

- linear map, 57, 67, 68, 70
- Massey-Omura cryptosystem, 100, 109, 182, 216
- matrices, 66-67, 68
 inverses, 67, 69
- Merkle-Hellman cryptosystem, 113-114
- Mersenne prime, 28, 29, 51, 125, 191, 207
 in the Gaussian integers, 228
- message unit, 54
- Miller-Rabin primality test, 130-131
 time estimate for, 136-137
- modular exponentiation, 23-24, 97
- modulus, 19
- monic polynomial, 17, 32
- Monte-Carlo factorization, 138-142
- Mordell theorem, 173
- multiple of point, 178
- multiplicity of root, 32
- nonresidue, quadratic, 43
- non-interaction, 122
- non-singular, 168
- nonsupersingular, 181
- NP-complete, 112, 118
- number field sieve, 152-153, 164-165
- numerical equivalents, 55
- oblivious transfer, 120-123
- one-way function, 85
- order of an element, 33
 of a point, 173
- parameters, 56, 83
- Pépin primality test, 190
- plaintext, 54
- Pocklington primality test, 187-188
- Pohlig-Silver-Hellman algorithm, 102-103, 183
- point at infinity, 168, 171
- Pollard $p - 1$ method, 192-193
- polynomial time, 10
- polynomials, 17
 derivative of, 32
- Euclidean algorithm for, 17
g.c.d. of, 17, 32
- irreducible, 32
- monic, 17, 32
- multiple roots, 17
- primitive, 38
- ring of, 31
- unique factorization, 32
- precomputation, 104
- primality test, 92, 125
 Adleman-Huang, 190
 Adleman-Pomerance-Rumely, 134-135
 Atkin, 187, 190
 Cohen-Lenstra, 134-135
 elliptic curve, 188-190
 Miller-Rabin, 130-131
 Pépin, 190
 Pocklington, 187-188
 Solovay-Strassen, 129
 trial division, 126
- prime field, 33
- prime number, 12
 in arithmetic progression, 35
 Fermat, 29, 51, 109, 190
 Mersenne, 28, 29, 51, 125, 191, 207
- Prime Number Theorem, 11, 92
- primitive polynomial, 38
 root of unity, 42
- private key cryptosystem, 88
- probabilistic algorithm, 86, 95, 127
 encryption, 89
- product of cryptosystems, 64, 78-79
- projective equation, 171
 plane, 171
 point, 171
- pseudoprime, 126
 Euler, 129
 strong, 130
- public key, 87, 88
- quadratic character, 174
 nonresidue, 43
 reciprocity, 45, 47
 residue, 43
 sieve, 160-162