

Index

- abelian group, 240, 380
 - free, 380
- addition
 - divisor, 382
 - integer, 32
 - jacobian, 382
 - matrix, 269
 - polynomial, 248
 - ring, 242
 - vector, 267
- additive stream cipher, 12, 183
- ADH attack, 417
- Advanced Encryption Standard, 171
- adversary, 4
- AES, 171
- affine boolean function, 199
- affine cipher, 8
- affine plane, 296
- affine point, 296, 484
- agreement theorem, 191
- algebraic closure, 260, 338, 370, 451
 - of a field, 260, 337
- algebraic integer, 256, 292, 359
- algebraic normal form, 199
- algebraic number theory, 367
- algebraically closed field, 248, 260
- algorithm
 - baby-step, giant-step, 121
 - Berlekamp polynomial factoring, 288
 - Berlekamp square root, 72
 - Buchberger, 284
 - Cantor, 407
 - Cantor–Koblitz, 407
 - Cantor–Zassenhaus, 288
 - Cornacchia, 357
 - division, 38
 - Duursma–Lee, 474
 - euclidean, 38, 252
 - extended euclidean, 39, 246
 - Fermat, 56
 - Gram–Schmidt, 537
 - Lenstra–Lenstra–Lovász, 537
 - meet-in-the-middle, 121
 - Miller, 457
 - Miller–Rabin, 61
 - Montgomery multiplication, 488
 - Pohlig–Hellman, 115
 - Pollard discrete logarithm, 123
 - Pollard factoring, 67
 - Pollard rho factoring, 124
 - Schoof point-counting, 74, 343, 367
 - Schoof square–root, 74
 - Shanks, 121
 - Tonelli–Shanks, 70
- aliasing, 275
- alphabet, 2
 - hexadecimal, 176
- anomalous elliptic curve, 312, 365, 366
- architecture, 475
- associativity
 - group operation, 239
 - integer addition, 32
 - integer multiplication, 34
 - point addition, 311, 351
 - scalar multiplication, 268
- asymmetric bilinear pairing, 451
- asymmetric keyed signature, 520
- asymmetric-key cryptosystem, 3
- asymptotic behavior, 130
- ate pairing, 506
 - twisted, 481
- Atkins procedure, 346
- attack
 - ADH, 417
 - brute-force, 107
 - collision, 225
 - correlation, 197, 207
 - differential analysis, 176
 - direct, 3
 - flooding, 222
 - frequency–analysis, 30
 - Frey–Rück, 412, 416, 449
 - impersonation, 114
 - implementation, 18
 - known-plaintext, 191
 - linear analysis, 177

577 **Index**

- linear-complexity, 18, 191
- man-in-the-middle, 511
- meet-in-the-middle, 15, 171
- MOV, 449
- replay, 510
- side-channel, 6
- authentication, 1, 21, 23, 218
- authentication signature
 - Lamport, 522
- autocorrelation function, 213
- autokey cipher, 11, 30

- baby-step, giant-step algorithm, 121
- Barreto–Naehrig elliptic curve, 465
- basis, 491
 - complementary, 500
 - lattice, 528
 - normal, 494
 - orthogonal, 537
 - polynomial, 492
- BCH bound, 551
- BCH code, 551
- BCH distance, 551
- Berlekamp multiplier, 501
- Berlekamp polynomial factoring algorithm, 288
- Berlekamp square-root algorithm, 72, 79
- Berlekamp–Massey algorithm, 216
- Beth–Piper keystream, 197
- Bézout identity, 39, 253, 503
- Bézout polynomial, 253
- Bézout theorem, 29, 283, 383, 388
- bijection function, 112
- bilinear form, 530
- bilinear map
 - asymmetric, 423
 - symmetric, 423
- bilinear pairing, 425
 - nondegenerate, 423
 - Tate, 451
 - Weil, 460
- binary field, 244, 246
- binomial theorem, 245
- bipolar alphabet, 212
- biprime, 36, 67, 83
- biprime cryptography, 83
- birthday surprise, 133, 226, 235
- bivariate monomial, 282
- bivariate polynomial, 281, 294
- bivariate rational function, 282
- Blahut’s theorem, 193
- block, 160
 - ciphertext, 160
 - plaintext, 160
- block cipher, 2, 160
- block decryptor, 3
- block encryptor, 3
- block substitution cipher, 9
- boolean function, 199, 215
 - affine, 199
 - linear, 199
 - nonlinear, 199, 200
 - normal form, 199
- bound
 - BCH, 551
 - Hasse, 308
 - Hasse–Weil, 309, 450
 - Singleton, 549
- Brent–Zimmermann polynomial, 507
- Buchberger algorithm, 284

