TRANSPOSITIONS CIPHER

A transposition is not a permutation of alphabet characters, but a permutation of places. Transposition or Permutation cipher works by breaking a message into fixed size blocks, and then permuting the characters within each block according to a fixed permutation, say P. The key to the transposition cipher is simply the permutation P. So, the transposition cipher has the property that the encrypted message i.e. the cipher text contains all the characters that were in the plain text message. In the other word, the unigram statistics for the message are unchanged by the encryption process.

In this method, the message is written in a rectangle, row by row. Reading the message off, row by row, but permuting the order of the columns. The order of the columns then become the key to the algorithm.

Example 1

Encrypt The plain text is**:** "***breaking transposition cipher***" use Transpositions cipher if the Key is equal to {4 1 3 5 7 6 2}.

Answer

Encryption process

In this case, the message is broken into block of seven characters because the key is *seven numbers*.

Figure 2.10.a shows the key and Fig. 2.10.b shows the encryption process of the previously described transposition cipher.

It can be noticed that the random string "X" was appended to the end of message to enforce a massage length, which is a multiple of the block size.

1	2	3	4	5	6	7
b	r	e	a	k	i	n
g	t	r	a	n	s	p
o	s	i	t	i	o	n
c	i	p	h	e	r	x

a

4	1	3	5	7	6	2
a	b	e	k	n	i	r
a	g	r	n	p	s	t
t	o	i	i	n	o	s
h	c	p	e	x	r	i

-b-

Table 2.10: Example of the transposition cipher encryption process

The cipher text is: **abeknir** agrnpst **toiinos** hcpexri

Cipher text "abeknir agrnpst **toiinos** hcpexri"

Decryption

4	1	3	5	7	6	2
a	b	e	k	n	i	r
a	g	r	n	p	s	t
t	o	i	i	n	o	s
h	c	p	e	x	r	i

-a-

1	2	3	4	5	6	7
b	r	e	a	k	i	n
g	t	r	a	n	s	p
o	s	i	t	i	o	n
c	i	p	h	e	r	x

b

Example of the transposition cipher decryption process

Example 2

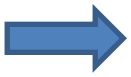
Encrypt the following message using transport cipher method , column by column

Text = " to be or not to be that is the quesion"

Key = 5 2 3 1 4 6

Encryption process

1	2	3	4	5	6
t	o	b	e	o	r
n	o	t	t	o	b
e	t	h	a	t	i
s	t	h	e	q	u
e	s	i	o	n	x



5	2	3	1	4	6
o	o	b	t	e	r
o	o	t	n	t	b
t	t	h	e	a	i
q	t	h	s	e	u
n	s	i	e	o	x

Ciphertext = "oobter ootntb ttheai qthseu nsieox"

Decryption Process

5	2	3	1	4	6
o	o	b	t	e	r
o	o	t	n	t	b
t	t	h	e	a	i
q	t	h	s	e	u
n	s	i	e	o	x

1	2	3	4	5	6
t	o	b	e	o	r
n	o	t	t	o	b
e	t	h	a	t	i
s	t	h	e	q	u
e	s	i	o	n	x

Plaintext " to be or not to be that is the quesion "

ClassWork

Encrypt the plaintext is "***The nose is pointing down and the houses are getting bigger***" use Transpositions cipher if the Key is " ***3 5 2 1 4*** ".

1	2	3	4	5
t	h	e	n	o
s	e	i	s	p
o	i	n	t	i
n	g	d	o	w
n	a	n	d	t
h	e	h	o	u
s	e	s	a	r
e	g	e	t	t
i	n	g	b	i
g	g	e	r	x

3	5	2	1	4
e	o	h	t	n
i	p	e	s	s
n	i	i	o	t
d	w	g	n	o
n	t	a	n	d
h	u	e	h	o
s	r	e	s	a
e	t	g	e	t
g	i	n	i	b
e	x	g	g	r

Ciphertext= "eohtn ipess niiot dwgno ntand hueho sresa etget ginib exggr"