

Index

- 2-COL, 27
- 2-SAT, 28
- 3-COL, 51
- 3-COL MAX DEGREE 4, 65
- 3-SAT, 50

- accepted, 22
- acceptor DTM, 22
- acceptor PTM, 72
- adaptive-chosen-message attack, 172
- adjacency matrix, 25
- AES, 118
- Alice, 2
- alphabet, 16
- AND, 24
- associated language, 23
- attacks
 - chosen plaintext attack, 5
 - ciphertext only attack, 4
 - known plaintext attack, 4
- authenticated key distribution, 193
- authentication, 170

- basis, 88
- BDLOG, 135
- Berlekamp–Massey algorithm, 112
- binary, 13
- bipartite, 252
- birthday attack, 180
- bit, 13
- bit commitment, 241
- bit generator, 205
- blank symbol $*$, 16
- block cipher, 115
 - AES, 118
 - DES, 115
- DES-X, 118
- Feistel cipher, 115
- Pohlig–Hellman cryptosystem, 119
- Rijndael, 118
- Triple DES, 117
- Blom key distribution, 188
- Blum prime, 139, 158
- Blum–Blum–Shub generator, 223
- Blum–Goldwasser cryptosystem, 224
- Blum–Micali generator, 211
- Bob, 2
- Boolean function, 24
 - AND, 24
 - conjunction (AND) \wedge , 24
 - disjunction (OR) \vee , 24
 - literal, 24
 - negation, 24
 - OR, 24
 - satisfiable, 24
 - satisfying truth assignment, 24
 - truth assignment, 24
- Boolean functions
 - conjunctive normal form (CNF), 24
 - disjunctive normal form (DNF), 36
- BOUNDED HALTING, 46
- bounded-error probabilistic polynomial time (BPP), 82

- Carmichael number, 76
- certificate, 41, 194
- challenge-response schemes, 230
- chosen plaintext attack, 5
- chosen-message attack, 172
- Church–Turing Thesis, 22
- cipher, 3

- ciphertext, 3
 - ciphertext only attack, 4
 - circuit, 88
 - circuit complexity, 89
 - computes, 88
 - depth, 88
 - gate, 88
 - input, 88
 - monotone, 94
 - output, 88
 - size, 88
 - circuit complexity, 89
 - clause, 24
 - CLIQUE, 26
 - clique, 252
 - Cocks–Ellis cryptosystem, 142
 - private key, 142
 - public key, 142
 - coin tossing, 241
 - coin-tossing head, 71
 - coin-tossing tape, 71
 - collision, 180
 - collision-resistant, 180
 - colouring, 27
 - commitment schemes, 241
 - complement, 56
 - completeness, 233
 - complexity class, 23
 - bounded-error probabilistic polynomial time
 - BPP, 82
 - co-NP, 56
 - exponential time EXP, 34
 - non-deterministic polynomial time NP, 41
 - non-uniform polynomial time P/poly, 84
 - NP-complete, 45
 - polynomial size circuits C-poly, 89
 - polynomial space PSPACE, 34
 - polynomial time P, 23
 - randomized polynomial time RP, 73
 - zero-error probabilistic polynomial time
 - ZPP, 80
 - COMPOSITE, 36
 - composite, 254
 - computation, 17
 - computational zero knowledge (CZK), 240
 - computes, 17, 88
 - configuration, 17
 - conjunction (AND) \wedge , 24
 - conjunctive normal form (CNF), 24
 - co-NP, 56
 - control unit, 16
 - cryptogram, 3
 - cryptogram space, 99
 - cryptosystem, 3
 - cycle, 252
 - decides, 23
 - decision problems, 22
 - 2-COL, 27
 - 2-SAT, 28
 - 3-COL, 51
 - 3-COL MAX DEGREE 4, 65
 - 3-SAT, 50
 - associated language, 23
 - BDLOG, 135
 - BOUNDED HALTING, 46
 - CLIQUE, 26
 - COMPOSITE, 36
 - DECODING LINEAR CODES, 163
 - DIV 3, 43
 - DNF-SAT, 36
 - EXP BOUNDED HALTING, 35
 - FACTOR, 61, 134
 - GEN DISCRETE LOG, 120
 - GOLDBACH, 65
 - GRAPH ISOMORPHISM, 61
 - GRAPH NON-ISOMORPHISM (GNI), 232
 - HAMILTON CYCLE, 43
 - INDEPENDENT SET, 44
 - k-CLIQUE, 26
 - k-COL, 27
 - k-SAT, 25, 49
 - MAX CLIQUE, 65
 - NON-ZERO POLY, 68
 - NON-ZERO POLY DET, 73
 - PARTITION, 64
 - PRIME, 57
 - PRIMITIVE, 200
 - QBF, 43
 - QUADRATIC NON-RESIDUES (QNR), 234
 - REACHABILITY, 28
 - SAT, 24
 - SUBSET SUM, 161
 - UNSAT, 65
 - VERTEX COVER, 65
- DECODING LINEAR CODES, 163
- decrypt, 3
- decryption function, 99
- depth, 88
- DES, 115