- calculus, 127
- canonical representative, 34, 374, 452
 - coordinate ring, 286, 442
 - finite field, 255
 - integer ring, 47, 285
 - jacobian, 394
 - prime field, 41
 - range of a pairing, 452
 - torsion points of elliptic curve, 443
- Cantor algorithm, 407
- Cantor reduction, 402
- Cantor–Koblitz algorithm, 407
- Cantor–Zassenhaus algorithm, 288
- cardinality, 35
- Carmichael integer, 57
- Cayley–Hamilton theorem, 271, 341
- cell tessellation, 530
- cellular array, 497
- central limit theorem, 209
- certification authority, 22
- challenge message, 511
- challenge–response sequence, 511
- characteristic of a field, 42, 245
- characteristic equation of Frobenius, 340
- characteristic polynomial of a matrix, 271, 292
- Chebychev’s inequality, 142
- check matrix, 549
- check polynomial, 551
- chinese remainder theorem, 40, 115, 399
 - for integers, 40
 - for polynomials, 253
- cipher
 - additive stream, 12
 - affine, 8, 28
 - autokey, 11
 - block, 2, 160
 - block substitution, 9
 - cascade, 14
 - Hill, 9
 - iterated, 14
 - permutation, 10
 - privacy, 12

578 **Index**

- cipher (*cont.*)
 - shift, 8
 - stream, 2, 182
 - substitution, 8
 - Vigenère, 9
- cipherspace, 3
- cipherstream, 12
- ciphertext, 3, 5
 - block, 160
 - message, 160
- circulant matrix, 528, 546
- claimant, 510
- class number, 357, 361
- closest-vector problem, 535, 547
- code, 548
 - BCH, 551
 - data compaction, 150
 - fixed-length block, 150
 - Gold, 213
 - Goppa, 552
 - Huffman, 151
 - linear, 548
 - maximal-distance, 549
 - Reed–Solomon, 525, 550
 - tree, 150
 - variable-length block, 150
- codeword, 548
- coefficient, 247
 - bivariate, 282
- collision attack, 225
- collision-free hash function, strongly, 224
- common factor, 34
- commutative property, 240
- commutative ring, 242
- commutativity
 - integer addition, 32
 - integer multiplication, 34
- complementary basis, 500
- complex field, 244
- complex multiplication
 - in an endomorphism ring, 335
 - in a number field, 355
 - of an elliptic curve, 75, 335, 355, 468
- complexity
 - discrete log, 129
 - exponential, 20
 - polynomial, 20
 - subexponential, 20, 130
- complexity theory, 19
- component, of a vector, 267
- componentwise product, 268
- composite integer, 35
- composite polynomial, 248
- computational secrecy, 6
- conditional probability, 136
- confusion, 139
- congruent square, 96
- conjecture
 - Goldbach, 79
 - twin-prime, 79
- conjugate, 376
 - coordinate ring, 376
 - extension field, 259, 377
- convolution, cyclic, 273
- convolution theorem, 201, 273
- coordinate ring, 286, 389
- coprime
 - integers, 35
 - polynomials, 250
- Cornacchia algorithm, 357, 366
- correlation, 212
- correlation attack, 197, 207
- coset, 241, 285, 286, 290
 - left, 241
 - right, 241
- covertiness, 1
- criterion, Euler, 43, 69, 71, 73
- cross-correlation function, 213
- cryptanalysis, elliptic curve, 294
- cryptanalyst, 2
- cryptography, 2
 - asymmetric-key, 3
 - biprime, 83
 - elliptic curve, 294
 - hyperelliptic curve, 411
 - lattice-based, 543
 - public-key, 13, 82
 - secret-key, 14
 - symmetric-key, 3
- cryptology, 2
- cryptosystem, 1
 - Ajtai–Dwork, 544
 - asymmetric-key, 3
 - Elgamal, 110
 - elliptic curve, 294
 - knapsack, 20, 102
 - Massey–Omura, 113
 - Merkle–Hellman, 102
 - NTRU, 557
 - Rabin, 99
 - RSA, 83
 - symmetric-key, 3
- cryptspace, 3
- curve
 - elliptic, 296
 - hyperelliptic, 369
 - plane, 295
- cycle, 239
- cyclic convolution, 273
- cyclic group, 33, 239
- cyclic subgroup, 33
- cyclotomic field, 256
- cyclotomic polynomial, 264, 287

