
This is a Chapter from the **Handbook of Applied Cryptography**, by A. Menezes, P. van Oorschot, and S. Vanstone, CRC Press, 1996.

For further information, see www.cacr.math.uwaterloo.ca/hac

CRC Press has granted the following specific permissions for the electronic version of this book:

Permission is granted to retrieve, print and store a single copy of this chapter for personal use. This permission does not extend to binding multiple chapters of the book, photocopying or producing copies for other than personal use of the person creating the copy, or making electronic copies available for retrieval by others without prior permission in writing from CRC Press.

Except where over-ridden by the specific permission above, the standard copyright notice from CRC Press applies to this electronic version:

Neither this book nor any part may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, microfilming, and recording, or by any information storage or retrieval system, without prior permission in writing from the publisher.

The consent of CRC Press does not extend to copying for general distribution, for promotion, for creating new works, or for resale. Specific permission must be obtained in writing from CRC Press for such copying.

©1997 by CRC Press, Inc.

Index

Symbols

$|S|$ (cardinality of a set S), 49
 \in (set member), 49
 \subseteq (subset), 49
 \subset (proper subset), 49
 \cap (set intersection), 49
 \cup (set union), 49
 $-$ (set difference), 49
 \times (Cartesian product), 49
 \emptyset (empty set), 50
 O -notation (big-O), 58
 Ω -notation (big-omega), 59
 Θ -notation (big-theta), 59
 o -notation (little-o), 59
 $\stackrel{\text{def}}{=}$ (by definition), 213
 $L_q[\alpha, c]$ (subexponential notation), 60
 \leq_P (polytime reduction), 61
 \sim (asymptotic equivalence), 134
 π (mathematical constant pi), 49
 e (base of natural logarithms), 49
 \sum (sum), 50
 \prod (product), 50
 $!$ (factorial), 50
 $\lfloor \cdot \rfloor$ (floor), 49
 $\lceil \cdot \rceil$ (ceiling), 49
 ϕ (Euler phi function), 65, 286
 $\mu(n)$ (Möbius function), 154
 \lg (base 2 logarithm), 50
 \ln (natural logarithm), 50
 $[a, b]$ (interval of integers), 49
 $|$ (divides relation), 63, 79
 \equiv (congruence relation), 67, 79
 \ll (much less than), 529
 \gg (much greater than), 170
 $\binom{n}{k}$ (binomial coefficient), 52
 $\left(\frac{a}{p}\right)$ (Legendre symbol), 72
 $\langle \cdot \rangle$ (inner product), 118
 $\|x\|$ (length of a vector x), 118
 $a \leftarrow b$ (assignment operator), 66
 $a \| b$ (concatenation of strings a, b), 38
 $\{0, 1\}^k$ (bitstrings of bitlength k), 447
 $\{0, 1\}^*$ (bitstrings of arbitrary bitlength), 447
 \mathbb{Q} (the rational numbers), 49
 \mathbb{R} (the real numbers), 49

\mathbb{Z} (the integers), 49
 \mathbb{Z}_n (integers modulo n), 68
 \mathbb{Z}_n^* (multiplicative group of \mathbb{Z}_n), 69
 Q_n (quadratic residues modulo n), 70
 \overline{Q}_n (quadratic non-residues modulo n), 70
 \mathbb{F}_q (finite field of order q), 81
 \mathbb{F}_q^* (multiplicative group of \mathbb{F}_q), 81
 $R[x]$ (polynomial ring), 78
 \vee (inclusive-OR), 213
 \oplus (exclusive-OR), 20
 \wedge (AND), 213
 \boxplus (addition mod 2^n), 263
 \boxminus (subtraction mod 2^n), 270
 \odot (modified multiplication mod $2^n + 1$), 263
 \leftarrow (left rotation), 213
 \rightarrow (right rotation), 213
 $A \rightarrow B$ (message transfer), 396

A

Abelian group, 75
 Abstract Syntax Notation One (ASN.1), 660
 Access control, 3
 Access control matrix, 387
 Access matrix model, 569
 Access structure, 526
 monotone, 527
 Accredited Standards Committee (ASC), 648
 Active adversary, 15, 37
 Active attack, 41, 495
 Ad hoc security, 43
 Adaptive chosen-ciphertext attack, 42
 Adaptive chosen-message attack, 433
 Adaptive chosen-plaintext attack, 41
 Addition chains, 621, 633
 Adversary, 13, 495
 active, 15
 insider, 496
 one-time, 496
 permanent, 496
 outsider, 496
 passive, 15
 Affine cipher, 239
 Algebraic normal form, 205
 Algorithm
 definition of, 57

- deterministic, 62
 - exponential-time, 59
 - polynomial-time, 59
 - randomized, 62
 - expected running time, 63
 - running time, 58
 - asymptotic, 58
 - average-case, 58
 - worst-case, 58
 - subexponential-time, 60
 - Alphabet of definition, 11
 - Alternating step generator, 209–211, 220
 - Anonymity, 3
 - ANSI standards, 648–651, 660
 - ordering and acquiring, 656
 - ANSI X9.17 pseudorandom bit generator, 173
 - Anti-palindromic keys of DES, 257
 - Appended authenticator, 361
 - Arbitrated signature scheme, 472–473
 - Arithmetic
 - integer, *see* Multiple-precision integer arithmetic
 - modular, *see* Multiple-precision modular arithmetic
 - Arthur-Merlin games, 421
 - ASN.1, *see* Abstract Syntax Notation One (ASN.1)
 - Asymmetric cryptographic system, 544
 - Asymptotic running time, 58
 - Atkin's primality test, 145
 - implementation report, 166
 - Attack
 - active, 41, 495
 - adaptive chosen-ciphertext, 42
 - adaptive chosen-message, 433
 - adaptive chosen-plaintext, 41
 - chosen-ciphertext, 41, 226
 - chosen-message, 433
 - chosen-plaintext, 41, 226
 - chosen-text, 417
 - ciphertext-only, 41, 225
 - dictionary, 42, 392
 - differential cryptanalysis, 258
 - differential-linear, 271
 - exhaustive key search, 233–234
 - forced delay, 417
 - forward search, 42, 288, 420
 - impersonation, 42, 417
 - interleaving, 42, 417, 531, 540
 - intruder-in-the-middle, 530, 540
 - key-only, 432
 - known-key, 42, 496, 534
 - known-key triangle, 538
 - known-message, 432
 - known-plaintext, 41, 225
 - linear cryptanalysis, 258
 - local, 419
 - meet-in-the-middle, 235
 - misplaced trust in server, 531
 - non-interactive, 419
 - off-line, 419
 - on-line, 419
 - passive, 41, 495
 - pre-play, 397
 - reflection, 417, 530, 540
 - related-key, 226
 - remote, 419
 - replay, 42, 417
 - time-memory tradeoff, 236
 - truncated differentials, 271
 - universal forgery, 482
 - Attacker, 13
 - Attacker (alternate names), 495
 - see also* Adversary
 - Attribute certificate, 561
 - Audit trail, 549, 583
 - Audit trail information, 545
 - Authenticated key establishment, 492, 493
 - Authenticated key exchange protocol
 - AKEP1/AKEP2, 499, 535, 541
 - Authentication
 - data origin, 4, 361
 - see also* Data origin authentication
 - entity, 4
 - see also* Entity authentication
 - explicit key, 492
 - key, 492
 - message, 361
 - mutual, 494
 - protocol, 493
 - transaction, 362
 - unilateral, 494
 - see also* Entity authentication (and Identification)
 - Authentication code, 376, 382
 - Authentication path, 557
 - Authentication server, 491, 549
 - Authentication tree, 466–468, 485, 556–559, 587
 - Authority revocation list (ARL), 577
 - Authorization, 3
 - Authorized subset, 527
 - Auto-key cipher, 242
 - Autocorrelation function, 180
 - Autocorrelation test, 182
 - Auxiliary-input zero-knowledge, 423
 - Avalanche effect, 277
 - Average-case running time, 58
- ## B
- Baby-step giant-step algorithm, 104–106, 128

- BAN logic, 420, 534, 541
- Bandwidth efficiency, 437
- Barrett reduction, 603–605, 631
- Base b representation, 592
- Basis, 80
- Bayes' theorem, 51
- BEAR block cipher, 282
- Beaufort cipher, 241
- Beller-Yacobi key transport
 - 2-pass, 514
 - 4-pass, 513
- Berlekamp's Q -matrix algorithm, 124, 132
- Berlekamp-Massey algorithm, 200–201
 - next discrepancy, 200
- Bernoulli trial, 52
- Biased, 172
- Big-endian, 344
- Big-O notation, 58
- Big-omega notation, 59
- Big-theta notation, 59
- Bijection, 7, 50
- Binary additive stream cipher, 194
 - keystream generator, 194
 - running key generator, 194
- Binary alphabet, 11
- Binary Euclidean algorithm, 632
- Binary extended gcd algorithm, 608–610, 632
- Binary gcd algorithm, 606–607, 632
- Binary operation, 75
- Binary representation, 592
- Binary tree, 557
 - balanced, 558
 - children, 557
 - depth of, 558
 - internal vertex, 557
 - leaf, 557
 - parent, 557
 - root vertex, 557
- Binomial
 - coefficient, 52
 - distribution, 52
 - theorem, 52
- Biometrics, 387, 420
- Birthday attack, 352, 369
- Birthday problem, 53
- Birthday surprise, 53
- Bit commitment, 421
- Bitzer's hash function, 374
- Black-box, 329, 341, 369, 378
- Blakley's threshold scheme, 538
- Blind signature scheme, 475, 487
 - based on DSA, 487
 - based on Nyberg-Rueppel, 487
 - Chaum, 475
 - fair, 487
- Blinded message, 475
- Blinding function, 475
 - based on RSA, 475
- Blob, 421
- Block cipher, 223–282
 - 3-WAY, 281
 - attacks on
 - differential cryptanalysis, 258
 - differential-linear, 271
 - exhaustive key search, 233–234, 273
 - key clustering attack, 281
 - linear cryptanalysis, 258
 - meet-in-the-middle attack, 235
 - related-key attack, 226, 281
 - time-memory tradeoff, 236, 273
 - truncated differentials, 271, 280
- BEAR, 282
- Blowfish, 281
- CAST, 281
- classical cipher, 237–250
- definition of, 16, 224
- DES, 250–259
- double DES, 235
- FEAL, 259–262
- GOST, 282
- IDEA, 263–265
- iterated, 251
- Khafre, 271
- Khufu, 271
- LION, 282
- LOKI'91, 270
- Luby-Rackoff, 282
- Lucifer, 276
- modes of operation, 228–233, 272
 - ANSI X3.106 standard, 649
 - ANSI X9.52 standard, 651
 - CBC with checksum (CBCC), 367
 - cipher feedback mode (CFB), 231
 - cipher-block chaining mode (CBC), 230
 - counter mode, 233
 - electronic codebook mode (ECB), 228–230
 - FIPS 81 standard, 654
 - ISO 8372 standard, 645
 - ISO/IEC 10116 standard, 647
 - output feedback mode (OFB), 232–233
 - plaintext-ciphertext block chaining (PCBC), 368
- Randomized DES (RDES), 278
- RC2, 282
- RC5, 269–270
- round function, 251
- SAFER, 266–269

