

- abelian group 266
- absolute value 307
- addition mod P 427
- additive identity 293, 497
- additive inverse 293
- adjoin root 425, 469
- Advanced Encryption Standard (AES) 100, 106, 159
- affine cipher 13
- algorithm xix, 150
- anagram 43, 98
- Arithmetica key exchange 183
- Artin group 185
- ASCII xix
- asymmetric cipher xviii, 160
- asynchronous cipher 99
- Atlantic City algorithm 153
- attack xviii
- authentication 189, 288

- baby-step giant-step 432
- Bell's theorem 187
- bijective 14, 486
- binary search 489
- binomial coefficient 19, 90, 200
- birthday paradox 28, 389
- bit operation 149
- block chaining 105
- block cipher 98, 139
- block interleaver 56
- Blum integer 164
- Blum–Blum–Shub generator 337
- braid group 184
- broadcast attack 170
- brute force attack 3, 14
- bubble sort 490

- cancellation property 294, 298
- cardinality 486
- Carmichael number 256, 258, 374
- cartesian power/product 486
- Cauchy–Schwarz–Bunyakowsky inequality 77, 495
- Cayley–Hamilton theorem 341

- certificate authority 280
- certificate of primality 405
- characteristic equation 341, 347
- characteristic of field 313
- cheating xvi, 279, 280
- Chebycheff's inequality 93
- Chebycheff's theorem 193
- Chinese Remainder Theorem 214
- chosen-plaintext attack xviii, 4, 14, 141, 178
- cipher xvii
- ciphertext xvii, 2
- ciphertext-only attack xviii, 4, 14, 142
- classic block interleaver 56
- classical cipher xviii
- code xvii
- code-book attack 105
- common divisor 110
- common modulus attack 169
- common multiple 110
- common words 32
- complex analysis 452
- complexity 149
- composite function 487
- compositeness test 264
- composition of permutations 48
- compression permutation 102
- conditional probability 27
- confusion 99, 101
- congruence 130, 216
- congruence class 130, 424
- congruential generator 333
- conjugacy problem 184
- contact method 44
- convolution product 237
- coprime 109
- coset 269
- Coxeter group 184
- counting irreducibles 479
- counting primitives 482
- crib xviii, 142
- cryptosystem xvii
- cryptogram 40
- cut deck of cards 54

- cycle 49
- cyclic group 321, 359
- cyclic subgroup 274
- cyclotomic polynomial 318, 348, 349

- Data Encryption Standard (DES)
 - 100, 159
- data integrity xvii
- decomposition into disjoint cycles 50
- decryption xvii
- degree of polynomial 301
- delay attack 288
- DES-cracker 100
- dictionary attack 12, 72
- differential cryptanalysis 101, 105
- diffusion 99, 101
- digital signature xvii
- digrams 33
- Dirichlet's theorem 192
- discrete absolute value 308
- discrete logarithm 136, 161, 171, 431
- disjoint cycle 50
- divides 62, 108, 299
- division algorithm 5, 302
- division ring 293
- divisor 62, 108, 299
- Dixon's algorithm 415

- E-box 103
- e-business 290
- e-money 290
- easy problems 154
- eavesdropper 279
- eigenvalue, eigenvector 341
- Einstein–Podolsky–Rosen effect 187
- elementary row operations 413
- ElGamal cipher 161, 172, 444
- elliptic curve 444, 448
- elliptic curve cipher 162, 173, 179
- encryption xvii
- Enigma xviii
- entanglement 187
- equidistribution of primes 193
- equivalence class 127
- equivalence relation 127
- Eratosthenes' sieve 112, 116
- error term in Prime Number Theorem 197
- Euclid's theorem 190
- Euclidean algorithm 118, 165, 302
- Euclidean ring 307
- Euler criterion 231, 366
- Euler phi-function 109
- Euler product 197
- Euler pseudoprime 260, 375
- Euler theorem 163, 228, 276
- Euler witness 262, 262
- evaluation homomorphism 463
- evaluation map 463
- event 25
- expected value 69
- exponent 137, 274, 277, 318
- exponential runtime 154
- exponentiation algorithm 207
- export regulations 189
- Extended Riemann Hypothesis 198, 256
- extension field 425, 469