579 **Index**

- data compaction, 150
- data confusion, 139, 158, 163
- data diffusion, 139, 158, 163
- Data Encryption Standard, 164
- datastream, 12
- dataword, 549
- deBruijn sequence, 195, 211, 215
- decoding, 552
- degree, 282, 381
 - bivariate polynomial, 282
 - extension field, 256
 - number field, 96, 256
 - of divisor, 381
 - of embedding, 453
 - of extension field, 256
 - of nonlinearity, 200
- derivative
 - formal, 248
 - partial, 370
- DES, 164
 - double, 170
 - triple, 170
- determinant
 - of a lattice, 529
 - of a matrix, 270
- differential cryptanalysis, 176
- Diffie–Hellman key exchange, 107, 294, 412
 - elliptic curve, 322
 - hyperelliptic curve, 412
 - pairing-based, 426
- diffusion, 139
- Digital Signature Standard, 236
- Digital Standard Algorithm, 236
- digram, 148
- diophantine equation, 28, 356, 470
- direct attack, 3
- direct product, 241
- direct sum, 241, 433
- Dirichlet theorem, 55
- discrete logarithm, 109
- discrete-log problem, 109, 554
- discriminant
 - complex multiplication, 468
 - of an elliptic curve, 297, 356
 - of polynomial, 297
 - of quadratic field, 359
- distance
 - euclidean, 269
 - Hamming, 269, 549
 - Kullback, 138
 - minimum, 549
 - unicity, 145
- distortion map, 448, 478
- distributivity, 268
 - in a ring, 242
 - scalar multiplication, 268
 - vector addition, 268
- divide
 - integer, 38
 - polynomial, 247
- division, 41
 - bivariate polynomial, 282
 - modular, 41
 - of integers, 34
 - of polynomials, 248
 - with remainder, 34
- division algorithm, 38
 - for integers, 38
 - for polynomials, 248
- divisor, 379, 392
 - degree of, 380
 - effective, 381
 - of a line, 403
 - principal, 385, 447
 - reduced, 382
 - semireduced, 382
 - with degree zero, 381
- divisor class, 287, 391, 406
 - group, 287, 391
- Dixon factoring, 90
- double DES, 170
- double-and-add method, 482
- doubly periodic, 353
- dual bases, 500
- dual lattice, 555
- Duursma–Lee algorithm, 474
- Duursma–Lee enhancement, 476
- eavesdropper, 4, 510
- Edwards polynomial, 366, 506
- Edwards representation, 366, 485
- effective divisor, 381
- eigenvalue, of a matrix, 271
- Eisenstein coefficient, 354
- element, primitive, 111, 186
- Elgamal cryptosystem, 110
- Elgamal signature scheme, 222
- Elkies procedure, 346
- elliptic curve, 296, 308, 365, 370
 - anomalous, 312, 365
 - Barreto–Naehrig, 465
 - Edwards representation, 366
 - Freeman, 470
 - friendly, 464
 - Koblitz, 319, 364
 - Legendre form, 298
 - ordinary, 312, 315
 - pairing-friendly, 473
 - principal divisor, 385
 - supersingular, 312
 - twist of, 309
 - Weierstrass form, 315

