

APPLIED CRYPTOGRAPHY



Transposition Ciphers

Sharanya Venkat
Richa
Aishwarya M A Ramanath

PES1201700218
PES1201700688
PES1201700872

WHAT IS CRYPTANALYSIS?

Cryptanalysis is the study of analyzing information systems in order to study the hidden aspects of the systems. Cryptanalysis is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown.

TYPES OF TRANSPOSITION CIPHERS

- Columnar Transposition
- Double Columnar Transposition
- Rail Fence Cipher

COLUMNAR TRANSPOSITION ~ ENCRYPTION

(2) CIPHER

- **EXAMPLE:** Suppose, We have:

PLAIN TEXT : 'HAMDARD UNIVERSITY KARACHI' and

KEYWORD : 'ZEBRAS'

According to columnar cipher.

Z	E	B	R	A	S
6	3	2	4	1	5



Key Word:

H	A	M	D	A	R
D	U	N	I	V	E
R	S	I	T	Y	K
A	R	A	C	H	I



Plain Text/ Message

- The six columns are now written out in the scrambled order defined by the keyword: AVYH MNIA AUSR DITC REKI HDRA

The message is written out in rows of a fixed length, and then read out again column by column, and the columns are chosen in some scrambled order. Width of the rows and the permutation of the columns are usually defined by a keyword.

COLUMNAR TRANSPOSITION ~ DECRYPTION

(3) DECIPHER(cont:)



- Now for decipher

Cipher: 'AVYH MNIA AUSR DITC REKI HDRA'

Key : 'ZEBRAS'

Z	E	B	R	A	S
6	3	2	4	1	5

H	A	M	D	A	R
D	U	N	I	V	E
R	S	I	T	Y	K
A	R	A	C	H	I

- Now read out by row wise, 'HAMDARD UNIVERSITY KARACHI.'

To decipher it, the recipient has to work out the column lengths by dividing the message length by the key length.

Then, write the message out in columns again, then reorder the columns by reforming the key word.

DOUBLE COLUMNAR TRANSPOSITION

Double Transposition

□ Plaintext: ATTACK AT DAWN

columns	0	1	2
row 0	A	T	T
row 1	A	C	K
row 2	X	A	T
row 3	X	D	A
row 4	W	N	X

Permute rows
and columns



columns	0	2	1
row 2	X	T	A
row 4	W	X	N
row 0	A	T	T
row 3	X	A	D
row 1	A	K	C

□ Ciphertext: XTAWXNATTXADAKC

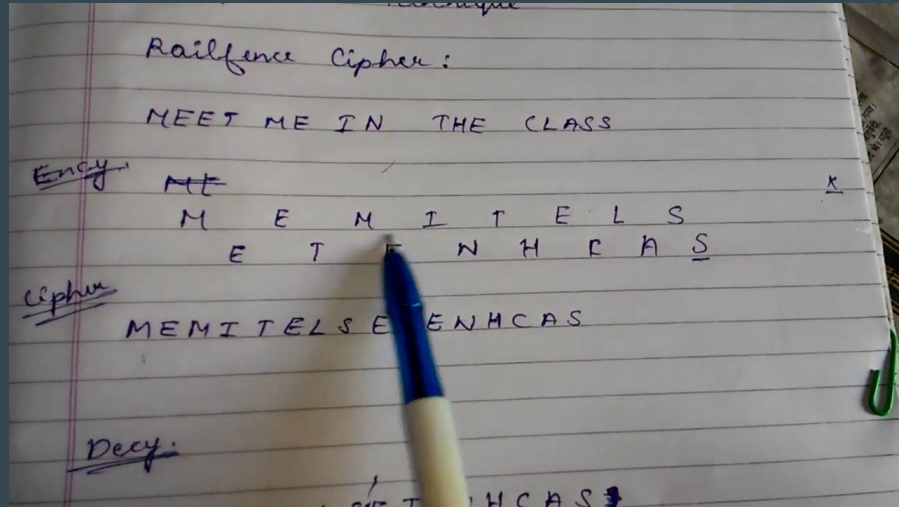
□ Key?

- 5 x 3 matrix, perms (2,4,0,3,1) and (0,2,1)

Double Transposition consists of two applications of columnar transposition to a message. The two applications may use the same key for each of the two steps, or they may use different keys.

To decrypt a double transposition, construct a block with the right number of rows under the keyword, blocking off the short columns. Write the cipher in by columns, and read it out by rows. Repeat, until decrypted text is found.

RAIL FENCE CIPHER ~ ENCRYPTION



In the rail fence cipher, the plain-text is written downwards and diagonally on successive rails of an imaginary fence. When we reach the bottom rail, we traverse upwards moving diagonally, after reaching the top rail, the direction is changed again.

Thus the alphabets of the message are written in a zig-zag manner. After each alphabet has been written, the individual rows are combined to obtain the cipher-text.

RAIL FENCE CIPHER ~ DECRYPTION

The number of columns in rail fence cipher remains equal to the length of plain-text message. And the key corresponds to the number of rails.

Hence, rail matrix can be constructed accordingly. Once we've got the matrix we can figure-out the spots where texts should be placed (using the same way of moving diagonally up and down alternatively).

Then, we fill the cipher-text row wise. After filling it, we traverse the matrix in zig-zag manner to obtain the original text.

SAMPLE OF HOW OUR PROJECT WORKS

```
aish21@LAPTOP-1V48D657: /mnt/c/crypto
aish21@LAPTOP-1V48D657: /mnt/c/crypto$ python3 project.py

=====
                        TRANSPOSITION CIPHERS
=====

1.Columnar Transposition
2.Double Columnar Transposition
3.Rail Fence Cipher
4.Exit/Quit

Please choose one of the above methods for encryption/decryption: 1

Please enter the message you wish to encrypt/decrypt below: this is for the screenshot
Choose 1. Encryption 2. Decryption
1

Columnar Transposition
Message: hiohcntisrers_t ftseos  eh_

1.Columnar Transposition
2.Double Columnar Transposition
3.Rail Fence Cipher
4.Exit/Quit

Please choose one of the above methods for encryption/decryption: 1

Please enter the message you wish to encrypt/decrypt below: hiohcntisrers_t ftseos  eh_
Choose 1. Encryption 2. Decryption
2

Columnar Transposition
Message: this is for the screenshot

1.Columnar Transposition
2.Double Columnar Transposition
3.Rail Fence Cipher
4.Exit/Quit

Please choose one of the above methods for encryption/decryption: 4

Goodbye!
Created By ~
Aishwarya
Sharanya
Richa
aish21@LAPTOP-1V48D657: /mnt/c/crypto$
```

THANK YOU