Applied Cryptography and Network Security

- -Introduction
- Security Golas
- Cryptographic Attacks
- Security Services and Mechanisms
- Classification of Cryptosystems

- Cryptography
- Cryptanalysis
- Cryptology

- Confidentiality
- Integrity
- Availability

Attacks can be occurred on network:

- Disclosure
- Traffic analysis

-Masquerading

- Modification
- Repudiation
- Replaying

Attacks	Passive/Active	Threatening
Snooping Traffic Analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of Service	Active	Availability

Data Confidentiality- protection of data from unauthorized disclosure

Data Integrity - assurance that data received is as sent by an authorized entity

Authentication - assurance that the communicating entity is the one claimed

Non Repudiation - protection against denial by one of the parties in a communication

Access Control - prevention of the unauthorized use of a resource

-Encipherment
- Data Integrity
- Digital Signature
- Authentication Exchange
- Traffic Padding
- Routing Control
- Access control

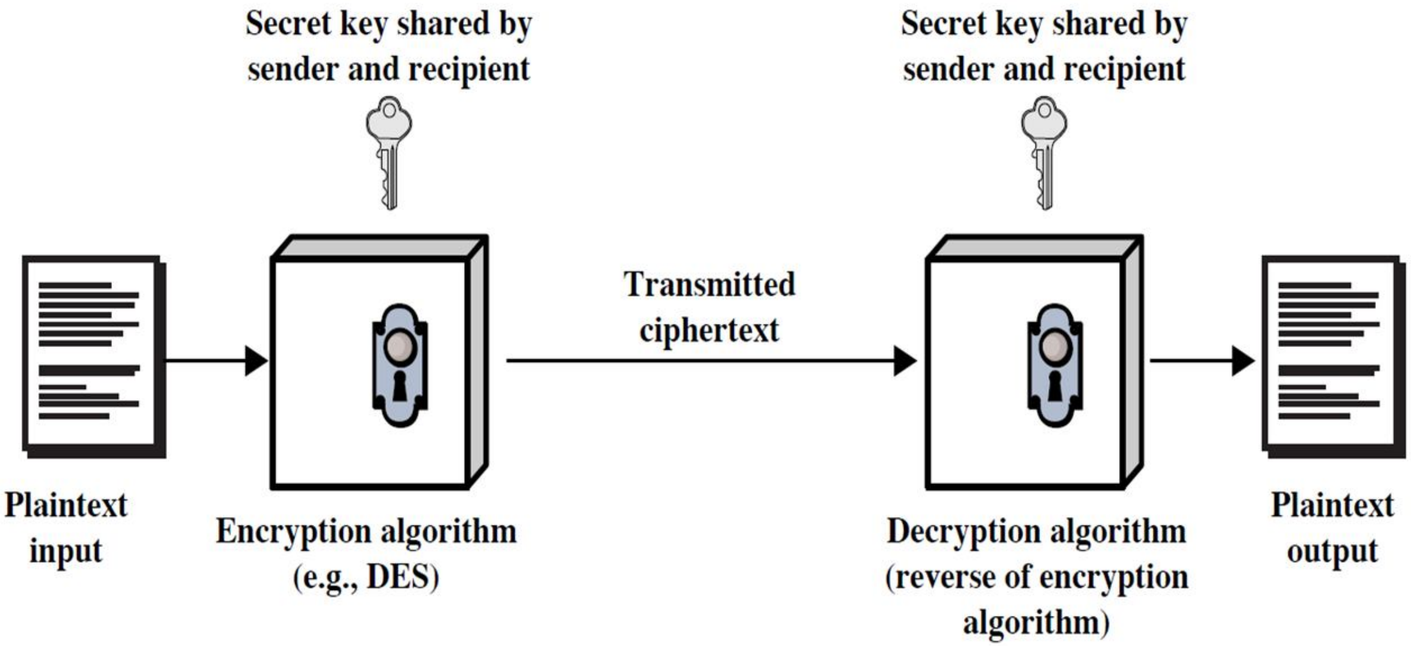
Security Service	Security Mechanism
Data Confidentiality	Encipherment, Routing control, Traffic padding
Data Integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, data integrity, authentication exchanges
Nonrepudiation	Digital signature
Access control	Access control mechanism

Classification of cryptosystems

Cryptosystems are classified based on the following:

- Type of operations used
- Number of keys used
- The way in which plain text is processed

Symmetric Cipher Model


Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Symmetric Encryption

- Mathematically:

$$Y = E_K(X) \quad \text{or} \quad Y = E(K, X)$$
$$X = D_K(Y) \quad \text{or} \quad X = D(K, Y)$$

- X = plaintext
- Y = ciphertext
- K = secret key
- E = encryption algorithm
- D = decryption algorithm
- Both E and D are known to public

Product Ciphers

- Uses a sequence of substitutions and transpositions
  - Harder to break than just substitutions or transpositions
- This is a bridge from classical to modern ciphers.

Cryptanalysis

- Objective: to recover the plaintext of a ciphertext or, more typically, to recover the secret key.

.

Cryptanalytic Attacks

- May be classified by how much information needed by the attacker:
    - Ciphertext-only attack
    - Known-plaintext attack
    - Chosen-plaintext attack
    - Chosen-ciphertext attack