- elliptic integral, 366
- elliptic polynomial
 - short Weierstrass form, 297
 - Weierstrass form, 296
- embedding degree, 437, 451, 453
 - of elliptic curve, 437
 - supersingular curve, 437
- encryption
 - block, 3
 - state-dependent, 182
- Encryption Standard
 - Advanced, 178
 - Data, 164
- endomorphism, 333, 339
 - elliptic curve, 333, 365
 - Frobenius, 339
 - ring, 335
- enhancement, Duursma–Lee, 476
- entropy, 137, 149
- equation of a line
 - vertical, 453
- equivalence class, 34, 41, 255, 285, 353
 - bivariate polynomial, 374
 - coordinate ring, 374
 - integers, 34
 - polynomial, 249
- Eratosthenes sieve, 77
- eta pairing, 506
- euclidean algorithm, 38
 - extended, 39, 83, 252
 - for euclidean domain, 252
 - for integers, 38
 - for polynomials, 252
- euclidean distance, 269
 - on a lattice, 529, 535
- euclidean domain, 252
- euclidean norm, of a lattice, 529
- euclidean weight, 268
- Euler criterion, 43, 60, 69, 71, 73
- Euler theorem, 36, 84
- evaluation, 283
 - of a bivariate polynomial, 282
 - of a univariate polynomial, 251
 - on a divisor, 381
- exponential complexity, 20
- exponentiation, square-and-multiply, 85
- extended euclidean algorithm, 39, 83
 - for integers, 39
 - for polynomials, 252
- extension field, 255
 - finite degree, 256
 - finite field, 257
 - quadratic, 257
- exterior corner, 284
- factor, 248
 - bivariate, 282
 - integer, 34
 - polynomial, 248
- factor base, 127
- factoring
 - elliptic curve method, 81
 - integer, 65, 89
 - polynomial, 247
- factoring algorithm
 - Dixon, 90
 - Fermat, 79
 - number field sieve, 96
 - Pollard $p - 1$, 67
 - Pollard rho, 133
 - quadratic sieve, 91
- false key, 145
- false prime, 57
- Feige–Fiat–Shamir identification, 513
- Feistel network, 162
- Feistel round, 162
- Fermat factoring, 79
- Fermat primality testing, 57
- Fermat two-squares theorem, 47, 79
- Fermat’s little theorem, 36, 56, 78, 246
- Fibonacci identity, 78
- Fibonacci sequence, 191
- field, 41
 - algebraically closed, 260
 - binary, 246
 - closure, 260, 370
 - complex, 244, 255
 - cyclotomic, 256
 - extension, 255
 - finite, 244
 - Galois, 244
 - ground, 255
 - number, 96, 256
 - prime, 42, 245
 - rational, 244
 - real, 96, 244, 248, 256
 - ternary, 246
- fingerprinting, 23
- finite field, 244
- finite group, 32, 239
- finite-dimensional vector space, 269
- finite-state machine, 182
- first-order Markov source, 136
- fixed-length block code, 150
- flooding attack, 222
- footprint, 284
- formal derivative, 248, 291, 306
 - partial, 370
- formally intractable, 20
- forward problem, 19
- Fourier transform, 193, 201, 272, 291, 551
 - inverse, 273
- fractional ideal, 361, 362
- free abelian group, 380
- Frey–Rück attack, 412, 416, 449

581 **Index**

- Frobenius eigenspace, 443, 452, 478
 Frobenius endomorphism, 339
 Frobenius map, 263, 337
 of a field element, 263
 on a curve, 339, 365
 Frobenius trace, 308, 312
 function
 bijection, 112
 Miller, 452
 one-way, 112
 totient, 35
 trapdoor, 112
 function field, 375
- Galois field, 244
 Gauss's lemma, 48
 gaussian integer, 97, 256
 gaussian rational, 97, 256, 359
 Geffe keystream, 197
 generator
 of a group, 239
 of an ideal, 249
 generator matrix
 of a code, 549
 of a lattice, 528, 555
 generator polynomial, 551
 genus, 295, 367, 369
 elliptic curve, 296
 hyperelliptic curve, 369
 Gibbs inequality, 138
 Gibson hash function, 229, 236
 Gold code, 213
 Goldbach conjecture, 79
 golden ratio, 257
 Goppa code, 552
 graded order, 283
 Gram–Schmidt orthogonalization, 537
 greatest common divisor, 35, 38
 of divisors, 381, 401
 of integers, 35
 of polynomials, 251
 ground field, 255
 group, 32, 238, 261
 abelian, 240
 cyclic, 33, 239
 finite, 32
 free, 380
 nonabelian, 240
 quotient, 285
 torsion, 241, 434
 group identity element, 32, 290
 GSM stream cipher, 206, 215, 217
 Guillou–Quisquater identification, 513
- Hadamard inequality, 530
 Hamming distance, 269, 549
 between codewords, 549
 between functions, 200
 between vectors, 200
 Hamming sphere, 552
 Hamming weight, 193, 269, 549
 between codewords, 549
 hash construction, Merkle–Damgaard, 227
 hash function, 23, 223
 Chaum, van Heijst, Pfitzmann, 229
 collision free, 224
 Gibson, 229, 236
 keyed, 223
 preimage resistant, 224
 unkeyed, 223
 hashing, 23, 224
 Hasse bound, 308
 Hasse theorem, 331
 Hasse–Weil bound, 309, 315, 367, 450
 Hasse–Weil interval for jacobian, 413, 420
 Hasse–Weil theorem, 309
 heft, of a matrix, 190, 271, 549
 Hermite constant, 534
 Hermite theorem, 533
 Hermite's inequality, 533, 535
 hexadecimal alphabet, 176, 418
 Hilbert class polynomial, 358, 362
 Hill cipher, 9
 homogeneous form, 378
 homomorphism, 333
 Horner's rule, 118, 471, 496
 Huffman code, 151
 hyperelliptic curve, 369, 411
 genus one, 392
 hyperelliptic involution, 420
 hyperelliptic polynomial, 371
- ideal, 243
 fractional, 362
 of bivariate polynomials, 284
 of polynomials, 249
 prime, 97, 243
 proper, 243
 ideal class group, 287, 362
 identification, 21, 218, 510
 zero-knowledge, 220
 identification protocol, 510
 Feige–Fiat–Shamir, 518
 Fiat–Shamir, 516
 Guillou–Quisquater, 519
 Okamoto, 515
 Schnorr, 513
 identification signature
 Guillou–Quisquater, 523
 Schnorr, 521
 identity element
 group, 32, 239, 286
 integer addition, 32
 ring, 242
 identity theft, 22
 imaginary quadratic number field, 75, 257, 359