- semi-weak keys (of DES), 257
 - anti-palindromic keys (of DES), 257
- SHARK, 281
- SKIPJACK, 282, 584
- TEA, 282
- triple DES, 272
- WAKE, 282
- Block of a sequence, 180
- Blocklength, 224
- Blom's KDS bound, 505
- Blom's key pre-distribution system, 506, 536
- Blowfish block cipher, 281
- Blum integer, 74–75
- Blum-Blum-Shub pseudorandom bit generator, 186–187, 308
- Blum-Goldwasser probabilistic public-key encryption, 308–311
 - decryption algorithm, 309
 - encryption algorithm, 309
 - key generation, 308
 - security of, 310
- Blum-Micali pseudorandom generator, 189
- Blundo's conference KDS bound, 529
- Boolean function, 202
 - algebraic normal form of, 205
 - correlation immune, 207
 - nonlinear order of, 205
- BPP**, 63
- Break-backward protection, 496
- Brickell-McCurley identification protocol, 423
- Broadcast encryption, 528
- Bucket hashing, 382
- Burmeister-Desmedt conference keying, 528
- Burst error, 363
- C**
- CA, *see* Certification authority (CA)
- CA-certificate, 572
- Caesar cipher, 239
- CALEA, 590
- Capability (access control), 570
- Capstone chip, 589
- Cardinality of a set, 49
- Carmichael number, 137
- Carry-save adder, 630
- Cartesian product, 49
- Cascade cipher, 234, 237
- Cascade generator
 - m -sequence, 221
 - p -cycle, 220
- Cascading hash functions, 334
- CAST block cipher, 281
 - patent, 659
- CBC, *see* Cipher-block chaining mode
- CBC-MAC, 353–354, 367
 - ANSI X9.9 standard, 650
 - ANSI X9.19 standard, 650
 - FIPS 113 standard, 654
 - ISO 8731-1 standard, 652
 - ISO 9807 standard, 652
 - ISO/IEC 9797 standard, 646
- Cellular automata stream cipher, 222
- Certificate
 - ANSI X9.45 standard, 651
 - ANSI X9.55 standard, 651
 - ANSI X9.57 standard, 651
 - caching, 576
 - chain, 572
 - directory, 549
 - pull model, 576
 - push model, 576
 - forward, 575
 - on-line, 576
 - public-key, *see* Public-key certificate
 - reverse, 575
 - revocation, 566, 576–577
 - RFC 1422, 655
 - secret-key, *see* Secret-key certificate
 - symmetric-key, *see* Symmetric-key certificate
 - X.509 standard, 660
- Certificate of primality, 166
- Certificate revocation list (CRL), 576–577
- Certification, 3
 - path, 572
 - policy, 576
 - topology, 572
- Certification authority (CA), 491, 548, 556, 559
- Certificational attack, 236
- Certificational weakness, 285
- CFB, *see* Cipher feedback mode
- CFB-64 MAC, 650
- Challenge, 397, 409
- Challenge-response identification, 397–405, 420–421
 - public-key, 403–405
 - ISO/IEC 9798-3, 404–405
 - modified Needham-Schroeder, 404
 - X.509, 404
 - symmetric-key, 400–403
 - ISO/IEC 9798-2, 401–402
 - SKID2, 402
 - SKID3, 402
- Channel, 13
 - physically secure, 13
 - secure, 13
 - secured, 13
 - unsecured, 13
- Characteristic of a field, 77

- Chaum's blind signature protocol, 475
- Chaum-van Antwerpen undeniable signature scheme, 476–478
 - disavowal protocol, 477
 - key generation, 476
 - security of, 478
 - signature generation, 476
- Chebyshev's inequality, 52
- Checksum, 362, 367–368
- Chi-square (χ^2) distribution, 177–179
 - degrees of freedom, 177
 - mean of, 177
 - variance of, 177
- Chinese remainder theorem (CRT), 68
 - Garner's algorithm, 612–613
 - Gauss's algorithm, 68
- Chipcard, 387, 424
- Chor-Rivest public-key encryption, 302–306, 318
 - attacks on, 318
 - decryption algorithm, 303
 - encryption algorithm, 303
 - key generation, 303
 - recommended parameter sizes, 305
 - security of, 305
- Chosen-ciphertext attack, 41, 226, 285
 - adaptive, 285
 - indifferent, 285
- Chosen-message attack, 433
 - directed, 482
 - generic, 482
- Chosen-plaintext attack, 41, 226
- Cipher, 12
 - see also* Encryption
- Cipher-block chaining mode (CBC), 230
 - integrity of IV in, 230
 - use in public-key encryption, 285
- Cipher feedback mode (CFB), 231
 - as a stream cipher, 233
 - ISO variant of, 231
- Cipher machine, 242–245
 - Jefferson cylinder, 243
 - rotor-based machine, 243–245, 276
 - Enigma, 245
 - Hagelin M-209, 245
 - Hebern, 244
 - Wheatstone disc, 274
- Ciphertext, 11
- Ciphertext-only attack, 41, 225
- Ciphertext space, 11
- Claimant, 385, 386
- Classical cipher, 237–250, 273–276
 - cipher machines, *see* Cipher machine
 - cryptanalysis, 245–250, 275–276
 - index of coincidence, 248
 - Kasiski's method, 248
 - measure of roughness, 249
 - polyalphabetic substitution cipher, *see* Polyalphabetic substitution cipher
 - substitution cipher, *see* Substitution cipher
 - transposition cipher, *see* Transposition cipher
- Classical modular multiplication, 600
- Classical occupancy problem, 53
- Claw-resistant (claw-free), 376, 468
- Clipper chip, 584, 589
 - key escrow, 584
 - law enforcement access field (LEAF), 584
- Clipper key escrow, 654
- Clock-controlled generator, 209–212
- co-NP**, 60
- Codebook, 240
- Codomain of a function, 6, 50
- Collision, 321
 - pseudo-collision, 371
- Collision resistance, 324, 325
- Collision resistant hash function (CRHF), 325
- Combining function, 205
- Common modulus attack on RSA, 289
- Commutative ring, 77
- Complementation property of DES, 256–257
- Complete function, 277
- Complexity classes, 59–62
 - BPP**, 63
 - co-NP**, 60
 - NP**, 60
 - NP-complete**, 61
 - NP-hard**, 62
 - NPC**, 61
 - P**, 60
 - RP**, 63
 - ZPP**, 63
- Complexity measure
 - 2-adic span, 218
 - linear complexity, 198–201
 - maximum order complexity, 217
 - Turing-Kolmogorov-Chaitin complexity, 217
 - Ziv-Lempel complexity, 217
- Complexity of attacks on a block cipher, 225–227
 - active complexity, 226
 - attack complexity, 226
 - data complexity, 226
 - passive complexity, 226
 - processing complexity, 226
 - storage complexity, 226
- Complexity theory, 57–63
- Complexity-theoretic security, 43
- Compliant, 532
- Composite integer, 64
- Composition of functions, 19

- Computation-resistance (MAC), 325
 - Computational problems
 - computationally equivalent, 88
 - polytime reduction, 88
 - Computational security, 43, 226
 - Computational zero-knowledge protocol, 407
 - Computationally equivalent decision problems, 61
 - COMSET, 421, 536
 - Conditional entropy, 56
 - Conditional probability, 51
 - Conditional transinformation, 57
 - Conference keying, 528–529, 540
 - Blundo's conference KDS bound, 529
 - Burmester-Desmedt, 528
 - definition of, 528
 - Confidentiality, 3, 4, 12
 - Confirmation, 3
 - Confounder, 418
 - Confusion, 20
 - Congruences
 - integers, 67
 - polynomials, 79
 - Conjugate gradient method, 129
 - Connection polynomial of an LFSR, 196, 204
 - known versus secret, 204
 - sparse versus dense, 205
 - Constrained linear equations problem, 423
 - Continued fraction factoring algorithm, 126
 - Continuous random variable, 176
 - Control vector, 569
 - patent, 639, 658
 - Conventional encryption, 15
 - Coprime, 64
 - Correcting-block chaining attack, 373
 - Correlated, 172
 - Correlation attack, 206, 218
 - Correlation immunity, 207, 218
 - Counter mode, 233
 - CRC-based MAC, 359
 - Credential, 501
 - CRHF, *see* Collision resistant hash function
 - Cross-certificate (CA-certificate), 572
 - Cross-certificate pair, 573
 - CRT, *see* Chinese remainder theorem
 - Cryptanalysis, 15
 - Cryptanalyst, 15
 - Cryptographic check value, 363
 - Cryptographic primitives, 4
 - taxonomy of, 5
 - Cryptographically secure pseudorandom bit generator (CSPRNG), 185–187
 - Blum-Blum-Shub generator, 186–187
 - Blum-Micali generator, 189
 - definition of, 171
 - Micali-Schnorr generator, 186
 - modified-Rabin generator, 190
 - RSA generator, 185–186
 - Cryptography
 - definition of, 4
 - goals of, 4
 - CRYPTOKI, 656
 - Cryptology, 15
 - Cryptoperiod of a key, 553
 - Cryptosystem, 15
 - Cut-and-choose protocol, 410, 421
 - Cycle of a periodic sequence, 180
 - Cyclic group, 69, 76
 - generator of, 76
 - Cyclic redundancy code (CRC), 363
 - Cyclic register, 220
 - Cycling attacks on RSA, 289, 313
- D**
- Data Authentication Algorithm (DAA), 654
 - Data Encryption Standard, *see* DES block cipher
 - Data integrity, 3, 4, 33, 359–368, 383
 - Data key, 552
 - Data origin authentication, 3, 4, 25, 359–368, 491
 - Davies-Meyer hash function, 341
 - de Bruijn FSR, 203
 - de Bruijn sequence, 203
 - De-skewing, 172
 - DEA, 649
 - Decimated subsequence, 211
 - Decision problems, 60
 - computationally equivalent, 61
 - polytime reduction, 61
 - Decryption, 11
 - Decryption exponent for RSA, 286
 - Decryption function, 11
 - DECT, 586
 - Degrees of freedom, 177
 - Delay element
 - of an FSR, 202
 - of an LFSR, 195
 - Delayed-carry adder, 630
 - Density of a knapsack set, 120
 - Derivative of a polynomial, 123
 - DES block cipher, 250–259, 276–278
 - ANSI X3.92 standard, 649
 - attacks on
 - differential cryptanalysis, 258–259
 - exhaustive key search, 233–234, 272
 - linear cryptanalysis, 258–259
 - complementation property, 256–257
 - decryption algorithm, 255
 - DESX, 273
 - double DES, *see* Double DES

