINCS, 332
- SSH, 140, 141, 146–150, 154–156, 158, 162, 166, 168, 173–175, 178, 180, 202
 - group exchange specification, 160
 - handshake, 146
 - host, 175, 178, 179
 - host keys, 143
 - hosts, 148
 - IPv4 hosts, 146
 - RSA keys, 148
 - server, 158, 160, 165
 - v2, 157
- SSL, 150, 151, 153, 154, 174
 - 3.0, 153
 - v2, 150, 151
 - v3, 154
- SSLey, 164
- subgroup, 166
- tail tailoring, 229
- Tate
 - pairing, 116
- TLS, 140, 144, 150, 151, 153, 154, 157, 158, 160, 162, 173, 174, 202
 - 1.0, 149, 154
 - 1.1, 141
 - 1.2, 141, 150, 155, 156, 165
 - 1.3, 154–156, 158, 160, 170
 - certificate, 144
 - handshake, 145
 - root certificate, 144
 - secret, 150
- transport layer security, *see* TLS
- trial division, 42, 43, 53, 55, 56, 67, 68, 75
- TWINKLE, 62, 323
- TWIRL, 324
- unique shortest vector problem, 29
- Weil
 - descent, 326
 - pairing, 67, 116
 - restriction, 128
- wheel, 42
- Wiener's attack, 95, 97
- wooping, 236
- word size, 224
- word-slicing, 233
- X.509 certificate, 317
- XTR, 123, 293, 327, 328