582 **Index**

- impersonation attack, 114
- indeterminate, 247, 282
 - bivariate, 282
- index calculus, 127, 294, 347
- indicator function, 531
- inequality
 - Chebyshev, 142
 - Hadamard, 530
 - Hermite, 533, 535
 - Mordell, 535
- inert, 47
- information-theoretic secrecy, 5, 139
- inner product, 268, 529
- integer
 - algebraic, 256, 292
 - biprime, 67
 - Carmichael, 57
 - composite, 35
 - gaussian, 256
 - number field, 292
 - prime, 35
 - smooth, 97
- integer factoring, 89
- intersection, of plane curves, 283
- intractable, 19
- inverse, 270
 - group, 32, 239
 - matrix, 270
 - problem, 19
 - ring, 242, 291
- inverse Fourier transform, 273
- irreducible polynomial, 371
 - bivariate, 282
 - existence, 279
 - hyperelliptic, 370
 - monovariate, 276
- isogeny, 333
- isomorphism
 - of elliptic curves, 298, 334
 - of finite fields, 280
 - of groups, 241, 434
- iterated cipher, 14

- j-invariant, 298, 309, 358
- Jacobi sums, 417, 421
- Jacobi symbol, 51, 60
- jacobian, 382, 391
 - as quotient group, 390
 - as reduced divisors, 392
- jacobian addition, 382
- jacobian class group, 287
- jacobian representation, 485
- Joux key exchange, 427, 471

- Kerckhoff's principle, 30
- kernel, of degree map, 381
- key, 3
 - asymmetric, 3
 - shadow, 524
 - symmetric, 3
- key exchange
 - Diffie–Hellman, 107, 294
 - Joux, 427
 - tripartite, 133
- key sequence, 211
- Key's theorem, 201, 216
- keyspace, 3
- keystream, 12, 184
 - Beth–Piper, 197
 - cryptographic system, 184
 - Geffe, 197
 - linear, 185
 - majority-clocking, 198
 - pseudorandom, 184
 - self-shrinking, 216
 - shrinking, 197
- knapsack cryptosystem, 20, 102, 547
- known ciphertext, 16
 - attack, 17
- known plaintext, 16
- Koblitz elliptic curve, 319, 364
- Korselt theorem, 57
- Kronecker delta, 500
 - function, 500
- Kullback distance, 138

- Lagrange interpolation, 397
- Lagrange theorem, 33, 240
- Lamport identification protocol, 525
- language, 2
- lattice, 353, 528, 530
 - reduction, 536
- leading coefficient, 247, 248
- leading index, 247
- least common multiple, 35
 - integer, 35
 - polynomial, 251
- left coset, 241, 290
- left inverse, 242, 291
- Legendre
 - form, 298
 - symbol, 44, 69
- lemma, Gauss, 48
- Lenstra–Lenstra–Lovász algorithm, 537
- line at infinity, 379
- linear algebra, 269
- linear boolean function, 199
- linear code, 548
- linear combination, 269
- linear complexity, 191, 201, 215
 - attack, 18, 190
- linear recursion, 12, 191
- linear-feedback shift register, 12
- linearly dependent, 269

