

- random, 92
 - walk, 174
- rank of an elliptic curve, 173
- reduction of an elliptic curve, 184, 193-194
- relatively prime, 14
- repeated squaring method, 23, 97, 104
- repeating expansion of fraction, 10, 200, 222
- residue, least absolute, 145
 - modulo m , 19, 193
 - quadratic, 43
- rho method, 138-142
- Riemann Hypothesis, 50, 134
- ring, 68
 - matrix, 68
 - polynomial, 31
- RSA, 22, 92-93, 106, 125, 137, 153
- Russian alphabet, 63, 78-79
 - surgeon, 61
- Schoof algorithm, 179, 183
- secret sharing, 27
- shift transformation, 56
- sieve of Eratosthenes, 161
 - quadratic, 160-162
- signature, 88, 95
- Silver-Pohlig-Hellman algorithm, 102-103, 183
- smooth integer, 102
 - point, 168
- Solovay-Strassen primality test, 129
- splitting field, 33
- square roots in a finite field, 42, 48, 52, 96, 179-180
- Stirling's formula for $n!$, 10, 148, 154
- strong pseudoprime, 130
- structure of cryptosystem, 56
- superincreasing, 112
- supersingular elliptic curves, 181
- surgeon, American, 61, 210
 - French, 61
 - Russian, 61
- symmetrical cryptosystem, 88
- three-coloring, 118
- time estimates, 4-5
 - for arithmetic operations, 3-7
 - for converting bases, 9
 - for elliptic curve factorization, 197-198
 - for Euclidean algorithm, 13, 14, 16, 17
 - for factor-base algorithm, 148-153
 - for factoring algorithms, 152-153
 - for Miller-Rabin primality test, 136-137
 - for modular exponentiation, 24
 - for multiplicative inverses, 19
 - for points on elliptic curve, 178
 - for quadraticsieve factoring, 164
 - for rho method, 141-142
 - for square roots *mod* p , 49-50
- torsion subgroup, 173, 185
- torus, 172-173
- trace, 186
- trapdoor function, 85
- traveling salesman, 112
- trial division, 126, 138
- trigraph, 54
- USSR, 211
 - Communist Party of, 212
- vector space, 31
- Vigenère cipher, 66
- Weierstrass p -function, 171-172
- Weil conjectures, 175-176
 - pairing, 180-181
- Wilson's Theorem, 25
- zero knowledge, 117
 - for discrete log, 119-120, 123
 - for factoring, 122-123
 - for map colorability, 118-119
- zeta-function, 175