- factor base 415, 417, 441
- factorial 19
- factoring into primes 112, 161, 299, 303
- factoring Mersenne numbers 203
- factoring special expressions 201
- fake one-time pad 331
- false witness 256, 257
- fast exponentiation 207
- feedback shift register 335
- Feistel network 101
- Fermat number 398
- Fermat prime 118
- Fermat pseudoprime 256
- Fermat's Little Theorem 200
- field 293, 423, 468
- field extension 426
- final permutation 105
- finite cyclic group 359
- finite field 321
- finite group 269
- Floyd's cycle-detection algorithm 390

- forward search attack 169
- frame check sequence 289
- frequency 31
- Friedman attack 71
- Frobenius automorphism 471

- Galois field 424
- Gaussian elimination 412
- general linear group 500
- Generalized Riemann Hypothesis 198
- generating function trick 89
- generator 274, 359
- gigabyte xix
- greatest common divisor 62, 64, 110, 118
- group 183, 266, 293
- group homomorphism 355
- group of permutations 47
- group of units 293

- hard problems 154
- hash functions 289
- Hensel's lemma 221
- heuristic xix
- Hill Cipher 139
- homogeneous form of elliptic curve 456
- homogenized equation 455
- homomorphic image 357
- homomorphism 355, 462

- ideal in ring 458
- identity element in a group 266
- identity function 487
- identity matrix 499
- identity on elliptic curve 456
- image of homomorphism 356
- impersonation 280
- inclusion-exclusion principle 115
- independent random variables 71
- independent trials 24, 26
- index calculus 136, 441
- index of coincidence 71, 72, 76
- index of subgroup 271
- infinite cyclic group 363
- infinitude of primes 190

- injective 486
- insertion sort 490
- integers mod m 130
- integral domain 294, 298
- inverse function 487
- inverse in a group 266
- inverse matrix 140
- integers mod m 130
- inverse mod P 180
- inverse permutation 49
- irreducible polynomial 299, 305, 479
- isomorphism 357, 462

- Jacobi symbol 244

- Kasiski attack 64
- Kerckhoff's principle xvii, 99
- kernel 356, 462
- key xvii, 2, 331
- key auto-key 99
- key distribution xvii, 12
- key exchange 171
- key generation 166, 175
- key management xvii, 12, 105, 166, 175, 332
- key permutation 102
- key scheduling 102
- key space 72
- knapsack cipher 160
- knapsack problem 161, 176
- knapsack vector 176
- known-plaintext attack xviii, 4, 14, 141
- Kolmogoroff complexity 156

- Lagrange's theorem 269
- lambda function 371
- Las Vegas algorithm 153
- law of large numbers 93, 94
- law of quadratic reciprocity 246
- laws of exponents 272
- least common multiple 60, 62, 110
- left coset 269
- left ideal 461
- left translate 269

- Legendre symbol 244
- length attack 183
- LFSR 335
- liar 256, 257, 262, 382
- limiting frequency 23, 24, 32
- line at infinity 454
- linear cipher 142
- linear combination 413
- linear complexity 157
- linear congruential generator 333
- linear cryptanalysis 101, 105
- linear dependency 412, 416
- linear feedback shift register 157, 335
- linear search 489
- LLL algorithm 179
- logarithmic integral 196
- Lucas–Lehmer test 400
- Lucifer 100

- Möbius inversion 239, 479
- MACs 289
- man-in-the-middle attack 172, 280, 282
- map 484
- MARS 106
- maximal ideal 468
- median-of-three trick 492
- merge sort 491
- Mersenne numbers 203
- Mersenne prime 118
- message authentication (MAC) 288, 289
- Miller–Rabin test 263
- minimum-disclosure proof xvii
- modulus 6
- monic polynomial 301
- monoalphabetic cipher 4, 96
- monoalphabetic substitution cipher 40
- Monte Carlo algorithm 153
- multiple 62, 108, 299
- multiple anagram attack 45
- multiple factors in polynomials 315
- multiple quadratic sieve 422
- multiple-round encryption 60
- multiplication mod P 428
- multiplicative function 234
- multiplicative inverse 7, 122, 142, 163, 293, 428, 499
- naive primality test 116
- Naor–Reingold generator 338
- no-biased algorithm 153
- non-repudiation xvi, 290
- norm 493
- NP-complete 154
- NP-hard 154
- NTRU cipher 179
- Number Field Sieve 169, 411

- oblivious transfer xvi, 284
- one-time pad 10
- oracle 154, 225, 287
- order 51, 137, 274
- ordered pair 485
- orderings 19
- ordinary pseudoprime 257