- DES-X, 118
- deterministic oracle Turing machine (DOTM), 54
- deterministic Turing machine (DTM), 16
 - accepted, 22
 - acceptor DTM, 22
 - alphabet, 16
 - blank symbol *, 16
 - computation, 17
 - computes, 17
 - configuration, 17
 - control unit, 16
 - decides, 23
 - halting state, 16
 - input, 17
 - language accepted by, 22
 - length, 17
 - output, 17
 - read–write head, 16
 - rejected, 22
 - running time, 21
 - size, 84
 - space, 33
 - space complexity, 34
 - starting square, 16
 - starting state, 16
 - states, 16
 - step, 17
 - tape, 16
 - time complexity, 21
 - transition function, 16
- dexp, 127
- differential cryptanalysis, 117
- DIFFIE–HELLMAN, 149, 191
- Diffie–Hellman key establishment, 190
- Digital Signature Algorithm (DSA), 175
- digital signatures, 170
 - certificate, 194
 - Digital Signature Algorithm (DSA), 175
 - Elgamal signature scheme, 174
 - RSA signature scheme, 171
- digraph, 252
- direct attack, 172
- directed graph, 252
- Discrete Log Assumption, 128
- discrete logarithm problem, 127
- disjunction (OR), \vee , 24
- disjunctive normal form (DNF), 36
- DIV 3, 43
- divides, 254
- dlog, 127
- DNF-SAT, 36
- DTM, 16
- ELGAMAL, 147
 - Elgamal, 149
 - private key, 147
 - public key, 147
 - ELGAMAL PRIVATE KEY, 148
 - Elgamal signature scheme, 174
 - encrypt, 3
 - encryption function, 99
 - ERROR CORRECTING LINEAR CODES, 163
 - Euclid’s algorithm, 32
 - Eve, 2
 - existential forgery, 173
 - EXP, 34
 - EXP BOUNDED HALTING, 35
 - expected running time, 72
 - exponential time EXP, 34
 - exponentiation, 32
- fac, 133
- FACTOR, 61, 134
- factoring algorithms, 130
 - Number Field Sieve, 131
 - Quadratic Sieve, 131
- Factoring Assumption, 131
- feedback coefficients, 107
- feedback polynomial, 107
 - primitive, 109
- Feistel cipher, 115
- Fermat witness, 75
- Fiat–Shamir identification scheme, 246
- Fibonacci sequence, 37
- fixed point, 167
- forger, 238
- FP, 30
- Fred, 2
- gate, 88
- gcd, 32
- GCHQ, 141
- GEN DISCRETE LOG, 120
 - generates, 107
- GOLDBACH, 65
- Goldwasser–Micali cryptosystem, 227
- Goppa codes, 163
- graph, 252
- GRAPH ISOMORPHISM, 61

- GRAPH NON-ISOMORPHISM (GNI), 232
 greatest common divisor, 32
- halting (PTM), 72
 halting state, 16
 HAMILTON CYCLE, 43
 Hamilton cycle, 252
 Hamilton path, 252
 Hamiltonian, 252
 hard-core predicate, 208
 hash function, 178
 birthday attack, 180
 collision, 180
 collision-resistant, 180
 hash functions
 SHA-1, 180
 SHA-256, 180
 SHA-384, 180
 SHA-512, 180
 Hill's cipher, 121
- identification schemes, 229
 challenge–response schemes, 230
 Fiat–Shamir, 246
 INDEPENDENT SET, 44
 independent set, 252
 ink complexity, 37
 input, 17, 88
 interactive proof, 231
 intractability assumptions
 Discrete Log Assumption, 128
 Factoring Assumption, 131
 RSA Assumption, 151
 invert, 129
 IP, 233
 irreducible, 122
- k -colourable, 252
 k -colouring, 252
 k -CLIQUE, 26
 k -COL, 27
 key, 4
 key establishment, 187
 authenticated key distribution, 193
 Diffie–Hellman key establishment, 190
 Key Exchange Algorithm (KEA), 194
 man in the middle attack, 192
 Key Exchange Algorithm (KEA), 194
 key space, 99
 keystream, 105
 KGB, 102
- known plaintext attack, 4
 known-signature attack, 172
 Kolmogorov–Chaitin complexity, 204
 k -SAT, 25, 49
- L^3 lattice basis reduction, 162
 language, 22
 language accepted by, 22
 Las-Vegas algorithms, 80
 length, 17
 length preserving, 214
 LFSR, 106
 linear code, 163
 linear complexity, 112
 Berlekamp–Massey algorithm, 112
 linear feedback shift register (LFSR),
 106
 feedback coefficients, 107
 feedback polynomial, 107
 generates, 107
 non-singular, 107
 periodic, 107
 literal, 24
- Mallory, 2
 man in the middle attack, 192
 MAX CLIQUE, 65
 McEliece's cryptosystem, 162
 Merkle–Hellman cryptosystem, 161
 message, 3
 message space, 99
 Miller witness, 75
 monotone, 94
 mult, 130
- negation, 24
 neg, 126
 negligible, 126
 next-bit test, 205
 non-deterministic polynomial time NP, 41
 certificate, 41
 non-linear filter generator, 114
 non-negligible, 135
 non-secret encryption, 141
 non-singular, 107
 non-uniform polynomial time P/poly,
 84
 NON-ZERO POLY, 68
 NON-ZERO POLY DET, 73
 NP-complete, 45
 NP-hard, 54

