Vocabulary List

Lines of the form A/B are two (or more) separate, related terms.

*-Property
Advanced Encryption Standard (AES)
BAN logic
Bell-LaPadula Model (BLP)
Caesar Cipher
Chinese Wall Policy
Clark-Wilson policy
CodeRed (3 versions)
Common Criteria
Diffie-Hellman algorithm
Huffman encoding
Lempel-Ziv algorithm
Lipner's integrity matrix model
Low Water Mark Policy
MD4/MD5/SHA1
Needham-Schroeder Protocol
Otway-Rees Protocol
Phil Zimmermann
Pretty Good Privacy (PGP)
Principle of Easiest Penetration
Principle of Least Privilege
Ring Policy
Shared Resource Matrix Methodology
Strict Integrity Policy
Vigenere cipher/tableau
X.509 access control list (ACL)
access control matrix (ACM)
access control policy
accurate/precise
adaptive chosen plaintext attack
addRoundKey (AES)
annualized loss expectancy
asymmetric cipher
authentication
availability
bandwidth/capacity/throughput
belief logic
block cipher
block encryption mode
breakable
capability-based system
cascade cipher
certificate
certification authority
certification chain
chosen ciphertext attack
chosen plaintext attack
cipher block chaining mode (CBC)
cipher feedback mode
ciphertext-only attack
collision resistant (strong, weak)
columnar transposition
compression
confidentiality
confusion
consumer problem/producer problem
countermeasure
covert channels
cryptanalysis
cryptographic hash functions
cryptographic protocol
cryptography
cryptosystem
denial of service (DoS)
diffusion
digital signature
discrete/zero-memory source
discretionary access control (DAC)
distributed denial of service (DDoS)
dominates relation
efficiency
e-mail compatibility
electronic code book mode (ECB)
encoding
encryption/decryption
entropy
evaluation assurance level (EAL)
false negative/positive
first-order model, etc.
freshness
fundamental theorem of the noiseless channel
fundamental theorem of the noisy channel
hierarchical levels
idealization
impersonation attack
information content
information flow policies
information theory
integrity
integrity *-property

integrity levels/policies
interleaving attack
intrusion detection system (IDS)
intrusion prevention system (IPS)
key distribution/management/revocation
key exchange problem
key stream generation modes
keyed cipher/keyless cipher
keyspace
known key attack
known plaintext attack
lattice
lattice-based security
local/remote attacks
lossless
lossy
malleable algorithm
man-in-the-middle attack
mandatory access controls (MAC)
message digest
metapolicy
mixColumns (AES)
modes of usage
monoalphabetic cipher
multi-level security (MLS)
need-to-know categories
noisy/noiseless
non-alterable
non-interference
non-repudiation
nonce
objects
one-time pad
one-way function
packet sniffing
partial order
passphrase-based key
perfect cipher
plaintext/ciphertext
policy
polyalphabetic substitution
prefix-free
preimage resistant, second preimage resistant
principal
private key ring
product cipher
protection profile (PP)
protocol
pseudo-random number generator (PRNG)
public key algorithm
public key infrastructure (PKI)
public key ring
radix-64 conversion
read/write/execute/create/destroy permissions
replay attack
role-based access control (RBAC)
salt
security
security labels/levels
security model/policy
security target (ST)
segmentation
sender/receiver
separation of duty
separation of function
session key
shared-key authentication protocol
shiftRows (AES)
simple integrity property
simple security property
simple substitution cipher
static seed in PRNG
storage channels
stream cipher
strong cryptosystem
strong tranquility property
subBytes (AES)
subjects
substitution cipher
symmetric channel
symmetric cipher/secret key algorithm
syn flooding
system attribute
system low/high
target of evaluation (TOE)
timestamp
timing channels
total order
transposition cipher
unforgeable
uniquely decodable
water mark policy
weak tranquility property
zero-order model