- encryption algorithm, 253
 - expansion permutation, 252
 - FIPS 46 standard, 654
 - initial permutation (IP), 252, 277
 - key schedule
 - decryption, 256
 - encryption, 255
 - modes of operation, *see* Block cipher, modes of operation
 - patent, 636
 - permuted choices (PC1, PC2), 252
 - properties and strengths, 256–259
 - round, 252
 - S-box, 252
 - semi-weak key, 257
 - anti-fixed point of, 257
 - test vectors, 256
 - triple-DES, 273
 - weak key, 257
 - fixed point of, 257
 - Designated confirmer signature, 487
 - Deterministic, 306
 - Deterministic algorithm, 62
 - Dickson polynomial, 314
 - Dickson scheme, 314
 - Dictionary attack, 42
 - Difference of sets, 49
 - Differential chaining attack, 375
 - Differential cryptanalysis
 - of block ciphers, 258, 271, 278–280
 - Differential-linear cryptanalysis, 271
 - Diffie-Hellman key agreement, 515–520, 522–524
 - ANSI X9.42 standard, 651
 - composite modulus, 537
 - patent, 637
 - Diffie-Hellman problem, 113–114
 - composite moduli, 114, 131
 - generalized, 113
 - Diffie-Lamport one-time signature scheme, 485
 - Diffusion, 20
 - Digital envelope, 550
 - Digital fingerprint, 321
 - Digital signature, *see* Signature
 - Digital Signature Algorithm (DSA), 452–454, 483
 - ANSI X9.30-1 standard, 651
 - FIPS 186 standard, 655
 - key generation, 452
 - patent, 640, 658
 - security of, 453
 - signature generation, 452
 - signature verification, 453
 - use and throw coupons, 483
 - Dimension of a vector space, 80
 - Dirichlet theorem, 135
 - Disavowal protocol, 477
 - Discrete Fourier Transform (DFT), 631
 - Discrete logarithms, 103–113
 - baby-step giant-step algorithm, 104–106
 - composite moduli, 114
 - exhaustive search, 104
 - for class groups, 130
 - for elliptic curves, 130
 - for hyperelliptic curves, 130
 - function field sieve, 129
 - generalized problem, 103
 - heuristic running time, 129
 - in subgroups of \mathbb{Z}_p^* , 113
 - index-calculus algorithms, 109–112
 - lambda method, 128
 - number field sieve, 128
 - Pohlig-Hellman algorithm, 107–109
 - Pollard's rho algorithm, 106–107
 - problem definition, 103
 - rigorously analyzed algorithms, 129
 - security of individual bits, 116
 - Divisible electronic coin, 487
 - Division
 - of integers, 63
 - of polynomials, 79
 - Division algorithm
 - for integers, 64
 - for polynomials, 78
 - Dixon's algorithm, 95, 127
 - DNA computer, 130
 - Domain of a function, 6, 50
 - Double DES, 235
 - Double spending, 487
 - Double-length MDC, 339
 - DSA, *see* Digital Signature Algorithm
 - Dynamic key establishment, 491
 - Dynamic secret sharing scheme, 527
- ## E
- E-D-E triple encryption, 235, 272
 - E-E-E triple encryption, 272
 - Eavesdropper, 13, 495
 - ECA, *see* Elliptic curve factoring algorithm
 - ECB, *see* Electronic codebook mode
 - Effective key size, 224
 - Electronic cash
 - divisible, 487
 - untraceable, 487
 - Electronic codebook mode (ECB), 228–230
 - ElGamal key agreement, 517
 - ElGamal public-key encryption, 294–298
 - generalized
 - decryption algorithm, 297
 - encryption algorithm, 297

- key generation, 297
 - in \mathbb{Z}_p^*
 - decryption algorithm, 295
 - encryption algorithm, 295
 - key generation, 294
 - recommended parameter sizes, 296
 - security of, 296
 - ElGamal signature scheme, 454–459, 484
 - generalized
 - key generation, 458
 - signature generation, 458
 - signature verification, 458
 - in \mathbb{Z}_p^*
 - key generation, 454
 - security of, 455–456
 - signature generation, 454
 - signature verification, 454
 - signature verification, 618
 - variants of, 457
 - Elliptic curve
 - discrete logarithm problem, 130
 - ElGamal public-key encryption, 297
 - in public-key cryptography, 316
 - patents, 659
 - RSA analogue, 315
 - supersingular curve, 130, 316
 - Elliptic curve factoring algorithm (ECA), 94, 125
 - implementation reports, 126
 - Elliptic curve primality proving algorithm, 145
 - Encrypted key exchange (EKE), 538
 - Encryption, 11
 - see also* Block cipher
 - see also* Public-key encryption
 - see also* Stream cipher
 - Encryption exponent for RSA, 286
 - Encryption function, 11
 - Encryption scheme, 12
 - breakable, 14
 - Enemy, 13, 495
 - Enigma, 245, 276
 - Entity, 13
 - Entity authentication, 3, 386, 491
 - ANSI X9.26 standard, 651
 - FIPS 196 standard, 655
 - ISO 11131 standard, 652
 - ISO/IEC 9798 standard, 401–402, 404–405, 421, 647
 - see also* Identification
 - Entropy, 56–57, 246
 - Ephemeral secret, 494
 - Equivalence class, 68, 79
 - Equivocation, 56
 - Error-correcting code, 298, 363, 506
 - Escrowed Encryption Standard (EES)
 - FIPS 185, 654
 - ESIGN signature scheme, 473–474, 486
 - key generation, 473
 - patent, 638, 658
 - security of, 474
 - signature generation, 473
 - signature verification, 473
 - Euclidean algorithm
 - for integers, 66
 - for polynomials, 81–83
 - Euler liar, 138
 - Euler phi function (ϕ), 65
 - Euler pseudoprime, 138
 - Euler witness, 137
 - Euler's criterion, 137
 - Euler's theorem, 69
 - Exclusive-or (XOR), 20
 - Exhaustive key search, 14, 233–234, 272
 - Existential forgery, 30, 326, 432
 - exp (exponential function), 50
 - Expected running time, 63
 - Explicit authentication, 492
 - Exponent array, 617
 - Exponent recoding, *see* Exponentiation
 - Exponential-time algorithm, 59
 - Exponentiation, 613–629, 633–634
 - addition chains, 621
 - exponent recoding, 627–629
 - signed-digit representation, 627–628
 - string-replacement representation, 628–629
 - fixed-base comb method, 625–627
 - fixed-base Euclidean method, 624–625
 - fixed-base windowing method, 623–624
 - left-to-right binary method, 615
 - left-to-right k -ary method, 615
 - modified left-to-right k -ary method, 616
 - Montgomery method, 619–620
 - repeated square-and-multiply algorithm, 71, 84
 - right-to-left binary method, 614
 - simultaneous multiple, 617–618
 - sliding-window method, 616
 - vector-addition chains, 622–623
 - Extendable secret sharing scheme, 526
 - Extended Euclidean algorithm
 - for integers, 67
 - for polynomials, 82
 - Extended Riemann Hypothesis (ERH), 165
 - Extension field, 77
 - Extractor, 406
- F**
- Factor base, 94, 109

- Factoring integers, *see* Integer factorization
Factoring polynomials, *see* Polynomial factorization
Fail-stop signature scheme, 478–481, 488
 Heijst-Pedersen, 478–481
Fair blind signature scheme, 487
Fair cryptosystems, 640–641, 658
 for Diffie-Hellman key agreement, 641
 patent, 640
FEAL block cipher, 259–262, 278–279
 attacks on, 278–279
 FEAL decryption algorithm, 261
 FEAL-8 encryption algorithm, 261
 FEAL-8 key schedule, 261
 FEAL-N, 262
 FEAL-NX, 262
 patent, 639
 test vectors, 262
Feedback shift register (FSR), 195–203
 de Bruijn, 203
 definition of, 202
 delay element of, 202
 feedback bit of, 202
 feedback function of, 202
 Feedback with carry shift register (FCSR), 217–218, 222
 initial state of, 202
 linear feedback shift register, *see* Linear feedback shift register (LFSR)
 non-singular, 203
 nonlinear feedback shift register, 202
 output sequence of, 202
 stage of, 202
Feedback with carry shift register (FCSR), 217–218, 222
Feige-Fiat-Shamir identification protocol, 410–412, 422
Feige-Fiat-Shamir signature scheme, 447–449, 483
 identity-based modification, 449
 key generation, 447
 security of, 448
 signature generation, 448
 signature verification, 448
Feistel cipher, 251, 276
Fermat liar, 136
Fermat number, 143, 166
Fermat witness, 136
Fermat's primality test, 136
Fermat's theorem, 69
Fiat-Shamir identification protocol
 basic version, 408
 patent, 638, 658
Fiat-Shamir signature scheme, 483
 patent, 638, 658
Field, 77
 characteristic of, 77
 definition of, 77
 extension field of, 77
 finite, *see* Finite field
 subfield of, 77
Filtering function, 208
Finite field, 80–85
 definition of, 80
 order of, 80
 polynomial basis, 83
FIPS, 654–655, 661
 ordering and acquiring, 656
FIPS 186 pseudorandom bit generator, 174–175
FISH stream cipher, 222
Fixed-point chaining attack, 374
Floyd's cycle-finding algorithm, 91, 125
Forced delay attack, 417
Formal methods, 534, 541
Forward certificate, 575
Forward error correction, 363
Forward search attack, 34, 42, 288, 420
Fractionation, 276
Frequency distribution
 of English digrams, 247
 of single English characters, 247
Frequency test, 181
Fresh key, 494
Function, 6–10, 50
 bijection, 7
 composition of, 19
 definition of, 6
 injective, 46
 inverse, 7
 involution, 10
 one-to-one, 7
 one-way, 8
 onto, 7
 permutation, 10
 surjective, 46
 trapdoor one-way, 9
Function field sieve, 129
Functional diagram, 6
Functional graph, 54
 component size, 55
 cycle length, 55
 predecessors size, 55
 rho-length, 55
 tail length, 55
 tree size, 55
Functionally trusted third party, 39
- ## G
- Gap of a sequence, 180