- P-box 105
- palindrome 39
- partial disclosure 170
- partition of set 129
- Pepin’s test 398
- perfect security 10, 12
- period 59, 71, 97, 332, 339, 346
- permutation 39, 47, 96
- plaintext xvii, 2
- Pocklington–Lehmer criterion 396
- point at infinity 448, 453, 454
- polarization identity 494
- Pollard $p - 1$ 168, 392
- Pollard rho 389, 410, 434
- polyalphabetic cipher 12, 13, 71, 97
- polynomial ring 300
- polynomial-time algorithm 153
- power residue 211
- power set 486
- primality certificate 405
- prime 299
- prime factorization 299
- prime number 62, 109

- Prime Number Theorem 191
- primes in sequences 192
- primitive polynomial 482, 343
- primitive root 136, 172, 229, 231, 445
- principal ideal 458
- principal square root 210, 287
- private key 164
- pRNG 331
- probabilistic algorithm xix, 153
- probability 22, 25
- probable prime 255
- probable word 142
- product of permutations 48
- product of random variables 71
- projective plane 454
- proper divisor 109, 299
- proper ideal 458
- proper subset 485
- pseudo-random number generator 331
- pseudoprime 255, 257
- public-key ciphers 160

- quadratic reciprocity 246
- quadratic residue mod p 231
- quadratic sieve 417
- quadratic symbol 244, 261
- quantum algorithms 179, 182, 188
- quantum channel 187
- quantum computer 155, 187
- quantum cryptography 187
- quantum teleportation 187
- quick sort 492
- quotient group 452
- quotient homomorphism 467
- quotient ring 181, 466

- random squares factoring 414
- random variable 69
- RC6 106
- reduced 469
- reduced form 425
- reduced mod P 424
- reduction homomorphism 463
- reduction modulo m 5

- reflexivity 127
- relation on a set 127
- relatively prime 109
- remainder 5
- replay attack 281, 288
- representative for equivalence class 128
- residue class 130
- Riemann hypothesis 197
- Riemann-Roch theorem 452
- riffle shuffle 54
- right coset 269
- right ideal 461
- right translate 269
- Rijndael 106
- ring 293
- ring homomorphism 462
- ring isomorphism 462
- root-taking 168
- roots in groups 363
- row operations 413
- RSA cipher 161, 162
- RSA function 168
- RSA modulus 164

- S-boxes 100, 103, 106
- sample space 25
- scalar product 494
- searching 489
- seed 331, 335
- selection sort 490
- semantic security 168
- Serpent 106
- session key 105, 161, 171, 281
- sets 484
- Shannon 99
- shared secret 2
- shift cipher 2
- Shor's factoring algorithm 188
- short pad attack 170
- signature xvi, 280
- simple substitution cipher 96
- simple transposition cipher 43
- single-letter frequencies 75
- small decryption exponent attack 169

small public exponent attack 169
 smooth 168, 392, 402, 415
 Solovay–Strassen test 260, 262
 Sophie Germain prime 281
 sorting 489
 square mod p 231
 square roots mod p 210, 243
 square-root algorithm 367
 square-root oracle 225
 stabilizer subgroup 478
 standard deviation 91
 Stirling’s formula 502
 stream cipher 98
 strong liar 382
 strong modular multiplication 177
 strong prime 168, 402
 strong pseudoprime 163, 378
 subexponential algorithms 155
 subfield 425, 469
 subgroup 268
 substitution cipher 40
 substitution homomorphism 463
 sum of random variables 70
 sums of powers of divisors 235
 Sun Ze’s theorem 214
 superincreasing sequence 177
 surjective 486
 symmetric cipher 4, 13, 159, 160
 symmetric group 47
 synchronous cipher 99
 systems of congruences 216

threshold scheme 282
 timestamp 281, 290
 timing attack 170, 281
 transposition cipher 97
 trapdoor 161
 trial 22
 trigram 33, 64
 triple DES 100
 trivial ideal 458
 twin primes 281
 Twinkle 338
 Twofish 106

unicode xix
 unique factorization 112, 310
 unit 293

variance 91
 Vernam cipher 10
 Vigenere cipher 58, 332

weak keys 158
 weak multiplicativity 234
 witness 256, 257, 378
 word problem 184

yes-biased algorithm 153

zero divisor 294
 zero-knowledge proof xvii, 287
 zeta function 197