APPLIED CRYPTOGRAPHY

SHARANYA VENKAT	PES1201700218
AISHWARYA M A RAMANATH	PES1201700872
RICHA	PES1201700688

CRYPTANALYSIS OF TRANSPOSITION CIPHER

OBJECTIVE: This project aims to use the knowledge of transposition ciphers gained during class hours, and implement the same using coding constructs.

SPECIFICATIONS: We have chosen to implement the project using Python. The module project.py allows the user to both encrypt and decrypt messages of their choice using one of the following transposition ciphers:

1. Columnar Transposition
2. Double Columnar Transposition
3. Rail Fence Cipher

WHAT IS CRYPTANALYSIS?

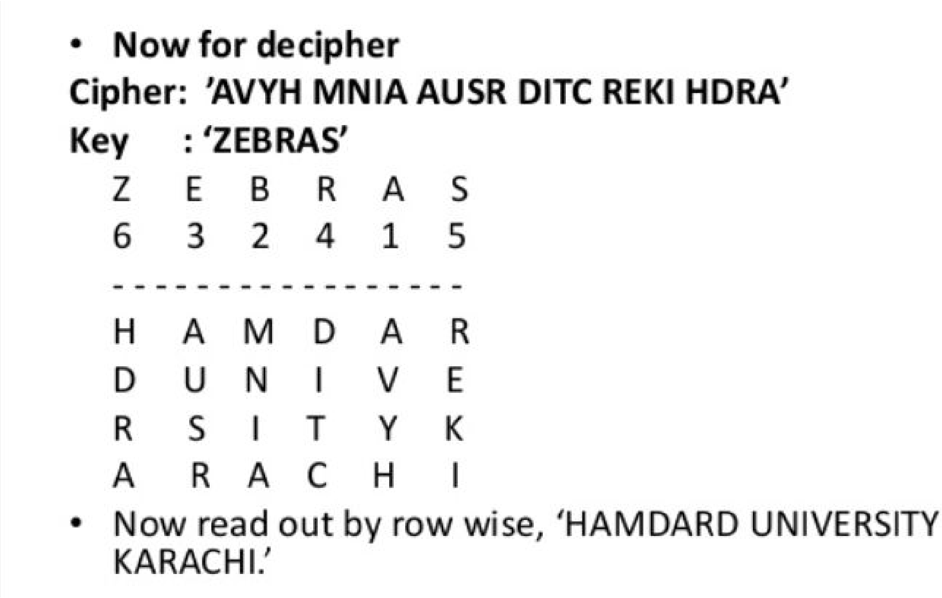
Cryptanalysis is the study of analyzing information systems in order to study the hidden aspects of the systems. Cryptanalysis is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown.

TYPES OF TRANSPOSITION CIPHERS

➢ COLUMNAR TRANSPOSITION

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.

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



- **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

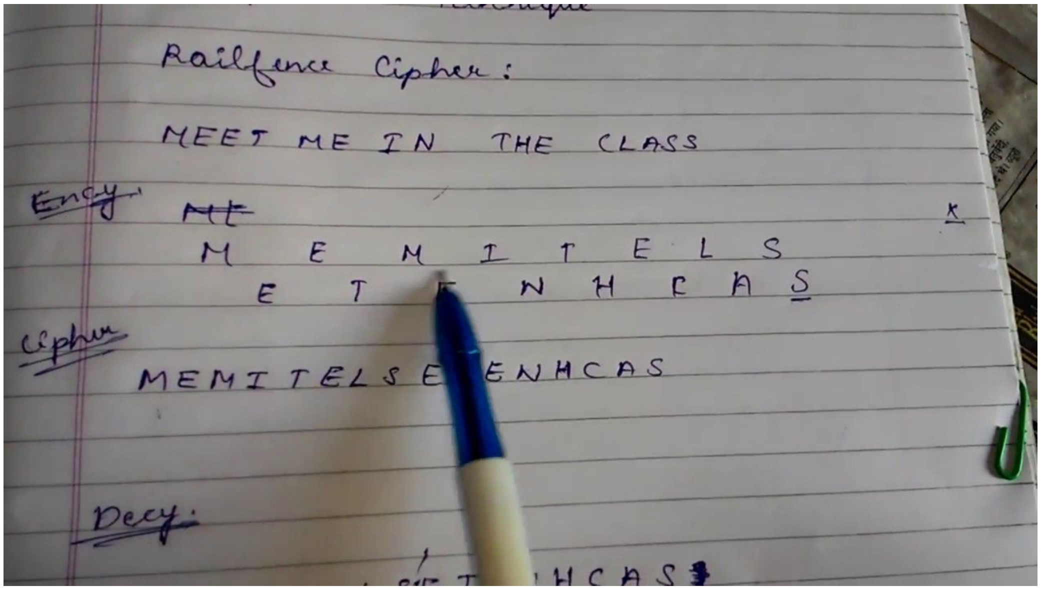
- Now read out by row wise, ‘HAMDARD UNIVERSITY KARACHI.’