- Garner's algorithm, 612–613
 - Gauss's algorithm, 68
 - Gaussian integer method, 128
 - gcd, *see* Greatest common divisor
 - Geffe generator, 206
 - General-purpose factoring algorithm, 90
 - Generator
 - of a cyclic group, 76, 160
 - algorithm for finding, 163
 - of \mathbb{F}_q^* , 81
 - of $\mathbb{F}_{2^m}^*$, 163
 - of \mathbb{Z}_n^* , 69
 - of \mathbb{Z}_p^* , 164
 - algorithm for selecting, 164
 - Generator matrix, 506
 - Girault self-certified public key, 522
 - GMR one-time signature scheme, 468–471, 486
 - authentication tree, 470
 - key generation, 469
 - security of, 470
 - signature generation, 469
 - signature verification, 469
 - GOAL stream cipher, 219
 - Goldwasser-Kilian primality test, 166
 - Goldwasser-Micali probabilistic public-key encryption, 307–308
 - decryption algorithm, 307
 - encryption algorithm, 307
 - key generation, 307
 - security of, 308
 - Golomb's randomness postulates, 180
 - Goppa code, 299, 317
 - Gordon's algorithm for strong prime generation, 150
 - GOST block cipher, 282
 - GQ identification protocol, 412–414, 422
 - patent, 639, 658
 - GQ signature scheme, 450–451
 - key generation, 450
 - message recovery variant, 451
 - patent, 639, 658
 - security of, 451
 - signature generation, 450
 - signature verification, 450
 - Grandmaster postal-chess problem, 418
 - Greatest common divisor
 - binary extended gcd algorithm, 608–610, 632
 - binary gcd algorithm, 606–607, 632
 - Euclidean algorithm, 66
 - Lehmer's gcd algorithm, 607–608, 632
 - of integers, 64
 - of polynomials, 81
 - Group, 75–76
 - cyclic, 76
 - definition of, 75
 - of units, 77
 - order of, 75
 - subgroup of, 76
 - Group signature, 488
 - GSM, 586
 - GSS-API, 655, 661
 - Günther's implicitly-certified public key, 521
 - Günther's key agreement, 522
- ## H
- Hagelin M-209, 245, 276
 - Hamming weight, 105
 - Handwritten signature, 23
 - Hard predicate, 115
 - Hash function, 33, 321–383
 - alternate terminology, 325, 371
 - applications, 321–322, 330–331
 - attacks, 368–375
 - birthday, 369–371
 - chaining, 373–375
 - Pseudo-collisions, 371–373
 - based on block ciphers, 338–343
 - Abreast Davies-Meyer, 380
 - Davies-Meyer, 341
 - Matyas-Meyer-Oseas, 341
 - MDC-2, 342
 - MDC-4, 343
 - Merkle's DES-based hash, 338, 339, 378
 - Miyaguchi-Preneel, 341
 - N-Hash, 380
 - Tandem Davies-Meyer, 380
 - based on modular arithmetic, 351–352
 - MASH-1, 352
 - MASH-2, 352
 - cascading, 334
 - collision resistant (CRHF), 325
 - customized, 343–351
 - HAVAL, 379
 - MD2, 380
 - MD4, 346
 - MD5, 347
 - RIPEMD, 380
 - RIPEMD-128, 339, 380
 - RIPEMD-160, 339, 350
 - Secure Hash Algorithm (SHA-1), 348
 - Snefru, 380
 - definition of, 322
 - ideal security, 336
 - initialization value (IV), 335
 - MD-strengthening, *see* MD-strengthening
 - Merkle's meta-method, 333
 - one-way (OWHF), 325
 - padding, 334–335
 - properties of

- 2nd-preimage resistance, 323
- collision resistance, 324
- compression, 322
- ease of computation, 322
- local one-wayness, 331
- near-collision resistance, 331
- non-correlation, 331
- partial-preimage resistance, 331
- preimage resistance, 323
- strong collision resistance, 324
- weak collision resistance, 324
- r -collision resistant, 424
- strong one-way, 325
- universal classes of, 376
- universal one-way, 377
- weak one-way, 325
- Hash-code, 321
- Hash-result, 321
- Hash-value, 33, 321
- HAVAL hash function, 379
- Heijst-Pedersen fail-stop signature scheme, 478–481
 - key generation, 478
 - proof-of-forgery algorithm, 481
 - signature generation, 479
 - signature verification, 479
- Hellman-Merkle patent, 637, 658
- Heuristic security, 43, 533
- High-order digit, 593
- Hill cipher, 240, 274
- Historical work factor, 44
- HMAC, 355
- Homomorphic property of RSA, 289
- Homophonic substitution cipher, 17, 240
- Hybrid protocol, 512
- Hyperelliptic curve
 - discrete logarithm problem, 130
 - ElGamal public-key encryption, 297
- Hypothesis testing, 179–180
- I**
- IC card, 387
- IDEA block cipher, 263–265, 279–280
 - attacks on, 279–280
 - decryption algorithm, 264
 - encryption algorithm, 264
 - key schedule, 264
 - patent, 640, 658
 - test vectors, 265
 - weak keys, 279
- Ideal secret sharing scheme, 526, 527
- Identification, 3, 24–25, 385–424
 - applications of, 387
 - attacks on, 417–420, 424
 - chosen-text, 417
 - forced delay, 417
 - impersonation, 417
 - interleaving, 417
 - local, 419
 - non-interactive, 419
 - off-line, 419
 - pre-play, 397, 398
 - reflection, 417
 - remote, 419
 - replay, 417
 - challenge-response, *see* Challenge-response
 - identification
 - mutual, 387
 - passwords, *see* Passwords (weak authentication)
 - questionnaire-based, 420
 - relation to signatures, 388
 - unilateral, 387
 - zero-knowledge, *see* Zero-knowledge identification
 - see also* Entity authentication
- Identification Friend or Foe (IFF) system, 421
- Identity verification, 385
- Identity-based key establishment, 493
- Identity-based system, 538, 561–562, 587
- IDUP, 661
- IEEE P1363 standard, 660
- IETF, 655
- Image of a function, 6, 50
- Impersonation, 27, 42, 386, 417
- Impersonator, 495
- Implicit key authentication, *see* Key authentication
- Implicitly-certified public key, 520–522, 562–563, 588
 - Diffie-Hellman using, 522–524
 - identity-based, 563
 - of Girault, 522
 - of Günther, 521
 - self-certified, 563
- Imprint, 321
- Improved PES (IPES), 279
- In-line trusted third party, 547
- Incremental hashing, 378
- Independent events, 51
- Index of coincidence, 248, 275
- Index-calculus algorithm, 109–112, 128
 - Gaussian integer method, 128
 - in \mathbb{F}_{2^m} , 111
 - implementation reports, 128
 - in \mathbb{Z}_p , 110
 - implementation reports, 128
 - linear sieve, 128
 - residue list sieve, 128
- Information dispersal algorithm (IDA), 539

- Information rate, 527
 - Information security, 2
 - objectives of, 3
 - Information security service, 14
 - breaking of, 15
 - Information theory, 56–57
 - Initial state
 - of an FSR, 202
 - of an LFSR, 196
 - Injective function, 46, 50
 - Inner product, 118
 - Input size, 58
 - Insider, 496
 - one-time, 496
 - permanent, 496
 - Integer, 49
 - multiple-precision, 593
 - negative
 - signed-magnitude representation, 593
 - two's complement representation, 594
 - single-precision, 593
 - Integer arithmetic, *see* Multiple-precision integer arithmetic
 - Integer factorization, 89–98
 - continued fraction algorithm, 126
 - Dixon's algorithm, 95, 127
 - elliptic curve algorithm, 94
 - general number field sieve, 98
 - general-purpose algorithms, 90
 - heuristic running times, 127
 - multiple polynomial quadratic sieve, 97
 - Pollard's $p - 1$ algorithm, 92–93
 - Pollard's rho algorithm, 91–92
 - problem definition, 89
 - quadratic sieve algorithm, 95–97
 - random square methods, 94–98
 - special number field sieve, 98
 - special-purpose algorithms, 90
 - trial division, 90–91
 - Integers modulo n , 67–71
 - Integrity check value (ICV), 363
 - Interactive proof system, 406
 - Arthur-Merlin games, 421
 - completeness, 406
 - soundness, 406
 - Interleaving attack, 42, 417, 531, 540
 - Interloper, 13
 - Internal vertex, 557
 - Internet security standards, 655–656, 661
 - Intersection of sets, 49
 - Intruder, 13, 495
 - Intruder-in-the-middle attack, 530, 540
 - Inverse function, 7
 - Inversion attack on stream ciphers, 219
 - Involution, 10
 - Irreducible polynomial, 78, 154–160
 - algorithm for generating, 156
 - algorithm for testing, 155
 - number of, 155
 - primitive polynomial, *see* Primitive polynomial
 - trinomials, 157
 - ISO standards, *see* ISO/IEC standards
 - ISO/IEC 9796, 442–444, 482–483
 - ISO/IEC standards, 645–648, 651–653, 660–661
 - committee draft (CD), 645
 - draft international standard (DIS), 645
 - ordering and acquiring, 656
 - working draft (WD), 645
 - Isomorphic, 81, 104
 - Iterated block cipher, 251
 - ITU, 653
- J**
- Jacobi sum primality test, 144, 166
 - Jacobi symbol, 73
 - computing, 73
 - Jefferson cylinder, 243, 274
 - Joint entropy, 56
 - JTC1, 645
- K**
- Karatsuba-Ofman multiplication, 630
 - Kasiski's method, 248, 275
 - KDC, *see* Key distribution center (KDC)
 - Kerberos authentication protocol, 401, 501–502, 535–536
 - RFC 1510, 656
 - Kerckhoffs' assumption, 225
 - Kerckhoffs' desiderata, 14
 - Key, 11
 - archival, 580
 - backup, 580
 - cryptoperiod of, 553
 - data, 552
 - de-registration, 580
 - derived, 568
 - destruction, 580
 - fresh, 494
 - generator, 549
 - installation, 579
 - key-encrypting, 552
 - key-transport, 552
 - layering, 551–553
 - long-term, 553
 - master, 551
 - notarization, 568
 - offsetting, 568
 - private, 27, 544

- public, 27, 544
- public-key vs. symmetric-key, 31–32, 551
- recovery, 580
- registration, 579
- revocation, 566, 580
- secret, 544
- separation, 567
- short-term, 553
- symmetric, 544
- terminal, 552
- update, 580
- variant, 568
- Key access server, 549
- Key agreement, 34, 35, 505–506, 515–524, 536–538
 - Blom’s key pre-distribution system, 506
 - definition of, 490
 - Diffie-Hellman, 516
 - ElGamal, 517
 - encrypted key exchange (EKE), 538
 - Günther, 522
 - MTI/A0, 517–519
 - relation to key transport, 491
 - Station-to-station (STS), 519
- Key authentication, 492
- Key clustering attack on block ciphers, 281
- Key confirmation, 492
- Key control, 494
- Key derivation, 490, 498
- Key distribution
 - confidential keys, 551–555
 - key layering, 551–553
 - key translation center, 553–554
 - symmetric-key certificates, 554–555
 - public keys, 555–566
 - authentication trees, 556–559
 - certificates, 559–561
 - identity-based, 561–562
 - implicitly-certified, 562–563
- Key distribution center (KDC), 491, 500, 547
- Key distribution pattern, 536
- Key distribution problem, 16, 546
- Key distribution system (KDS), 505
 - Blom’s KDS bound, 505
 - security against coalitions, 505
- Key escrow, 584–586
 - agent, 550, 584
 - Clipper, 584
- Key establishment, 489–541
 - analysis of, 530–534, 540–541
 - attacks on
 - interleaving, 531
 - intruder-in-the-middle, 530
 - misplaced trust in server, 531
 - reflection, 530
 - authenticated, 492, 493
 - compliant, 532
 - definition of, 35, 490
 - identity-based, 493
 - key agreement, *see* Key agreement
 - key transport, *see* Key transport
 - message-independent, 493
 - operational, 532
 - resilient, 532
 - simplified classification, 491
- Key life cycle, 577–581
 - key states, 580
- Key management, 36–38, 543–590
 - ANSI X9.17 standard, 650
 - ANSI X9.24 standard, 650
 - ANSI X9.28 standard, 651
 - ANSI X9.42 standard, 651
 - centralized, 546
 - controlling key usage, 567–570
 - definition of, 35, 544
 - ISO 8732 standard, 652
 - ISO 10202-7 standard, 652
 - ISO 11166 standard, 652
 - ISO 11568 standard, 653
 - ISO/IEC 11770 standard, 647
 - key agreement, *see* Key agreement
 - key distribution, *see* Key distribution
 - key establishment, *see* Key establishment
 - key life cycle, 577–581
 - key transport, *see* Key transport
- Key management facility, 549
- Key notarization, 568
 - patent, 642, 658
- Key pair, 12
- Key pre-distribution scheme, 540
 - definition of, 490
- Key server, 549
- Key space, 11, 21, 224
- Key tag, 568
- Key translation center (KTC), 491, 500, 547, 553
- Key transport, 35, 497–504, 506–515, 535–536
 - AKEP1, 499
 - AKEP2, 499
 - Beller-Yacobi (2-pass), 514
 - Beller-Yacobi (4-pass), 513
 - COMSET, 536
 - definition of, 490
 - Kerberos, 501–502
 - Needham-Schroeder public-key, 508
 - Needham-Schroeder shared-key, 503
 - Otway-Rees protocol, 504
 - relation to key agreement, 491
 - Shamir’s no-key protocol, 500

