Cryptography & Network Security

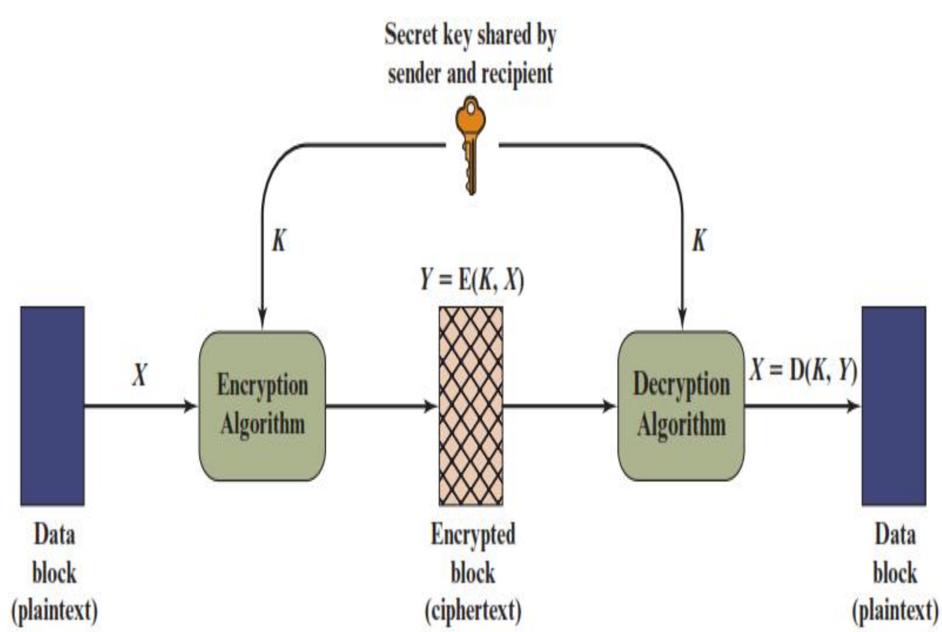
UNIT I

Symmetric Cipher Model

A Symmetric Cipher is a cryptographic system that uses the same key for both encryption and decryption. This is one of the oldest and most widely used cryptographic techniques.

Components of Symmetric Cipher Model

- **Plaintext (P):** The original message that needs to be secured.
- **Encryption Algorithm:** A mathematical function that transforms plaintext into ciphertext using a key.
- **Secret Key (K):** Shared between sender and receiver. It must be kept secret.
- **Ciphertext (C):** The encrypted message.
- **Decryption Algorithm:** The reverse process that converts ciphertext back into plaintext using the same key.



Mathematical Form

Encryption: $C = E\_K(P)$

Decryption: $P = D\_K(C)$

where E_K and D_K are the encryption and decryption transformations under key K.

Features

- **Same Key:** Sender and receiver share the same secret key.
- **Speed:** Typically faster than asymmetric encryption.
- **Security Dependency:** Overall security depends on the secrecy (confidential distribution & storage) of the key.

Mathematical Example – Caesar Cipher

Consider the Caesar Cipher, a simple historical symmetric substitution cipher. We map the alphabet A–Z to numbers 0–25 and shift each letter by a fixed key K modulo 26.

Given: Key $K = 3$

Alphabet Mapping: A=0, B=1, ..., Z=25

Encryption

Formula: $C = (P + K) \bmod 26$

Plaintext: "HELLO"

Numeric: H=7, E=4, L=11, L=11, O=14

Apply K=3:

Letter	Num	Num+K	(Num+K) mod 26	Cipher Letter
H	7	7+3=10	10	J
E	4	4+3=7	7	H
L	11	11+3=14	14	O
L	11	11+3=14	14	O
O	14	14+3=17	17	R

Ciphertext: "JHOOR"

Decryption

Formula: $P = (C - K) \bmod 26$

Ciphertext: "JHOOR"

Numeric: J=9, H=7, O=14, O=14, R=17

Subtract K=3:

Letter	Num	Num-K	(Num-K) mod 26	Plain Letter
J	9	9-3=6	6	G
H	7	7-3=4	4	E
O	14	14-3=11	11	L
O	14	14-3=11	11	L
R	17	17-3=14	14	O

Recovered Plaintext: "GELLO" (Note: This illustrates a common indexing slip; correct mapping for H=7 should recover HELLO. See correction below.)

Correction: Using zero-based mapping A=0, H=7, J=9. Decryption (9−3)=6 which corresponds to G if 0-indexed A=0; however in our original mapping we associated 7 with H, so ciphertext letter J (10) should have been used, not

9. To avoid such off-by-one errors, be consistent: A=0, B=1,...,Z=25. Then J=9 indeed maps to 9; (9−3)=6→G, which shows that our encryption earlier produced J from H correctly only if H=7 giving 7+3=10→J (index10). Thus ciphertext J is index10, not 9. The corrected numeric row is below.

Corrected Decryption Table

Cipher Letter	Index	Index-K	(Index-K) mod 26	Plain Letter
J	10	10-3=7	7	H
H	7	7-3=4	4	E
O	14	14-3=11	11	L
O	14	14-3=11	11	L
R	17	17-3=14	14	O

Recovered Plaintext (corrected): "HELLO"