Chapter 1

Goals

Passive

Confidentiality (protect info)

- Snooping — unauthorized access / interception of data
- Traffic analysis — monitoring online traffic

Active

Integrity (changes by authorized entity through mechanism)

- Modification — intercept msg & change
- Spoofing / Masquerading — impersonate somebody
- Replaying — obtain copy & msg & replay
- Repudiation — deny send / receive msg

Active

Availability (info constantly changed, must accessible to entity)

(DoS)

- Denial of service — slow down / interrupt service

Attacks

Services

- Data confidentiality
- Data integrity — anti-change, anti-replay
- Authentication — peer entity, data origin
- Nonrepudiation — proof of origin, proof of delivery
- Access control

Mechanisms

- Encipherment, routing control
- E, digital signature, data integrity
- E, ds, authentication exchanges
- ds, di, notarization
- access control mechanism
- traffic padding

Techniques

- Cryptography
  - secret writing
- Steganography
  - covered writing (image)