X.509 three-way, 512
 X.509 two-way, 511
 Key update, 490
 Keyed hash function, *see* Message authentication code (MAC)
 Keying material, 544
 Keying relationship, 544
 Keystream, 20, 193, 194
 Keystream generator, 21, 194
 Khafre block cipher, 271
 attacks on, 281
 patent, 644
 Khufu block cipher, 271
 attacks on, 281
 patent, 644
 Knapsack generator, 209, 220
 Knapsack problem, 131
 Knapsack public-key encryption, 300–306
 Chor-Rivest, 302–306
 Merkle Hellman, 300–302
 Knapsack set, 117
 density of, 120
 Known-key attack, 42, 496, 534
 Known-key triangle attack, 538
 Known-message attack, 432
 Known-plaintext attack, 41, 225
 KryptoKnight, 535, 541
 KTC, *see* Key translation center (KTC)

L

L^3 -lattice basis reduction algorithm, 118–120, 131
 Lagrange's theorem, 76
 Lambda method for discrete logarithms, 128
 Lamport's one-time-password scheme, 396
 Lanczos method, 129
 Lattice, 118
 dimension of, 118
 reduced basis, 118
 Lattice basis reduction algorithm, 118–120, 131, 317
 Law of large numbers, 52
 Law of quadratic reciprocity, 72
 lcm, *see* Least common multiple
 Leading coefficient, 78
 LEAF, 584–585
 Leaf of a binary tree, 557
 Least common multiple, 64
 Least significant digit, 593
 Legendre symbol, 72
 computing, 73
 Lehmer's gcd algorithm, 607–608, 632
 Length of a vector, 118
 Liar, 135
 Euler, 138
 Fermat, 136

 strong, 139
 Life cycle, *see* Key life cycle
 Linear code, 506
 Linear combination, 80
 Linear complexity, 198–201
 algorithm for computing, *see* Berlekamp-Massey algorithm
 of a finite sequence, 198
 of a random periodic sequence, 199
 of a random sequence, 198
 of an infinite sequence, 198
 profile, 199
 Linear complexity profile, 199–200
 algorithm for computing, 201
 limitations of, 200
 of a random sequence, 199
 Linear congruential generator, 170, 187
 multivariate congruential generator, 187
 truncated, 187
 Linear consistency attack, 219–220
 Linear cryptanalysis
 of block ciphers, 258, 271, 278, 280
 of stream ciphers, 219
 Linear feedback shift register (LFSR), 195–201
 connection polynomial of, 196
 definition of, 195
 delay element of, 195
 feedback bit of, 196
 initial state of, 196
 maximum-length, 197
 non-singular, 196
 output sequence of, 195
 stage of, 195
 Linear sieve, 128
 Linear syndrome attack, 218
 Linear system (solving large), 129
 Linearly dependent, 80
 Linearly independent, 80
 LION block cipher, 282
 Little-endian, 344
 Little-o notation, 59
 Lock-in, 221
 Logarithm, 49
 LOKI block cipher, 281
 LOKI'89, 281
 LOKI'91, 270, 281
 Long-term key, 553
 Low-order digit, 593
 Luby-Rackoff block cipher, 282
 LUC cryptosystem, 314
 LUCDIF, 316
 LUCELG, 316
 Lucas-Lehmer primality test, 142
 Lucifer block cipher, 276

patent, 641, 659

M

m-sequence, 197

MAC, *see* Message authentication code (MAC)

Manipulation detection code, *see* Modification detection code

Mapping, 6, 50

Markov cipher, 280

MASH-1 hash function, 352

ISO/IEC 10118-4 standard, 647

MASH-2 hash function, 352

ISO/IEC 10118-4 standard, 647

Master key, 551

Matyas-Meyer-Oseas hash function, 341

ISO/IEC 10118-2 standard, 647

Maurer's algorithm for provable prime generation, 153, 167

Maurer's universal statistical test, 183–185, 189

Maximum order complexity, 217

Maximum-length LFSR, 197

Maximum-rank-distance (MRD) code, 317

McEliece public-key encryption, 298–299, 317

decryption algorithm, 299

encryption algorithm, 299

key generation, 298

recommended parameter sizes, 299

security of, 299

MD-strengthening, 334, 335, 337

MD2 hash function, 380

RFC 1319, 655

MD4 hash function, 346

RFC 1320, 655

MD5 hash function, 347

RFC 1321, 655

MD5-MAC, 358

MDC, *see* Modification detection code

MDC-2 hash function, 342

ISO/IEC 10118-2 standard, 647

patent, 639

MDC-4 hash function, 343

patent, 639

MDS code, 281, 506

Mean, 51

Measure of roughness, 249

Mechanism, 34

Meet-in-the-middle attack

on double DES, 235

on double encryption, 235

time-memory tradeoff, 236

on multiple encryption

time-memory tradeoff, 236

Meet-in-the-middle chaining attack, 374

Merkle channel, 48

Merkle one-time signature scheme, 464–466, 485

authentication tree, 466

key generation, 464

patent, 643

security of, 465

signature generation, 465

signature verification, 465

Merkle puzzle scheme, 47, 537

Merkle's DES-based hash function, 338, 339, 378

Merkle's meta-method for hashing, 333

Merkle-Hellman knapsack encryption, 300–302, 317–318

basic

decryption algorithm, 301

encryption algorithm, 301

key generation, 300

multiple-iterated

key generation, 302

patent, 637

security of, 302

Mersenne number, 142

Mersenne prime, 142, 143, 160

Message authentication, *see* Data origin authentication

Message authentication code (MAC), 33, 323, 352–359, 381–383

applications of, 323, 330

based on block ciphers, 353–354

CBC-MAC, *see* CBC-MAC

CFB-64 MAC, 650

RIPE-MAC, *see* RIPE-MAC

birthday attack on, 352

customized, 356–358

bucket hashing, 382

MD5-MAC, 358

Message Authenticator Algorithm (MAA), 356

definition, 325

for stream ciphers, 358–359

CRC-based, 359

Lai-Rueppel-Woollven scheme, 383

Taylor's scheme, 383

from MDCs, 354–355

envelope method with padding, 355

hash-based MAC, 355

HMAC, 355

secret prefix method, 355

secret suffix method, 355

XOR MAC, 382

ISO 8730 standard, 652

ISO 9807 standard, 652

properties of

compression, 325

computation-resistance, 325

- ease of computation, 325
 - key non-recovery, 325
- retail MAC, 650
- types of attack
 - adaptive chosen-text, 326
 - chosen-text, 326
 - known-text, 326
- types of forgery
 - existential, 326
 - selective, 326
- see also* CBC-MAC
- Message authentication tag system, 376
- Message Authenticator Algorithm (MAA), 356
 - ISO 8731-2 standard, 652
- Message concealing in RSA, 290, 313
- Message digest, 321
- Message integrity code (MIC), 323
- Message space, 11
- Message-independent key establishment, 493
- Micali-Schnorr pseudorandom bit generator, 186
- Miller-Rabin primality test, 139, 165
- MIME, 656, 661
- Minimum disclosure proof, 421
- Minimum polynomial, 156
- Mips year, 126
- MISSI, 590
- Mixed-radix representation, 611, 630
- Mixing algebraic systems, 279
- Miyaguchi-Preneel hash function, 341
- Möbius function, 154
- mod notation, 64
- Modes of operation
 - multiple modes, *see* Multiple encryption, modes of operation
 - single modes, *see* Block cipher, modes of operation
- Modification detection code (MDC), 33, 323, 324
- Modified-Rabin pseudorandom bit generator, 190
- Modified-Rabin signature scheme, 439–442, 482
 - key generation, 440
 - security of, 441
 - signature generation, 440
 - signature verification, 440
- Modular arithmetic, *see* Multiple-precision modular arithmetic
- Modular exponentiation, *see* Exponentiation
- Modular reduction, 599
 - Barrett, 603–605, 631
 - Montgomery, 600–602, 631
 - special moduli, 605–606
- Modular representation, *see* Mixed-radix representation
- Modulus, 67
- Monic polynomial, 78
- Mono-alphabetic substitution cipher, *see* Substitution cipher
- Monobit test, 181
- Monotone access structure, 527
- Montgomery exponentiation, 619–620
- Montgomery multiplication, 602–603
- Montgomery reduction, 600–602, 631
- MOSS, 656
 - RFC 1848, 656
- Most significant digit, 593
- MTI protocols, 518, 537
- MTI/A0 key agreement, 517–519, 537
 - Goss variant, 537
 - patent, 644, 659
- Multi-secret threshold scheme, 527
- Multiple encryption, 234–237
 - definition of, 234
 - double encryption, 234
 - modes of operation, 237
 - triple-inner-CBC mode, 237
 - triple-outer-CBC mode, 237
 - triple encryption, 235
 - E-D-E, 235
 - two-key triple-encryption, 235
- Multiple polynomial quadratic sieve, 97
- Multiple-precision integer, 593
- Multiple-precision integer arithmetic, 592–599
 - addition, 594–595
 - division, 598–599
 - normalization, 599
 - gcd, *see* Greatest common divisor
 - multiplication, 595–596
 - discrete Fourier transform (DFT), 631
 - Karatsuba-Ofman, 630
 - squaring, 596–597
 - subtraction, 594–595
- Multiple-precision modular arithmetic, 599–606
 - addition, 600
 - exponentiation, *see* Exponentiation
 - inversion, 610
 - multiplication
 - classical, 600
 - Montgomery multiplication, 602–603
 - reduction, 599
 - Barrett, 603–605, 631
 - Montgomery, 600–602, 631
 - special moduli, 605–606
 - subtraction, 600
- Multiplexer generator, 220
- Multiplicative group
 - of \mathbb{Z}_n , 69
 - of a finite field, 81
- Multiplicative inverse, 68
 - computing, 71, 84, 610