➢ DOUBLE COLUMNAR TRANSPOSITION

This was one of the most secure hand ciphers used in the Second World War. 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

Also known as a zig zag cipher. This method gets its name from the way in which it is encoded. 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. To decipher it,we construct rail matrix, figure out the spots where the letters should be written and fill cipher-text row wise. After filling it, we traverse the matrix in zig-zag manner to obtain the original text.



Railfence Cipher:

MEET ME IN THE CLASS

Ency.

~~ME~~

k

M E M I T E L S

E T E N H C A S

Cipher

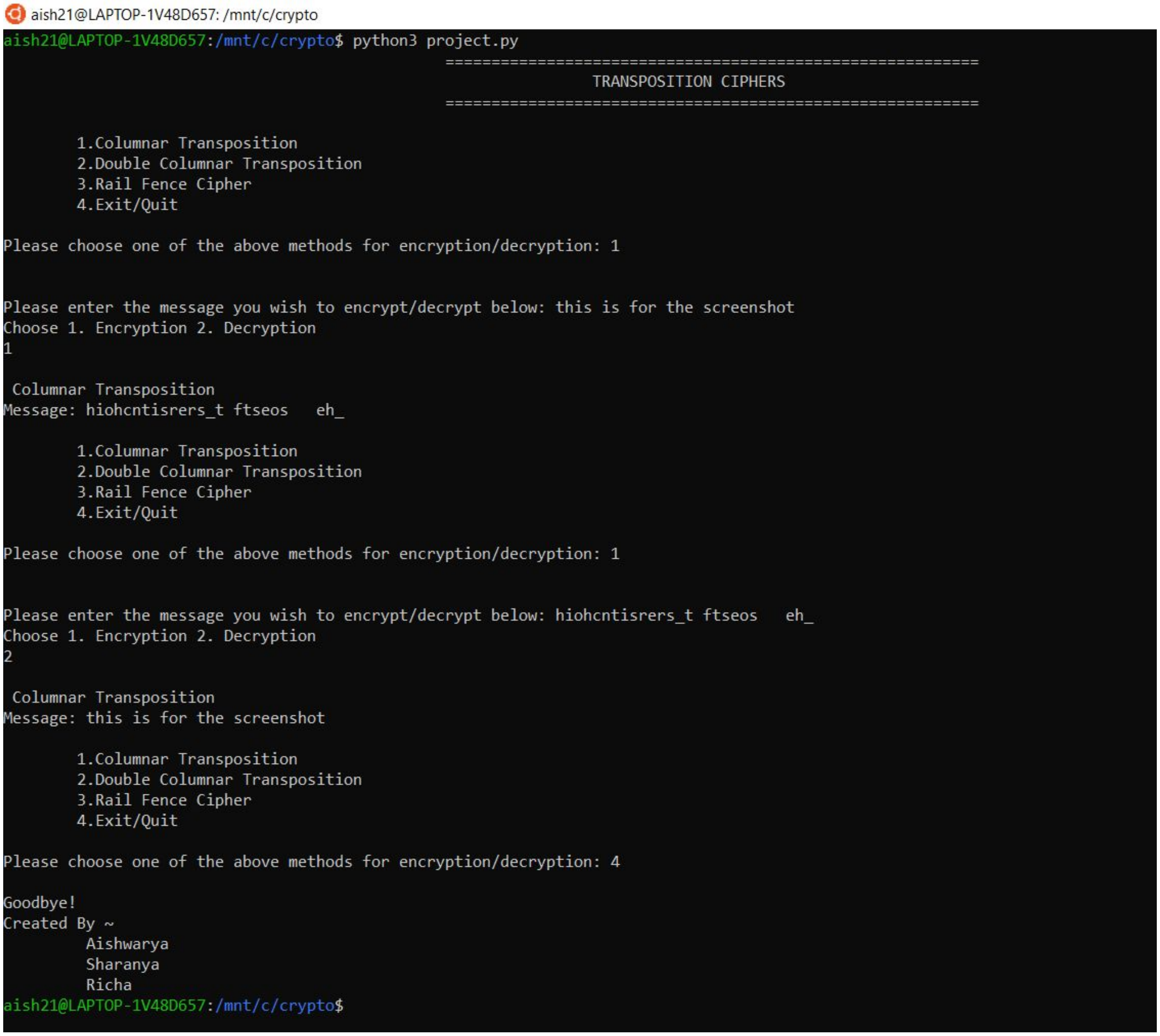
MEMITELSE ENHCAS

Decy:

T HCAS

OUR IMPLEMENTATION

Here is one snapshot of our implementation of the columnar transposition, the key we have used is “HACK”.



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$
```

OUR CONTRIBUTIONS

Each of us worked on one coding one of the methods for encryption and decryption. We then worked together to combine them all seamlessly into one working model, that can be seen in the screenshot above.