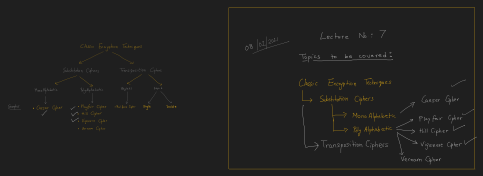

Transposition Ciphers

In Cryptography, a Transposition Cipher is a method of encryption by which the positions held by units of plaintext are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext.

Types of Transposition Ciphers :

a) Keyless → Railfence
b) Keyed → Single Columnar
→ Double Columnar

Railfence Cipher

The Rail Fence Technique is an example of transposition. It uses a simple algorithm.

1. Write down the plaintext message as a sequence of diagonals.
2. Read the plaintext written in step 1 as a sequence of rows.

The Rail Fence technique involves writing the plaintext message as a sequence of diagonals and then reading it row by row to produce ciphertext.

Plaintext: Come Home Tomorrow

Encryption:

C M H M T M R O
O E O E O O R W

Ciphertext: CMHMTMROOEOEOORW

Decryption:

- Count the number of characters in the ciphertext. Divide it into 2 halves.
- If number of characters are ODD , then add 1 character more in the upper half. For ex: If there are 9 Characters in the CT, the upper half will have 5 characters and 4 in the lower half respectively.
- Write the Characters of respective halves along the rows.
- Read them diagonally and retrieve the Plaintext.

Ciphertext: CMHMTMROOEOEOORW

1. Count the no. of characters : 16
2. Divide into 2 halves of 8 characters each.
3. Write the halves one above the other

C M H M T M R O
O E O E O O R W

4. Read them diagonally
5. COMEHOMETOMORROW

Simple Columnar Transposition Cipher (Single Transposition)

Its a variation of the Rail Fence Cipher.

1. Write the plaintext message row by row in a rectangle of a predefined size depending upon a key.

For Example : ZEBRAS
6 3 2 4 1 5

2. Read the message column by column.

3. The message thus obtained is the ciphertext message.

Plaintext: We are discovered. Flee at once.

Keyword: zebras
6 3 2 4 1 5

Encryption: We need to divide the plaintext into groups of 6 characters, as the key is of 6 characters.

6 3 2 4 1 5
W E A R E D
I S C O V E
R E D F L E
E A T O N C
E Q K J E U

Here, the characters QKJEU are added as Dummy Characters to make the guessing even more difficult.

Ciphertext:

EVLNE ACDTK ESEAQ
1 2 3
ROFOJ DEECU WIREE
4 5 6

Decryption: As the receiver is aware of the key He/she will start filling the columns in the same order of the key with the CT characters

6 3 2 4 1 5
W E A R E D
I S C O V E
R E D F L E
E A T O N C
E Q K J E U

Simple Columnar Transposition Cipher with Multiple Rounds
(Double Transposition)

A Single Columnar Transposition could be attacked by guessing the possible column lengths, writing the message out in columns and then looking for possible anagrams.

Thus, to make it stronger, a double transposition is often used. This is simply a columnar transposition applied twice.

The same key can be used or 2 different keys can be used.

For example, we can take the result of the previous transposition cipher and perform a second encryption with a different keyword STRIPE which gives a permutation 564231.

5 6 4 2 3 1
E V L N E A
C D T K E S
E A Q R O F
O J D E E C
V W I R E E

CT: ASFCE NKRER EEOEE LTQDI ECEOV VDAJW

PRACTICE EXERCISE

Q. PT : Spartans are coming. Hide your Wife and kids.

Key 1: POTATO → 425163

Key 2: SPARTA → 531462

Sol:

Encryption 1:

4 2 5 1 6 3
S P A R T A
N S A R E C
O M I N G H
I D E Y O U
R W I F E A
N D K I D S

RRNYFI PSMDWD ACHUAS SNOIRN AAIEIK TEGOED

Encryption 2:

5 3 1 4 6 2
R R N Y F I
P S M D W D
A C H U A S
S N O I R N
A A I E I K
T E G O E D

NWHOIG IDSNKD RSCNAE YDUIEO RPASAT FWARIE