Multiplicative property in RSA, 288, 435, 482
Multiplicity of a factor, 122
Multispeed inner-product generator, 220
Multivariate polynomial congruential generator, 187
Mutual authentication, 387, 402, 405, 494
Mutual information, 57
Mutually exclusive events, 51

N

N-Hash function, 380
Name server, 549
Needham-Schroeder public-key, 508, 536
Needham-Schroeder shared-key, 401, 503, 535
Next-bit test, 171
Next-discrepancy, 200
Nibble, 443
NIST, 654
Noise diode, 40
Non-interactive protocol, 493
Non-interactive ZK proof, 424
Non-malleable encryption, 311, 319
Non-repudiation, 3, 4, 582–584
 ISO/IEC 13888 standard, 648
Non-singular
 FSR, 203
 LFSR, 196
Nonce, 397, 497
Nonlinear combination generator, 205–208
 combining function of, 205
Nonlinear feedback shift register, *see* Feedback shift register (FSR)
Nonlinear filter generator, 208–209
 filtering function, 208
Nonlinear order, 205
Normal basis, 168
 exponentiation, 642
 multiplication, 642
 patents, 642–643, 659
Normal distribution, 176–177
 mean of, 176
 standard, 176
 variance of, 176
Normal polynomial, 168
Normalization, 599
Notarized key, 569
Notary
 agent, 550
 seal, 569
 service, 582
NP, 60
NP-complete, 61
NP-hard, 62
NPC, 61

Number field sieve
 for discrete logarithms, 128
 for integer factorization, 98, 126
 implementation reports, 126, 127
 general number field sieve, 98
 special number field sieve, 98, 126
Number theory, 63–75
Nyberg-Rueppel signature scheme, 460–462, 485
 security of, 461
 signature generation, 461
 signature verification, 461

O

Object identifier (OID), 660
OFB, *see* Output feedback mode
Off-line trusted third party, 548
Ohta-Okamoto identification protocol, 422
On-line certificate, 576
On-line trusted third party, 547
On-line/off-line signature, 486
 patent, 644
One-key encryption, 15
One-sided statistical test, 179
One-time insider, 496
One-time pad, 21, 192–193, 274
 patent, 657
One-time password scheme, 395–397
One-time signature scheme, 462–471
 Diffie-Lamport, 485
 GMR, 468–471
 Merkle, 464–466
 Rabin, 462–464
 validation parameters, 462
One-to-one function, 7–8, 50
One-way cipher, 377
One-way function, 8–9, 327
 DES-based, 190, 328
 exponentiation modulo a prime, 115, 329
 multiplication of large primes, 329
 Rabin function, 115
 RSA function, 115
One-way hash function (OWHF), 325
One-way permutation, 115, 328
Onto function, 7, 50
Open Systems Interconnection (OSI), 653, 660
Operational, 532
Opponent, 13, 495
 see also Attacker
Optimal normal basis, 168, 659
Oracle, 88
Order
 generating element of maximum order in \mathbb{Z}_n^* , 163
 of \mathbb{Z}_n^* , 69

- of a finite field, 80
 - of a group, 75
 - of a group element, 76, 160
 - algorithm for determining, 162
 - of an element in \mathbb{Z}_n^* , 69
- Otway-Rees protocol, 504, 536
- Output feedback mode (OFB), 232–233
 - as a stream cipher, 233
 - changing IV in, 232
 - counter mode, 233
 - feedback size, 233
- Outsider, 496
- OWHF, *see* One-way hash function
- Ownership, 3
- P**
- P**, 60
- Palindromic keys of DES, 257
- Party, 13
- Passcode generator, 402
- Passive adversary, 15
- Passive attack, 41, 495
- Passkey, 395
- Passphrase, 390
- Passwords (weak authentication), 388–397, 420
 - aging, 390
 - attacks on, 391–393
 - dictionary, 392
 - exhaustive search, 391
 - password-guessing, 392
 - pre-play, 397
 - replay, 391
 - encrypted password file, 389
 - entropy, 392
 - generator, 387
 - one-time, 395–397
 - Lamport's scheme, 396
 - passkey, 395
 - passphrase, 390
 - personal identification number (PIN), 394
 - rules, 389
 - salting, 390
 - stored password file, 389
 - UNIX, 393–394
- Patents, 635–645, 657–659
 - ordering and acquiring, 645
 - priority date, 636
 - validity period, 636
- PEM, *see* Privacy Enhanced Mail (PEM)
- Pepin's primality test, 166
- Perceptrons problem, 423
- Perfect forward secrecy, 496, 534
- Perfect power
 - testing for, 89
- Perfect secrecy, 42, 227, 307
- Perfect secret sharing scheme, 526, 527
- Perfect zero-knowledge protocol, 407
- Period of a periodic sequence, 180
- Periodic sequence, 180
 - autocorrelation function of, 180
 - cycle of, 180
 - period of, 180
- Permanent insider, 496
- Permutation, 10, 50
- Permutation polynomial, 314
- Permuted kernel problem, 423
- Personal Identification Number (PIN)
 - ANSI X9.8 standard, 649
 - ISO 9564 standard, 652
- PGP, *see* Pretty Good Privacy (PGP)
- Phi function (ϕ), 65
- Photuris, 661
- Physically secure channel, 13
- PIKE stream cipher, 222
- PIN, *see* Passwords (weak authentication), *see* Personal Identification Number (PIN)
- PKCS standards, 656, 661
 - ordering and acquiring, 657
 - PKCS #1, 445–447, 483
- Plaintext, 11
- Plaintext-aware encryption scheme, 311–312
- Playfair cipher, 239, 274
- Pless generator, 218
- PN-sequence, 181
- Pocklington's theorem, 144
- Pohlig-Hellman algorithm, 107–109, 128
- Pohlig-Hellman cipher, 271
 - patent, 642, 659
- Poker test, 182, 188
- Policy Certification Authority (PCA), 589
- Pollard's $p - 1$ algorithm, 92–93, 125
- Pollard's rho algorithm
 - for discrete logarithms, 106–107, 128
 - for factoring, 91–92, 125
- Polyalphabetic substitution cipher, 18, 241–242, 273–274
 - auto-key cipher, 242
 - Beaufort cipher, 241
 - cipher machine, *see* Cipher machine
 - PURPLE cipher, 276
 - Vigenère cipher
 - auto-key, 242
 - compound, 241
 - full, 242
 - running-key, 242
 - simple, 18, 241
 - single mixed alphabet, 242
- Polygram substitution cipher, 239

- Polynomial, 78
 - irreducible, 78
 - leading coefficient of, 78
- Polynomial basis, 83
- Polynomial factorization, 122–124, 132
 - Berlekamp's Q -matrix algorithm, 124
 - square-free factorization, 123
- Polynomial-time algorithm, 59
- Polynomial-time indistinguishability, 318
- Polynomial-time statistical test, 171
- Polynomially security public-key encryption, 306
- Polytime reduction, 61, 88
- Practical security, 43
- Pre-play attack, 397, 398
- Pre-positioned secret sharing scheme, 527
- Precision, 593
- Preimage, 6, 50
- Preimage resistance, 323
- Pretty Good Privacy (PGP), 661
- Primality proving algorithm, *see* Primality test, true primality test
- Primality test
 - probabilistic primality test, 135–142
 - comparison, 140–142
 - Fermat's test, 136
 - Miller-Rabin test, 139
 - Solovay-Strassen test, 138
 - true primality test, 142–145
 - Atkin's test, 145
 - Goldwasser-Kilian test, 166
 - Jacobi sum test, 144
 - Lucas-Lehmer test, 142
 - Pepin's test, 166
- Prime number, 9, 64
- Prime number generation, 145–154
 - algorithms
 - Gordon's algorithm, 150
 - Maurer's algorithm, 153
 - NIST method, 151
 - random search, 146
 - DSA primes, 150–152
 - incremental search, 148
 - provable primes, 152–154
 - random search, 145–149
 - strong primes, 149–150
- Prime number theorem, 64
- Primitive element, *see* Generator
- Primitive normal polynomial, 168
- Primitive polynomial, 157–160
 - algorithm for generating, 160
 - algorithm for testing, 157
 - definition of, 84
- Primitives, 4
- Principal, 495
- Principal square root, 74
- Privacy, *see* Confidentiality
- Privacy Enhanced Mail (PEM), 588, 655
 - RFCs 1421–1424, 655
- Private key, 26, 27, 544
- Private-key certificate, *see* Symmetric-key certificate
- Private-key encryption, 15
- Probabilistic public-key encryption, 306–312, 318–319
 - Blum-Goldwasser, 308–311
 - Goldwasser-Micali, 307–308
 - security level
 - polynomially secure, 306
 - semantically secure, 306
- Probability, 50
- Probability density function, 176
- Probability distribution, 50
- Probability theory, 50–55
- Probable prime, 136
- Product cipher, 20, 251
- Proof of knowledge, 406, 421, 422
- Proposed Encryption Standard (PES), 279
- Protection lifetime, 553, 578
- Protocol
 - authentication, 493
 - cut-and-choose, 410, 421
 - definition of, 33, 490
 - failure of, 34
 - hybrid, 512
 - identification, *see* Identification
 - key establishment, *see* Key establishment
 - message-independent, 493
 - non-interactive, 493
 - witness hiding, 423
 - zero-knowledge, 405–417
- Provable prime, 134, 142
- Provable security, 43, 533
- Prover, 386
- Pseudo-collision, 371
- Pseudo-Hadamard transform, 266
- Pseudo-noise sequence, 181
- Pseudoprime, 136
 - Euler, 138
 - strong, 139
- Pseudorandom bit generator (PRBG), 173–175
 - ANSI X9.17, 173
 - definition of, 170
 - FIPS 186, 174–175
 - linear congruential generator, 170, 187
- Pseudorandom bit sequence, 170
- Pseudorandom function, 331
- Pseudorandom sequences, 39–41
- Pseudosquares modulo n , 74, 99, 308