583 **Index**

- linearly independent, 269, 271, 528
 logarithm, finite-field, 110, 496
- m*-sequence, 214
m-torsion point, 339
 majority-clocking keystream, 198
 man-in-the-middle attack, 511
 marginal probability, 136
 Markov source, 136, 156
 Massey's theorem, 192
 Massey–Omura cryptosystem, 113
 matrix, 270
 circulant, 546
 inverse, 270
 permutation, 11
 square, 270
 Toeplitz, 190
 transpose, 269
 vandermonde, 550
 matrix heft, 271, 549
 matrix rank, 271, 549
 maximal-distance code, 549
 maximal-length sequence, 216
 meet-in-the-middle
 algorithm, 121
 attack, 171
 Merkle–Damgaard hash construction, 227
 Merkle–Hellman knapsack, 102
 Mersenne prime, 419, 507
 message
 ciphertext, 3
 plaintext, 2
 message digest, 23, 219, 223
 message hash, 23
 Miller algorithm, 454, 457
 Miller function, 452
 Miller reduction, 458
 Miller–Rabin algorithm, 61
 minimal basis, 284
 minimal polynomial, 280
 minimum distance, 549
 of a code, 549
 of a lattice, 529
 Minkowski theorem, 531, 555
 Möbius function, 276
 Möbius inversion formula, 277, 291
 modular division, 41
 modular equivalence, 285
 modular reduction, 285
 modulation property, 274
 monic polynomial, 248
 bivariate, 283
 monic rational function, 388
 monoid, 240, 290
 monomial
 bivariate, 282
 univariate, 247
- Montgomery multiplication, 488, 505
 Mordell's inequality, 535
 morphism, 333
 MOV attack, 449
 multinomial coefficient, 157
 multiplication
 complex, 255
 matrix, 269
 polynomial, 248
 multiplier
 Berlekamp, 501
 bit-serial, 504
 dual-bases, 504
 Montgomery, 488
 Omura–Massey, 498
 parallel, 475
 quarter-square, 505
 serial, 475
mutual information, 155
 Mumford transform, 397
- nat, 137
 natural language, 2
 nondeterministic polynomial, 20
 nonlinear combination generator, 202
 nonlinear order, 199
 nonlinear output, 201
 nonlinear recursion, 194
 nonresidue
 quadratic, 42
 nonsingular polynomial, 295
 elliptic, 295
 norm, 376
 euclidean domain, 252
 in a coordinate ring, 375, 420
 of a divisor, 381
 of a lattice point, 529
 of a matrix, 270
 of a vector, 268, 538
 normal basis, 494
 optimal, 495
 normal form, 199
 number field, 96, 256, 292
 imaginary quadratic, 257, 355
 quadratic, 257
 real quadratic, 257
 number-field sieve, 67, 91, 96, 131
 number ring, 256
 number theory, 32
- Okamoto identification protocol, 513
 Omura–Massey multiplier, 498
 one-time pad, 4, 30, 140, 153, 158, 183
 one-way function, 13, 112, 134
 trapdoor, 84, 112
 opposite, of a point, 373, 382, 395
 optimal normal basis, 495
 orbit, 33

- order, 33, 239
 - in a number field, 362
 - in ring theory, 362
 - nonlinear, 199
 - of a boolean term, 199
 - of a group, 33, 239
 - of a pole, 384
 - of a zero, 384
 - of an element, 33
- ordinary elliptic curve, 312, 315
- ordinary point, 373, 395, 419
- origin
 - of lattice, 528
 - vector space, 268
- orthogonal, 268, 529, 530
 - basis, 537
 - complement, 538
- orthogonality defect, 530
- ownership protection, 23, 218
- pad, one-time, 4
- pairing, 425
 - ate, 506
 - eta, 506
 - Tate, 451
 - Weil, 460
- pairing-friendly curve, 464
- parallel multiplier, 475
- Pell equation, 470
- perfect secrecy, 4, 5, 107, 157
- period, of cyclic sequence, 185
- permutation, 270
 - cipher, 10
 - group, 240
 - matrix, 11
- Plücker formula, 295
- plaintext
 - block, 160
 - message, 2, 160
- plane
 - affine, 296
 - curve, 294
 - projective, 323
- Pohlig–Hellman algorithm, 115
- point
 - affine, 296, 395
 - at infinity, 296, 484
 - opposite, 373, 382
 - ordinary, 395
 - rational, 298
 - singular, 295
 - special, 373, 382
- point addition, 294
- point counting
 - in extension field, 325
 - in ground field, 343
 - Satoh algorithm, 367
 - Schoof algorithm, 343
- point doubling, 306, 321
- point halving, 365, 368
- point representation, 484
- point tripling, 477, 505
- pole, 383
 - of a rational function, 376, 383
- pollard algorithm
 - discrete logarithm, 123
 - factoring, 67, 133
 - rho factoring, 124, 133
- polynomial
 - Bézout, 253
 - bivariate, 281, 294, 323
 - characteristic, 271
 - check, 551
 - cyclotomic, 263
 - Edwards, 366
 - homogeneous, 323
 - hyperelliptic, 371
 - nonsingular, 295
 - prime, 250
 - primitive, 186, 258
 - quotient, 249
 - remainder, 249
 - singular, 295
 - trivariate, 323
 - univariate, 247
 - Weierstrass, 296
- polynomial addition
 - bivariate, 282
 - univariate, 248
- polynomial basis, 492, 501
- polynomial multiplication
 - bivariate, 281
 - univariate, 248
- polynomial ring, 248
 - bivariate, 284
 - univariate, 247
- practical secrecy, 6
- preimage resistant, 224
- primality testing, 55
- primality testing algorithm, 55
 - Fermat, 57
 - Goldwasser–Kilian–Atkin, 55
 - Miller–Rabin, 59
 - Solovay–Strassen, 59
 - Wilson, 79
- prime field, 42, 244, 245
- prime ideal, 97, 243
- prime integer, 35
 - Mersenne, 419
- prime number theorem, 55
 - Dirichlet, 55
- prime polynomial, 248, 250, 291
- primitive, 508
 - element, 111, 186, 258

