CHAPTER FOUR

CRYPTANALYSIS OF TRANSPOSITION CIPHER PROBLEMS USING COMBINATORIAL OPTIMIZATION PROBLEMS TECHNIQUES

4.1 Terminology

- **Cryptography:** is the study of principles and techniques by which information can be concealed in ciphertexts and later revealed by legitimates users employing the secret key. Its concern **Encryption** and **Decryption** processes
- **Cryptanalysis:** is the science (and art) of recovering information from ciphertexts without knowledge of the key.
- **Encryption**: is a process of encoding a message so that the meaning of the message is not obvious.
- **Decryption:** is the reverse process: transforming an encrypted message back into its normal form.
- **Cryptosystem**: A system for encryption and decryption.
- The original form of a message is known as **Plaintext**, and the encrypted form is called **Ciphertext**.

4.2 Notations

- M: plaintext message, $P = [m_1,m_2,...,m_n]$.
- C: ciphertext can be written as $C = [c_1,c_2,...,c_m]$.
- E : is the encryption algorithm.
- D is the decryption algorithm.

- the transformations between P and C are $C = E(M)$ and $M = D(C)$, so $M = D(E(M))$.
- K: key, so that the $C = E(K,M)$. and $M = D(K,E(K,M))$.

4.3 Simple Transpositions

The goal of **transposition** is diffusion, spreading the information from the message or the K out widely across the C. Because a transposition is a rearrangement of the symbols of a message, it is also known as a **permutation**.

The **columnar transposition** is a rearrangement of the characters of the plaintext into columns.

The following example is a five-column transposition. The plaintext characters are separated into blocks of five and arranged one block after another, as shown here.

c_1	c_2	c_3	c_4	c_5
c_6	c_7	c_8	c_9	c_{10}
c_{11}	c_{12}	etc.		

The resulting C is formed by transversing the columns.

$c_1c_6c_{11}\ldots c_2c_7c_{12}\ldots c_3c_8$,etc.

Example (4.1): you would write the plaintext message as:

T	H	I	S	I
S	A	M	E	S
S	A	G	E	T
O	S	H	O	W
H	O	W	A	C
O	L	U	M	N
A	R	T	R	A
N	S	P	O	S
I	T	I	O	N
W	O	R	K	S

The resulting ciphertext would then be read off as:

tssoh oaniw haaso lrsto imghw
utpir seeoa mrook istwc nasns

The length of this message happened to be a multiple of five, so all columns came out the same length.

Let E and $D=E^{-1}$ be encryption and decryption function of TCP respectively. The ciphertext C_m of TCP, where $1\leq m\leq n!$, using arbitrary encryption key EK_m with length n is:

$$C_m = E(M,EK_m) \qquad \ldots(E)$$

Let DK_m be the decryption key corresponding to the EK_m (σ of n-sequence) for ciphertext C_m of TCP and P_m be the decrypted text using DK_m, is:

$$M=M_m=D(C_m,DK_m) \qquad \ldots(D)$$

Its clear that C_m (and M_m) consists of n columns.

Example (4.2): Let's have the following PT message (showed in uppercase letters):

1	2	3	4
T	H	E	Q
U	I	C	K
B	R	O	W
N	F	O	X
J	U	M	P
S	O	V	E
R	T	H	E
L	A	Z	Y
D	O	G	X

The size of the permutation is known as the period. For this example a simple transposition cipher with a period of 4 is used. Let $\Pi = (3,1,4,2)$ be encryption key. Then the message is broken into blocks of 4 characters. Upon encryption the 3[rd] character in the block will be moved to position 1, the 1st to position 2, the 4th to position 3 and the 2nd to position 4.

3	1	4	2
e	t	q	h
c	u	k	i
o	b	w	r
o	n	x	f
m	j	p	u
v	s	e	o
h	r	e	t
z	l	y	a
g	d	x	o

The resulting ciphertext (in lowercase letters) would then be read off as:

etqhc ukiob wronx fmjpu vseoh retzl yagdx o

Notice also that decryption can be achieved by following the same process as encryption using the "inverse" of the encryption permutation. In this case the decryption key (DK), Π^{-1} is equal to (2, 4, 1, 3).