- NSA, 1, 175, 194
 VENONA, 102
 Number Field Sieve, 131
- one time pad, 101
 one-way functions, 125
 dexp, 127
 pmult, 130
 length preserving, 214
 permutation, 214
 strong one-way functions, 129
 weak one-way functions, 135
- OR, 24
 output, 17, 88
- pairwise secrecy, 122
 palindrome, 35
 PARTITION, 64
 path, 252
 Peggy, 3
 perfect matching, 97
 perfect secrecy, 102
 perfect zero knowledge (PZK), 236
 periodic, 107
 permutation, 214
 plaintext, 3
 pmult, 130
 Pohlig–Hellman cryptosystem, 119
 polynomial expected running time, 73
 polynomial running time (PTM), 72
 polynomial size circuits C-poly, 89
 polynomial space PSPACE, 34
 polynomial time, 23
 polynomial time P, 23
 polynomial time computable FP, 30
 polynomial time reduction, 44
 polynomially indistinguishable, 218
 polynomially reducible \leq_m , 44
 positive polynomial, 126
 predicate, 207
 predictor, 205
 PRIME, 57
 prime, 254
 Prime Number Theorem, 136, 254
 prime power, 78
 PRIMITIVE, 200
 primitive polynomial, 109
 primitive root, 255
 probabilistic algorithm, 70
 probabilistic circuit, 92
 probabilistic encryption, 216
 probabilistic Turing machine
 acceptor PTM, 72
 coin-tossing head, 71
 coin-tossing tape, 71
 expected running time, 72
 halting (PTM), 72
 polynomial expected running time, 73
 polynomial running time (PTM), 72
 time complexity (PTM), 72
 probabilistic Turing machine (PTM), 71
 product cipher, 121
 pseudorandom generator, 206
 Blum–Blum–Shub generator, 223
 Blum–Micali generator, 211
 PSPACE, 34
 PTM, 71
 public exponent, 145
 public key cryptography, 4, 141
 Cocks–Ellis cryptosystem, 142
 Elgamal, 147
 McEliece’s cryptosystem, 162
 Merkle–Hellman cryptosystem, 161
 Rabin’s cryptosystem, 158
 RSA, 145
 public modulus, 145
- QBF, 43
 quadratic non-residue, 234, 256
 QUADRATIC NON-RESIDUES (QNR),
 234
 quadratic residue, 209, 256
 Quadratic Sieve, 131
 query tape, 54
- Rabin’s cryptosystem, 158
 randomized polynomial time RP, 73
 REACHABILITY, 28
 read–write head, 16
 reduction, 44
 rejected, 22
 Rijndael, 118
 RSA, 145, 152
 public exponent, 145
 public key, 145
 public modulus, 145
 RSA assumption, 151
 RSA FACTOR, 152, 166
 RSA PHI, 166
 RSA PRIVATE KEY, 152
 RSA signature scheme, 171
 running time, 21

- safe prime, 150
- SAT or satisfiability, 24
- satisfiable, 24
- satisfying truth assignment, 24
- Schwartz's Lemma, 69
- secret sharing, 196
 - Shamir's secret sharing scheme, 197
- selective forgery, 173
- session key, 147
- SHA-1, 180
- SHA-256, 180
- SHA-384, 180
- SHA-512, 180
- Shamir's secret sharing scheme, 197
- Shamir's three pass protocol, 201
- shrinking generator, 114
- simple substitution, 100
- Sophie Germain prime, 150
- soundness, 233
- space, 33
- space complexity, 34
- starting square, 16
- starting state, 16
- states, 16
- statistical test, 206
- step, 17
- stream cipher, 105
 - keystream, 105
 - non-linear filter generator, 114
 - shrinking generator, 114
- strong one-way functions, 129
- SUBSET SUM, 43, 161
- super-increasing, 161
- symmetric cryptosystems, 4, 99
 - one time pad, 101
 - Hill's cipher, 121
 - simple substitution, 100
 - Vernam's cryptosystem, 101
 - Vigenère cipher, 100
- tape, 16
- time complexity, 21
- time complexity (PTM), 72
- total break, 173
- transcript, 237
- transition function, 16
- trapdoor functions, 150
- TRAVELLING SALESMAN, 65
- Trent, 3
- Triple DES, 117
- truth assignment, 24
- Turing equivalent, 66
- Turing-reducible, 54
- unary, 12
- undeniability, 170
- unforgeability, 170
- universal forgery, 173
- UNSAT, 65
- VENONA, 102
- Vernam's cryptosystem, 101
- VERTEX COVER, 65
- vertices, 252
- Victor, 3
- Vigenère cipher, 100
- weak one-way functions, 135
 - mult, 130
- XOR, 101
- zero knowledge, 235
 - computational zero knowledge, 240
 - forger, 238
 - perfect zero knowledge, 236
 - transcript, 237
- zero-error probabilistic polynomial time ZPP, 80