- primitive polynomial, 186, 258, 279
 number of, 279
- principal divisor, 387, 447, 461
 elliptic curve, 385
- probability
 conditional, 136
 marginal, 136
- probability space, 138
- product
 componentwise, 268
 inner, 268
- projection
 into subspace, 552
 property, 500
- projective plane, 283, 296, 323
- projective representation, 485
- proper ideal, 243
- protocol, 5, 508
 authentication, 219
 identification, 510
 security, 508
 zero-knowledge, 510
- pseudorandom sequence, 13, 184, 211
- public encryption key, 3
- public key exchange, 3
- public-key cryptography, 82
- quadratic equation, 90
- quadratic nonresidue, 42
- quadratic number field, 257, 359
 imaginary, 75, 257, 359
 real, 257
- quadratic reciprocity, 49
- quadratic residue, 42
- quadratic sieve, 67, 91, 104
- quarter-square multiplier, 505
- quotient, 38
 integer, 38
 polynomial, 249
- quotient group, 241, 285
- quotient ring, 255, 285
- Rabin cryptosystem, 99
- ramify, 47
- rank, of a matrix, 190, 271, 549
- rational field, 244
- rational function, 243, 376, 383
 bivariate, 376, 384, 447
 monic, 243, 385
 univariate, 243
- rational number, 95, 244
 gaussian, 256, 359
- rational point, 298
 elliptic curve, 301, 309
 hyperelliptic curve, 372, 413
- real field, 96, 244, 248, 256
- real quadratic number field, 257
- recursion
 binary, 194
 linear, 191
 nonlinear, 194
- reduced divisor, 382, 392, 395
- reduced Tate pairing, 452
- Reed–Solomon code, 525, 550
- remainder, 38
 integer, 38
 polynomial, 249
- representation
 canonical, 47, 255, 394
 Edwards, 485
 jacobian, 485
 Montgomery, 489
 projective, 485
 signed, 47
- representative
 canonical, 34, 41, 47, 285, 374
 coordinate ring, 286, 374
- residue, 40
 quadratic, 42
- rho algorithm, 124, 133
- right coset, 241
- right inverse, 242, 291
- Rijndael, 179
- ring, 34, 97, 238, 242
 commutative, 242
 coordinate, 374
 of bivariate polynomials, 282
 of univariate polynomials, 248
 quotient, 285
 unital, 242, 282
 with identity, 242
- ring of integers, 242
 of number field, 292
- root, 252
- round, 171
 Feistel, 162
- RSA, 83
- rule, Horner, 471
- S-box, 176
- Satoh algorithm, 367
- scalar, 247
 multiplication, 267
- Schnorr identification protocol, 513, 525
- Schoof algorithm, 343, 367
 square-root, 74
- secrecy, 4, 21, 219
 computational, 6
 information-theoretic, 5, 139
 perfect, 5, 139
 practical, 6
 theoretic, 139
 unconditional, 6

