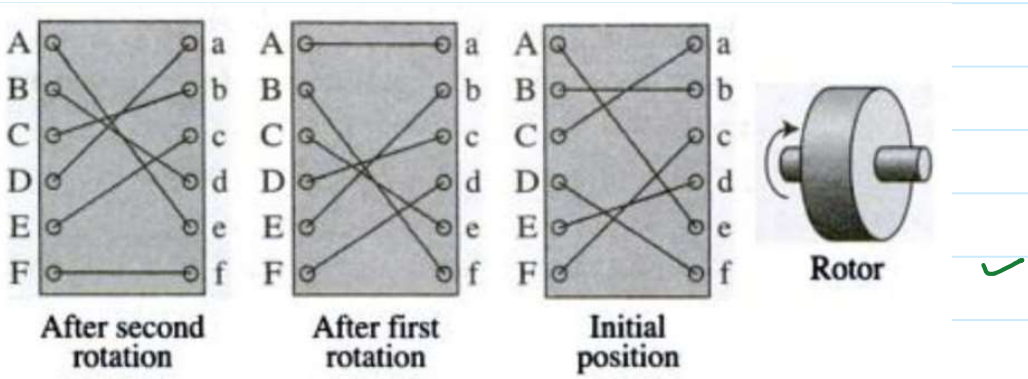
Lecture-4 (MC407)

Traditional Ciphers:

(1) Substitution Ciphers
- Additive Cipher
- Multiplicative Cipher
- Affine cipher
- Autokey Cipher
- playfair cipher
- Vigenere Cipher
- Hill cipher
- One-time Pad
- Rotor Cipher

(2) Transposition Ciphers

Rotor Cipher:



plaintext: bee

Ciphertext: BCA

Enigma Machine:

Transposition Ciphers

It reorders the symbols.

Types

1. Keyless Transp. Cip. ✓ (No key)
2. Keyed Tran. " (Key will be used for encryption & decryption)

1. Keyless Transp. Ciphers.

(i) rail-fence cipher:

plaintext: he is coming.

h	i	c	m	n	
e	s	o	i	g	

ciphertext: hicmnesoig

h e i
s c o
m i n
g x g.

ciphertext: hsmgecixio
ng

Alice & Bob may agree on the no. of rows (say 3)

h	s	m	g
e	c	i	x
i	o	n	g

Ciphertext: hsmgecixiong

2. Keyed Transposition Cipher:

plaintext: start the attack early morning.

Key: $\begin{bmatrix} 2 & 1 & 4 & 5 & 3 \\ 1 & 2 & 3 & 4 & 5 \end{bmatrix}$ ✓✓ [2 1 4 5 3] - Encryption key.

start theat tacke arlym ornin gabcd

ciphertext: tsrta htate atkec raylm roinn agcdb.

Decryption key: [2 1 5 3 4] ✓

Combination of Keyless Trans. cipher & keyed transp. cipher can be used to get a stronger cipher.

plaintext: enemy attacks tonight

$$\begin{bmatrix} e & n & e & m & y \\ a & t & t & a & c \\ k & s & t & o & n \\ i & g & h & t & z \end{bmatrix}$$

$$\downarrow \quad \text{key: } \begin{bmatrix} 3 & 1 & 4 & 5 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{bmatrix}$$

$$\begin{bmatrix} E & E & M & Y & N \\ T & A & A & C & T \\ T & K & O & N & S \\ H & I & T & N & G \end{bmatrix}$$

ciphertext : ETTHEAKI - - ..

1. Stream Ciphers 2. Block Ciphers.

1. Stream Ciphers : Encryption / Decryption are done one letter at a time.

$P = P_1 P_2 P_3 \cdots$, $C = C_1 C_2 C_3 \cdots$, $K = k_1 k_2 k_3 \cdots$

P ↓ plaintext stream, C ↓ Ciphertext stream, K ↓ Key stream

$C_i = E_{k_i}(P_i)$

Additive Cipher : $C_i = (P_i + k) \bmod 26$

$K = kkkk \cdots$

Substitution Cipher

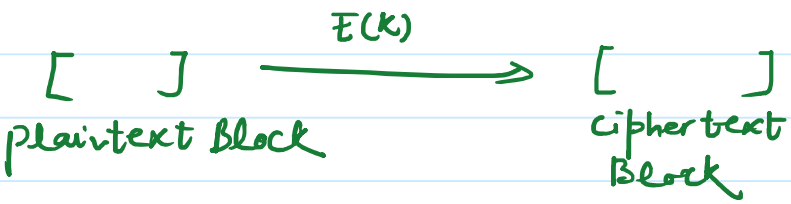
a	b	c	d	- - -
B	F	G	K	- - -

Vigenere

$K = k_1 k_2 \cdots k_m, k_1 k_2 \cdots k_m \cdots$

↓ key stream

2. Block Cipher : Encryption/decryption is done blockwise



Ex : 1. Playfair Cipher : (Block size is 2)

2. Hill Cipher

Block Ciphers are polyalphabetic ciphers.