Vocabulary List

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

*-Property
3DES
Advanced Encryption Standard (AES)
Bell-LaPadula Model (BLP)
Caesar Cipher
Chinese Wall Policy
Clark-Wilson policy
CodeRed (3 versions)
Common Criteria
Diffie-Hellman algorithm
Feistel cipher
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
access control list (ACL)
access control matrix (ACM)
access control policy
accurate/precise
adaptive chosen plaintext attack
addRoundKey
asymmetric cipher
authentication
availability
bandwidth/capacity/throughput
block cipher
block encryption mode
breakable
buffer overflow
capability-based system
cascade cipher
certificate
certification authority
chosen ciphertext attack
chosen plaintext attack
cipher block chaining mode (CBC)
ciphertext-only attack
collision resistant (strong, weak)
columnar transposition
compression
confidentiality
confusion
countermeasure
covert channels
cryptanalysis
cryptographic hash functions
cryptographic protocol
cryptography
cryptosystem
denial of service (DoS)
diffusion
digital signature
discretionary access control (DAC)
distributed denial of service (DDoS)
dominates relation
double DES
e-mail compatibility
electronic code book mode (ECB)
encryption/decryption
false negative
false positive
freshness
hierarchical levels
information flow policies
ingress filtering
integrity *-property
integrity
integrity levels/policies
interleaving attack
intrusion detection system (IDS)
intrusion prevention system (IPS)
key distribution
key exchange problem
key stream generation modes
keyed cipher/keyless cipher
keyspace
known plaintext attack
lattice-based security
local/remote attacks
malleable algorithm
mandatory access controls (MAC)

metapolicy
mixColumns
modes of usage
monoalphabetic cipher
multi-level security (MLS)
need-to-know categories
noisy/noiseless
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
preimage resistant, second preimage resistant
principal
private key ring
product cipher
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)
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
simple integrity property
simple security property
simple substitution cipher
static seed in PRNG
storage channels
stream cipher
strong (encryption)
strong tranquility property
subBytes
subjects
substitution cipher
symmetric cipher/secret key algorithm
syn flooding
system attribute
system low/high
timestamp
timing channels
total order
transposition
trapdoor/backdoor
unforgeable
water mark policy
weak tranquility property