- Public key, 26, 27, 544
 - compared vs. symmetric-key, 31–32, 551
 - implicitly-certified, 520–522
 - Public-key certificate, 39, 559–561, 587
 - data part, 559
 - distinguished name, 559
 - signature part, 559
 - Public-key encryption, 25–27, 283–319
 - advantages of, 31
 - disadvantages of, 32
 - ElGamal, 294–298
 - knapsack, 300–306
 - Chor-Rivest, 302–306
 - Merkle-Hellman, 300–302
 - LUC, *see* LUC cryptosystem
 - McEliece, 298–299
 - non-malleable, 311
 - plaintext-aware, 311–312
 - probabilistic, 306–312
 - Blum-Goldwasser, 308–311
 - Goldwasser-Micali, 307–308
 - Rabin, 292–294
 - reversible, 28
 - RSA, 285–291
 - types of attacks, 285
 - Williams, 315
 - PURPLE cipher, 276
 - Puzzle system, 376, 537
- Q**
- Quadratic congruential generator, 187
 - Quadratic non-residues, 70
 - Quadratic residues, 70
 - Quadratic residuosity problem, 99, 127, 307
 - Quadratic sieve factoring algorithm, 95–97, 126
 - implementation reports, 126
 - Quantum computer, 130
 - Quantum cryptography, 48, 535
 - Quotient, 64, 78
- R**
- Rabin one-time signature scheme, 462–464
 - key generation, 463
 - resolution of disputes, 463
 - signature generation, 463
 - signature verification, 463
 - Rabin public-key encryption, 292–294, 315
 - decryption algorithm, 292
 - encryption algorithm, 292
 - key generation, 292
 - security of, 293
 - use of redundancy, 293
 - Rabin signature scheme, 438–442, 482
 - ISO/IEC 9796, 442–444
 - key generation, 438
 - signature generation, 438
 - signature verification, 439
 - use of redundancy, 439
 - Rabin's information dispersal algorithm (IDA), 539
 - RACE/RIPE project, 421, 536
 - Radix representation, 592–593
 - base b , 592
 - binary, 592
 - high-order digit, 593
 - least significant digit, 593
 - low-order digit, 593
 - mixed, 611, 630
 - most significant digit, 593
 - precision, 593
 - radix b , 592
 - Ramp schemes, *see* Secret sharing
 - Random bit generator, 39–41, 171–173
 - cryptographically secure pseudorandom bit generator, *see* Cryptographically secure pseudorandom bit generator (CSPRBG)
 - definition of, 170
 - hardware techniques, 172
 - pseudorandom bit generator, *see* Pseudorandom bit generator (PRBG)
 - software techniques, 172
 - Random cipher, 225
 - Random cipher model, 246
 - Random function, 190
 - poly-random, 190
 - Random mappings model, 54
 - Random oracle model, 316
 - Random square methods, 94–98
 - Random variable, 51
 - continuous, 176
 - entropy of, 56
 - expected value of, 51
 - mean of, 51
 - standard deviation of, 51
 - variance of, 51
 - Randomized algorithm, 62–63
 - Randomized DES (RDES) block cipher, 278
 - Randomized encryption, 225, 296, 306
 - Randomized stream cipher, 216
 - Range of a function, 46
 - Rate of an iterated hash function, 340
 - Rational numbers, 49
 - RC2 block cipher, 282
 - RC4 stream cipher, 222, 282
 - RC5 block cipher, 269–270, 280–281
 - attacks on, 280–281
 - decryption algorithm, 270
 - encryption algorithm, 270

- key schedule, 270
 - patent, 659
 - test vectors, 270
 - weak keys, 281
 - Real number, 49
 - Real-time, 385
 - Reblocking problem in RSA, 435–436, 482
 - Receipt, 3
 - Receiver, 13
 - Reduced basis, 118
 - Redundancy, 29, 431
 - of English, 245
 - Reflection attack, 417, 530, 540
 - Registration authority, 549
 - Related-key attack on block ciphers, 281
 - Relatively prime, 64
 - Remainder, 64, 78
 - Replay attack, 42, 417
 - Requests for Comments, *see* RFCs
 - Residue list sieve, 128
 - Resilient key establishment protocol, 532
 - Response, 409
 - Retail banking, 648
 - Retail MAC, 650
 - Reverse certificate, 575
 - Reversible public-key encryption scheme, 28
 - Revocation, 3
 - RFCs, 655–656
 - ordering and acquiring, 657
 - Ring, 76–77
 - commutative, 77
 - definition of, 76
 - group of units, 77
 - polynomial, 78–79
 - Rip van Winkle cipher, 216
 - RIPE-MAC, 354, 381
 - RIPEMD hash function, 380
 - RIPEMD-128 hash function, 339, 380
 - RIPEMD-160 hash function, 339, 350
 - ISO/IEC 10118-3 standard, 647
 - Root vertex, 557
 - Rotor-based machine, *see* Cipher machine
 - Round function, 251
 - Round of a product cipher, 20
 - RP**, 63
 - RSA-129 number, 126, 130
 - RSA problem, 98–99, 127, 287
 - security of individual bits, 116
 - RSA pseudorandom bit generator, 185–186
 - RSA public-key encryption, 285–291, 312–315
 - decryption algorithm, 286, 611, 613
 - decryption exponent, 286
 - elliptic curve analogue, 315
 - encryption algorithm, 286
 - encryption exponent, 286
 - key generation, 286
 - modulus, 286
 - patent, 638
 - prime selection, 290
 - recommended modulus size, 290
 - security of, 287–290
 - adaptive chosen-ciphertext attack, 289, 313
 - common modulus attack, 289
 - cycling attacks, 289, 313
 - forward search attack, 288
 - message concealing, 290, 313
 - multiplicative properties, 288
 - polynomially related plaintext, 313
 - relation to factoring, 287
 - small decryption exponent, 288
 - small encryption exponent, 288, 291, 313
 - unbalanced, 314
 - RSA signature scheme, 433–438, 482
 - ANSI X9.31-1 standard, 651
 - bandwidth efficiency, 437
 - ISO/IEC 9796, 442–444
 - key generation, 434
 - patent, 638
 - PKCS #1, 445–447
 - reblocking problem, 435–436, 482
 - redundancy function, 437
 - security of, 434–435
 - signature generation, 434, 613
 - signature verification, 434
 - Run of a sequence, 180
 - Running key generator, 194
 - Runs test, 182, 188
- S**
- S/MIME, 661
 - Safe prime, 537
 - algorithm for generating, 164
 - definition of, 164
 - SAFER block cipher, 266–269, 280
 - attacks on, 280
 - SAFER K-64 decryption algorithm, 269
 - SAFER K-64 encryption algorithm, 268
 - SAFER K-64 key schedule, 268
 - SAFER K-128, 280
 - SAFER SK-64 key schedule, 268
 - SK-128, 280
 - test vectors, 269
 - Salt, 288, 390
 - Schnorr identification protocol, 414–416, 422
 - patent, 639
 - Schnorr signature scheme, 459–460, 484
 - Brickell-McCurley variant, 484

- Okamoto variant, 484
- patent, 639
- signature generation, 459
- signature verification, 460
- SEAL stream cipher, 213–216
 - implementation report, 222
 - patent, 222
 - test vectors, 215
- Sealed authenticator, 361
- Sealed key, 568
- 2nd-preimage resistance, 323, 325
- Secrecy, *see* Confidentiality
- Secret broadcasting scheme, 540
- Secret key, 544
- Secret-key certificate, 588
- Secret sharing, 524–528, 538–540
 - access structure, 526
 - authorized subset, 527
 - dynamic, 527
 - extendable, 526
 - generalized, 526–528
 - ideal, 527
 - information rate, 527
 - multi-secret threshold, 527
 - perfect, 526, 527
 - pre-positioned, 527
 - ramp schemes, 539
 - shared control schemes, 524–525
 - threshold scheme, 525–526
 - verifiable, 527
 - visual cryptography, 539
 - with disenrollment, 528
- Secure channel, 13
- Secure Hash Algorithm (SHA-1), 348
 - ANSI X9.30-2 standard, 651
 - FIPS 180-1 standard, 654
 - ISO/IEC 10118-3 standard, 647
- Secured channel, 13
- Security domain, 570
- Security policy, 545
- Seed, 21, 170
- Selective forgery, 326, 432
- Self-shrinking generator, 221
- Self-synchronizing stream cipher, 194–195
- Semantically secure public-key encryption, 306
- Semi-weak keys of DES, 257
- Sender, 13
- Sequence
 - block of, 180
 - de Bruijn, 203
 - gap of, 180
 - m*-sequence, 197
 - periodic, 180
 - pn-sequence, 181
 - pseudo-noise, 181
 - run of, 180
- Sequence numbers, 399
- Serial test, 181, 188
- Session key, 36, 494
- Session key establishment, 491
- SHA-1, *see* Secure Hash Algorithm (SHA-1)
- Shadow, 538
- Shamir's no-key protocol, 500, 535
- Shamir's threshold scheme, 526, 539
- Shared control schemes, 524–525
- Shares, 524–528, 538
- SHARK block cipher, 281
- Shift cipher, 239
- Short-term key, 553
- Shrinking generator, 211–212
 - implementation report, 221
- Sieving, 97
- Signature, 3, 22–23, 28–30, 425–488
 - arbitrated, 472–473
 - blind, *see* Blind signature scheme
 - designated confirmer, 487
 - deterministic, 427
 - Diffie-Lamport, 485
 - Digital Signature Algorithm (DSA), 452–454
 - ElGamal, 454–459
 - ESIGN, 473–474
 - fail-stop, *see* Fail-stop signature scheme
 - Feige-Fiat-Shamir, 447–449
 - framework, 426–433
 - generation algorithm, 426
 - GMR, 468–471
 - GQ, 450–451
 - group, 488
 - handwritten, 23
 - Merkle one-time, 464–466
 - modified-Rabin, 439–442
 - Nyberg-Rueppel, 460–462
 - on-line/off-line, 486
 - Ong-Schnorr-Shamir (OSS), 482, 486
 - Rabin, 438–442
 - Rabin one-time, 462–464
 - randomized, 427
 - relation to identification, 388
 - resolution of disputes, 30
 - RSA, 433–438
 - Schnorr, 459–460
 - strongly equivalent, 485
 - types of attacks, 432
 - undeniable, *see* Undeniable signature scheme
 - verification algorithm, 426
 - with appendix, 481
 - framework, 428–430
 - ISO/IEC 14888 standard, 648

