

- Fermat factorization, 15, 96, 143-144
- Monte-Carlo method, 138-140
- Pollard $p - 1$ method, 192-193
- quadratic sieve, 160-162
- rho method, 138-142
- trial division, 126, 138
- Fermat factorization, 15, 96, 143-144
 - prime, 29, 51, 109, 190
- Fermat's Little Theorem, 20, 126
- Fibonacci numbers, 16-17, 77-78, 159, 211-212, 223
- fields, 31
 - automorphism of, 32, 36
 - characteristic of, 33
 - finite, 20, 33
 - Galois extension, 32
 - isomorphism, 32
 - of p elements, 20, 33
 - prime, 33
 - splitting, 33
- finite fields, 20, 33
 - automorphism of, 36
 - existence and uniqueness, 35-36
 - generator, 34
 - irreducible polynomials over, 38-39, 104, 110
 - roots of unity in, 42
 - square roots in, 42, 48, 52, 96, 179-180
 - subfields, 38
- fixed digraph, 81
 - message unit, 62, 64
- frequency analysis, 56
- Frobenius, 183, 229
- function, one-way, 85
 - trapdoor, 85
- Fundamental Theorem of Arithmetic, 12, 26

- Galois field extension, 32
- Gauss sum, 44, 45, 134
- Gaussian integers, 17, 37, 42-43, 171
- generator of finite field, 34
- Germain, Sophie, 207
 - prime, 207

- "giant step — baby step" method, 103
- global elliptic curve, 183
- graph, 118
- greatest common divisor, 12
 - of Gaussian integers, 17
 - of polynomials, 17, 32
- group, abelian, 33
 - cyclic, 34

- hash function, 89
- Hasse's theorem, 174
- hexadecimal, 10

- imbedding plaintexts, 179
- index-calculus algorithm, 103-106
- infinity, line at, 171
 - point at, 168, 171
- inverses, multiplicative, 19
- irreducible polynomial, 32, 104, 110
- isomorphism, 32

- Jacobi symbol, 47

- k*-threshold scheme, 27
- key, 56
 - deciphering, 83
 - enciphering, 56, 83
 - exchange, 89, 98
- knapsack cryptosystem, 113-115
 - problem, 112
 - superincreasing, 112

- Lagrange's theorem, 157
- lattice, 171
- least absolute residue, 145
 - common multiple, 13
- Legendre symbol, 43, 174
- Lenstra elliptic curve factorization, 191-192, 195-198
- lifting, 52, 80
- line at infinity, 171
- linear algebra, 58, 66-68
 - modulo N , 68-70, 105
 - modulo 2, 146-147