- secret sharing, 508
 security
 of RSA, 84
 perfect, 5
 protocol, 508
 semigroup, 240
 semireduced divisor, 382, 395
 separation principle, 218
 sequence
 deBruijn, 195, 215
 Fibonacci, 191
 key, 211
 maximal, 213
 pseudorandom, 211
 typical, 143
 serial multiplier, 475
 shadow key, 524
 Shanks algorithm, 121, 133
 Shannon–McMillan theorem, 143
 shift cipher, 8
 shift register, 185
 linear-feedback, 12
 shift-register sequence, 185
 linear, 185
 maximal, 186
 nonlinear output, 200
 shortest-basis problem, 536
 shortest-vector problem, 535, 547
 shrinking keystream, 197
 side-channel attack, 6
 sieve
 Eratosthenes, 77
 number-field, 91, 96
 quadratic, 91, 104
 signature, 21
 Elgamal, 222, 236
 RSA, 221
 Schnorr identification, 521
 signed representation, 47
 Singleton bound, 549
 singular point, 295
 singular polynomial, 295
 smooth curve, 295
 smooth integer, 97, 106, 127, 294
 Solovay–Strassen algorithm, 59
 span, a vector space, 269
 special point, 373, 382, 395
 sphere packing, 530
 lattice, 530
 split, 47
 square matrix, 270
 square root
 mod a biprime, 28, 64
 prime field, 69
 square-root algorithm
 Berlekamp, 72
 Schoof, 74
 Tonelli–Shanks, 70
 standard cell, 530
 state vector, 182
 steganography, 25
 Stein’s recursion, 78
 Stirling’s approximation, 157
 stream cipher, 2, 181, 182
 additive, 183
 GSM, 215
 subexponential complexity, 130
 subfield, 244
 prime, 281
 subgroup, 33
 cyclic, 33, 239
 sublattice, 529
 subring, 243
 subset-sum problem, 102
 subspace, vector, 268
 substitution box, 167
 substitution cipher, 8
 subtraction, integer, 32
 superincreasing, 103
 supersingular elliptic curve, 312, 450
 in extension field, 314
 in prime field, 313
 support, 381
 of divisor, 381
 symbol
 Jacobi, 51
 Legendre, 44
 symmetric-key cipher, 160
 symmetric-key cryptosystem, 3

 Tate pairing, 451
 asymmetric, 451
 reduced, 452
 Tate tower, 472
 term, bivariate, 282
 ternary field, 246
 tessellation, 530
 theorem
 agreement, 191
 Bézout, 283, 383, 388
 binomial, 245
 Blahut, 193
 Cayley–Hamilton, 271, 341
 chinese remainder, 40, 115, 253
 convolution, 201
 Dirichlet, 55
 Fermat two-squares, 47
 Fermat’s little, 36
 Hasse, 331
 Hasse–Weil, 309
 Hermite, 533
 Key’s, 201, 216
 Korselt, 57
 Lagrange, 33, 240

587 **Index**

- Massey, 192
- Minkowski, 531
- prime number, 55
- quadratic reciprocity, 49
- Riemann–Roch, 296
- Shannon–McMillan, 143
- torsion structure, 442
- unique factorization, 66, 250
- Weil reciprocity, 390
- Toeplitz matrix, 190
- Tonelli–Shanks algorithm, 70
- torsion group, 241, 434
- torsion points, 241, 339, 433, 444, 461
 - of elliptic curve, 452
- torsion structure theorem, 442
- torus, 352, 367
 - complex, 352
 - discrete, 340
 - real, 352
- total degree, 282
- totient function, 35, 83, 89, 262, 279, 291
- trace
 - binary, 318, 500
 - Frobenius, 308, 312
 - of a field element, 259, 500, 505
 - of a matrix, 270
 - on elliptic curve, 365, 436
- transform, Fourier, 193
- translation property, 274
- transpose, of a matrix, 269
- trapdoor, 84
 - function, 112
- tree code, 150
- trigram, 148
- trinomial, 493, 507
- tripartite key exchange, 133, 426
- triple DES, 170
- triple-and-add method, 483
- trusted authority, 22, 513
- trusted courier, 4
- trustworthy, 1
- truth table, 200
- twin-prime conjecture, 79
- twist, elliptic curve, 309, 356
- two-squares theorem, 47, 79
- typical sequence, 143
- unconditional secrecy, 6
- unicity distance, 145, 151
- unimodular matrix, 529
- unique factorization theorem
 - integer, 66
 - polynomial, 250
- unit, 35
 - of a ring, 243, 291
 - of \mathbb{Z}_n , 35
- unital ring, 282
- univariate polynomial, 247
- validation, 384
- vandermonde matrix, 550
- variable-length block code, 150
- vector, 267, 379
 - addition, 267
- vector space, 267
 - finite-dimensional, 269
- vector subspace, 268, 548
- verifier, 510
- Vigenère cipher, 9, 30
- watermarking, 23
- Weierstrass form, 296, 363
 - short, 297, 300
- Weierstrass function, 353
- weight
 - euclidean, 268
 - Hamming, 193, 268
- Weil divisor, 380
- Weil pairing, 460
- Weil reciprocity, 390, 420
- Wilson primality test, 79
- witness message, 511
- xedni calculus, 347
- zero
 - affine, 324
 - integer, 32
 - of a bivariate polynomial, 282, 384
 - of a polynomial, 252
 - of a rational function, 376, 383
 - of a univariate polynomial, 251
 - projective, 324
- zero knowledge, 510
 - identification, 220
- zero polynomial, 247
 - bivariate, 282
 - coefficient, 247
- zeta function, 330
 - elliptic curve, 330
 - hyperelliptic curve, 413