Two fundamental services: confidentiality and authentication. Key management is associated with these two services.

Encryption/Decryption: to achieve confidentiality
- symmetric ciphers
  - classical ciphers
  - block ciphers
  - modern ciphers
- public-key system
  - RSA

Authentication:
- MAC
- Hash function
  - MD5
  - SHA-1
- HMAC
- Authenticated key exchange protocol (i.e. Needham-Schroeder protocol)
  - Denning protocol
  - Neumann protocol
- Digital signature

Key management (distribution)
- session key distribution
  - Needham-Schroeder protocol (KDC)
  - Diffie-Hellman protocol (public-key like)
- public key distribution
  - certificate
  - CA (certificate authority)

Applications: Kerberos, X.509, PGP, S/MIME, IPsec, SSL/TLS, SET, Intrusion Detection, Firewall, viruses and worms

Kerberos (KDC)
- AS and TGS
- ticket
- counter replay attacks

X. 509
- directory service: supply certificate
- CA hierarchy (tree)
- Chain of certificate
- Revocation
PGP
- key-rings
- public-key management (anarchy)

IPsec
- SA
- ESP and AH protocols
- Transport and Tunnel modes
- Key management
  - ISAKMP
  - IKE

SSL/TLS
- SSL record protocol
- SSL handshake protocol
- Session reuse

SET
- Dual signature

Intrusion Detection
- two approaches
- detection metrics
- password management

Firewall
- classification
- configuration
- access control
- BLP model

Malicious software
- viruses and worms
- buffer overflow
- countermeasures