- PKCS #1, 445–447
- with message recovery, 29
- framework, 430–432
- ISO/IEC 9796 standard, 442–444, 646, 660
- with redundancy, 29
- Signature notarization, 583
- Signature space, 427
- Signature stripping, 510
- Signed-digit representation, 627–628
- Signed-magnitude representation, 593
- Signer, 23
- Significance level, 179
- Signing transformation, 22
- Simple substitution cipher, *see* Mono-alphabetic substitution cipher
- Simulator, 407
- Simultaneous diophantine approximation, 121–122
 - algorithm for, 122
 - unusually good, 121
- Simultaneous multiple exponentiation, 617
- Simultaneously secure bits, 115
- Single-key encryption, 15
- Single-length MDC, 339
- Single-precision integer, 593
- Singleton bound, 506
- SKEME, 661
- SKID2 identification protocol, 402, 421
- SKID3 identification protocol, 402, 421
- SKIP, 661
- SKIPJACK block cipher, 282, 654
- Sliding-window exponentiation, 616
- Small decryption exponent in RSA, 288
- Small encryption exponent in RSA, 288, 291, 313
- Smart card, 387
 - ISO 10202 standard, 652
- Smooth
 - integer, 92
 - polynomial, 112
- Snefru hash function, 380
 - 8×32 S-boxes, 281
- Solovay-Strassen primality test, 138, 165
- Span, 80
- Sparse linear equations, 129
 - conjugate gradient method, 129
 - Lanczos method, 129
 - Wiedemann algorithm, 129
- Special-purpose factoring algorithm, 90
- SPKM, 656, 661
- Split-knowledge scheme, 525
- Splitting an integer, 89
- Spread spectrum, 45
- Square roots, 99–102
 - composite modulus, 101–102, 127
 - prime modulus, 100–101, 127
- SQROOT problem, 101
- Square-free factorization, 123
 - algorithm for, 123, 132
- Square-free integer, 137
- Square-free polynomial, 123
- Stage
 - of an FSR, 202
 - of an LFSR, 195
- Standard deviation, 51
- Standard normal distribution, 176
- Standards, 645–657, 660–661
 - ANSI, 648–651
 - FIPS, 654–655
 - IEEE, 660
 - Internet, 655–656
 - ISO/IEC, 645–648, 651–653
 - PKCS, 656
 - RFC, 655–656
 - X.509, 653
- Station-to-station (STS) key agreement, 519, 538
- Statistical test, 175–185, 188–189
 - autocorrelation test, 182
 - frequency test, 181
 - hypothesis, 179
 - Maurer’s universal statistical test, 183–185, 189
 - one-sided test, 179
 - poker test, 182
 - polynomial-time, 171
 - runs test, 182
 - serial test, 181
 - significance level, 179
 - two-sided test, 180
- Statistical zero-knowledge protocol, 424
- Steganography, 46
- Step-1/step-2 generator, 220
- Stirling numbers, 53
- Stirling’s formula, 59
- Stop-and-go generator, 220
- Stream cipher, 20–21, 191–222
 - A5, 222
 - attacks on
 - correlation attack, 206, 218
 - inversion attack, 219
 - linear consistency attack, 219–220
 - linear cryptanalysis, 219
 - linear syndrome attack, 218
 - lock-in, 221
 - cellular automata, 222
 - classification, 192–195
 - clock-controlled generator, 209–212
 - alternating step generator, 209–211
 - m -sequence cascade, 221

- p*-cycle cascade, 220
 - self-shrinking generator, 221
 - shrinking generator, 211–212
 - step-1/step-2 generator, 220
 - stop-and-go generator, 220
 - comparison with block ciphers, 192
 - FISH, 222
 - GOAL, 219
 - initial state, 193, 194
 - keystream, 193, 194
 - next-state function, 193
 - nonlinear combination generator, 205–208
 - Geffe generator, 206
 - multiplexer generator, 220
 - multispeed inner-product generator, 220
 - Pless generator, 218
 - summation generator, 207
 - nonlinear filter generator, 208–209
 - knapsack generator, 209
 - one-time pad, 192–193
 - output function, 193, 194
 - PIKE, 222
 - randomized stream cipher, 216
 - RC4, 222
 - Rip van Winkle cipher, 216
 - SEAL, 213–216
 - self-synchronizing stream cipher, 194–195
 - synchronous stream cipher, 193–194
 - Strict avalanche criterion (SAC), 277
 - String-replacement representation, 628–629
 - Strong collision resistance, 324
 - Strong equivalent signature schemes, 485
 - Strong liar, 139
 - Strong one-way hash function, 325
 - Strong prime, 149–150
 - algorithm for generating, 150
 - definition of, 149, 291
 - Hellman-Bach patent, 643
 - usage in RSA, 291
 - Strong pseudoprime, 139
 - Strong pseudoprime test, *see* Miller-Rabin primality test
 - Strong witness, 139
 - Subexponential-time algorithm, 60
 - Subfield, 77
 - Subgroup, 76
 - Subliminal channel, 485
 - broadband, 485
 - narrowband, 485
 - Subset sum problem, 61, 117–122, 190
 - meet-in-the-middle algorithm, 118
 - naive algorithm, 117
 - superincreasing, 300
 - using L^3 algorithm, 120
 - Subspace of a vector space, 80
 - Substitution cipher, 17–18, 238–241
 - homophonic, 17, 240
 - mono-alphabetic, 17, 239
 - affine cipher, 239
 - Caesar cipher, 239
 - shift cipher, 239
 - unicity distance of, 247
 - polyalphabetic, 18
 - polygram, 239
 - Hill cipher, 240
 - Playfair cipher, 239
 - Substitution-permutation (SP) network, 251
 - Summation generator, 207, 218
 - Superincreasing subset sum problem, 300
 - algorithm for solving, 300
 - Superuser, 389
 - Surjective function, 46, 50
 - SWIFT, 586
 - Symmetric cryptographic system, 544
 - Symmetric key, 544
 - compared vs. public-key, 31–32, 551
 - Symmetric-key certificate, 554–555, 587
 - Symmetric-key encryption, 15–21
 - advantages of, 31
 - block cipher, 223–282
 - definition of, 15
 - disadvantages of, 31
 - stream cipher, 191–222
 - Synchronous stream cipher, 193–194
 - binary additive stream cipher, 194
 - Syndrome decoding problem, 190, 423
- ## T
- Tapper, 13
 - TEA block cipher, 282
 - TEMPEST, 45
 - Teraflop, 44
 - Terminal key, 552
 - Test vectors
 - DES, 256
 - FEAL, 262
 - IDEA, 265
 - MD4, 345
 - MD5, 345
 - MD5-MAC, 358
 - RC5, 270
 - RIPEMD-160, 345
 - SAFER, 269
 - SHA-1, 345
 - 3-WAY block cipher, 281
 - Threshold cryptography, 534
 - Threshold scheme, 525–526
 - Blakley, 538

- Shamir, 526, 539
 - Ticket, 501, 570, 586
 - Time-memory tradeoff, 236, 273
 - Time-variant parameter, 362, 397–400, 497
 - nonce, 397
 - random numbers, 398–399
 - sequence numbers, 399
 - timestamps, 399–400
 - Timestamp, 3, 399–400, 420, 581–582
 - agent, 550
 - Toeplitz matrix, 382
 - Transaction authentication, 362
 - Transformation, 6
 - Transinformation, 57
 - Transposition cipher, 18, 238
 - compound, 238
 - simple, 18, 238
 - unicity distance of, 246
 - Trapdoor one-way function, 9, 26
 - Trapdoor predicate, 318
 - Tree authentication, 376
 - patent, 637
 - Trinomial, 154
 - Triple encryption, 235–237, 272
 - Triple-DES, 272, 651
 - ANSI X9.52 standard, 651
 - Triple-inner-CBC mode, 237
 - Triple-outer-CBC mode, 237
 - Truncated differential analysis, 271, 280
 - Trust model, 572
 - centralized, 573
 - directed graph, 575
 - distributed, 575
 - hierarchy with reverse certificates, 575
 - rooted chain, 573
 - separate domains, 573
 - strict hierarchical, 573
 - Trusted server, 491
 - Trusted third party (TTP), 30, 36, 491, 547–550, 581–584
 - authentication server, 549
 - certificate directory, 549
 - certification authority (CA), 548
 - functionally trusted, 39
 - in-line, 547
 - KDC, *see* Key distribution center (KDC)
 - key access server, 549
 - key escrow agent, 550
 - key generator, 549
 - key management facility, 549
 - key server, 549
 - KTC, *see* Key translation center (KTC)
 - name server, 549
 - notary agent, 550
 - off-line, 548
 - on-line, 547
 - registration authority, 549
 - timestamp agent, 550
 - unconditionally trusted, 39
 - TTP, *see* Trusted third party (TTP)
 - Turing-Kolmogorov-Chaitin complexity, 217
 - Two's complement representation, 594
 - 2-adic span, 218
 - Two-bit test, 181
 - Two-key triple-encryption, 235
 - chosen-plaintext attack on, 236
 - known-plaintext attack on, 237
 - Two-sided statistical test, 180
 - Type I error, 179
 - Type II error, 179
- ## U
- Unbalanced RSA, 314
 - Unblinding function, 475
 - Unconcealed message, 290
 - Unconditional security, *see* Perfect secrecy, 533
 - Unconditionally trusted third party, 39
 - Undeniable signature scheme, 476–478, 487–488
 - Chaum-van Antwerpen, 476–478
 - confirmer, 487
 - Unicity distance
 - definition of, 246
 - known-plaintext, 235
 - of a cascade cipher, 272
 - of a mono-alphabetic substitution cipher, 247
 - of a transposition cipher, 246
 - Unilateral authentication, 387, 401–402, 405, 494
 - Union of sets, 49
 - Unique factorization domain, 81
 - Unit, 68, 77, 103, 114
 - Universal classes of hash function, 376
 - Universal exponent, 287
 - Universal forgery, 482
 - Universal one-way hash function, 377
 - Universal statistical test, *see* Maurer's universal statistical test
 - UNIX passwords, 393–394
 - Unsecured channel, 13
 - Unusually good simultaneous diophantine approximation, 121, 317
 - Userid, 388
- ## V
- Validation, 3
 - Validation parameters, 462
 - Variance, 51
 - Vector space, 79–80
 - dimension of, 80
 - standard basis, 80

subspace of, 80
 Vector-addition chains, 622–623
 Verifiable secret sharing, 527, 539
 Verification algorithm, 426
 Verification transformation, 22
 Verifier, 23, 385, 386
 Vernam cipher, *see* One-time pad
 Vigenère cipher, *see* Polyalphabetic substitution cipher
 Visual cryptography, 539

W

WAKE block cipher, 282
 Weak collision resistance, 324
 Weak keys of DES, 257
 Weak one-way hash function, 325
 Wheatstone disc, 274
 Wholesale banking, 648
 Wiedemann algorithm, 129
 Williams' public-key encryption, 315
 Witness, 135, 409
 Euler, 137
 Fermat, 136
 strong, 139
 Witness hiding protocol, 423
 Witness indistinguishability, 423
 Witnessing, 3
 Work factor, 44
 historical, 44
 Worst-case running time, 58
 Wyner's wire-tap channel, 535

X

X.509 authentication protocol, 536
 three-way, 512
 two-way, 511
 X.509 certificate, 587
 X.509 standard, 653
 XOR, *see* Exclusive-or

Y

Yuval's birthday attack, 369

Z

Zero-knowledge identification, 405–417, 421–424
 Brickell-McCurley, 423
 comparison of protocols, 416–417
 constrained linear equations problem, 423
 extended Fiat-Shamir, 422
 Feige-Fiat-Shamir, 410–412
 Fiat-Shamir (basic version), 408
 Fischer-Micali-Rackoff, 422
 GQ, 412–414
 Ohta-Okamoto, 422
 permuted kernel problem, 423

Schnorr, 414–416
 syndrome decoding problem, 423
 Zero-knowledge protocol, 405–417, 421–424
 auxiliary-input, 423
 black-box simulation, 423
 challenge, 409
 completeness, 406
 computational, 407
 extracting secret, 406
 for possession of discrete log, 422
 parallel version, 412
 perfect, 407
 proof of knowledge, 406, 421, 422
 proof of membership, 421
 response, 409
 simulator, 407
 soundness, 406
 statistical, 424
 witness, 409
 Ziv-Lempel complexity, 217
 \mathbb{Z}_p -operation, 82
 ZPP, 63