APPLIED CRYPTOGRAPHY

•••

Transposition Ciphers

Sharanya Venkat	PES1201700218
Richa	PES1201700688
Aishwarya M A Ramanath	PES1201700872

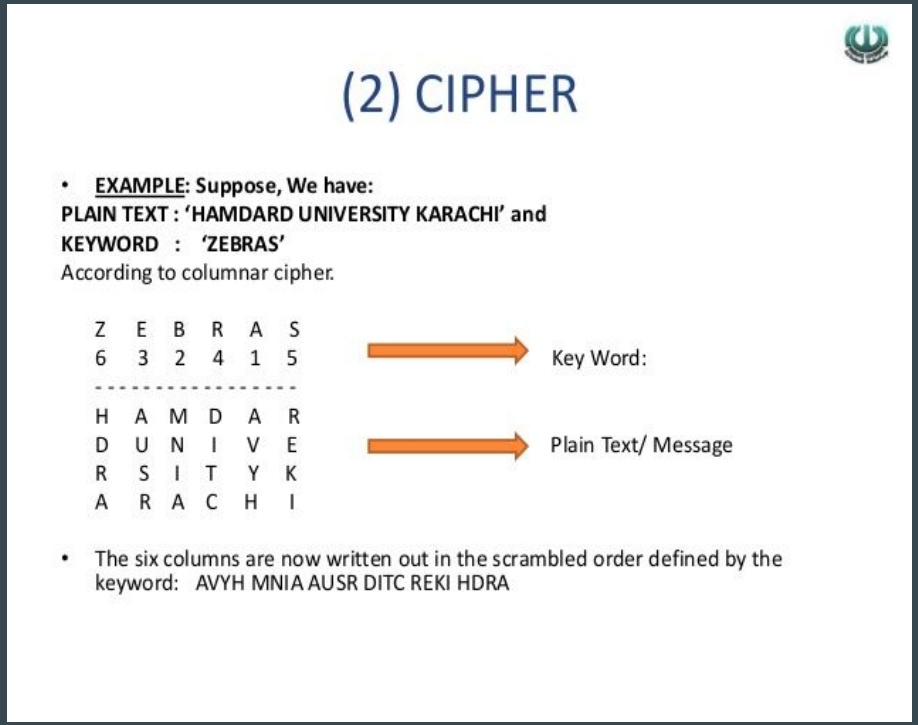
WHAT IS CRYPTANALYSIS?

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

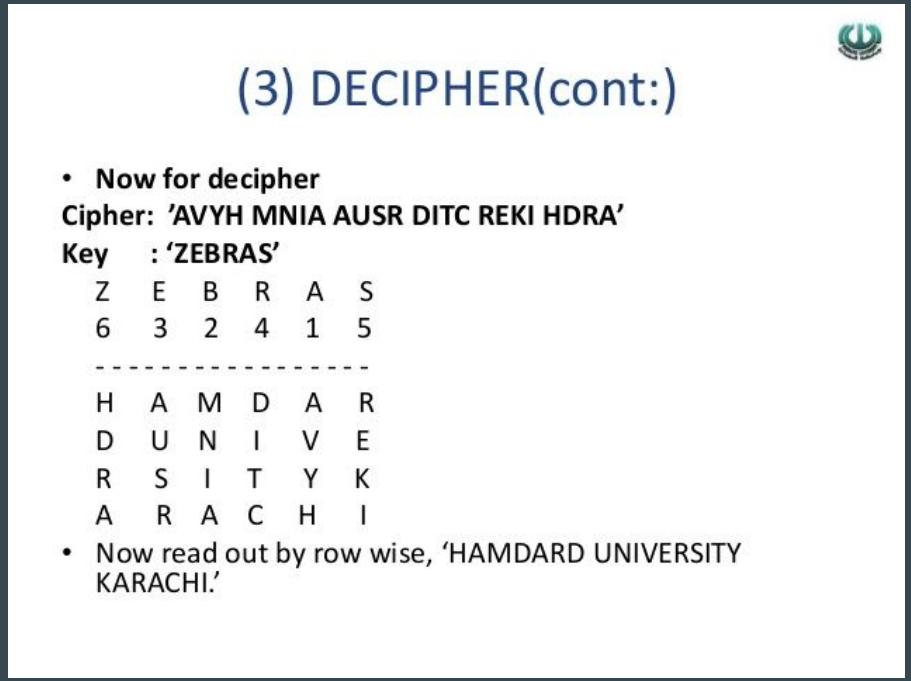
- Columnar Transposition
- Double Columnar Transposition
- Rail Fence Cipher

COLUMNAR TRANSPOSITION ~ ENCRYPTION



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.

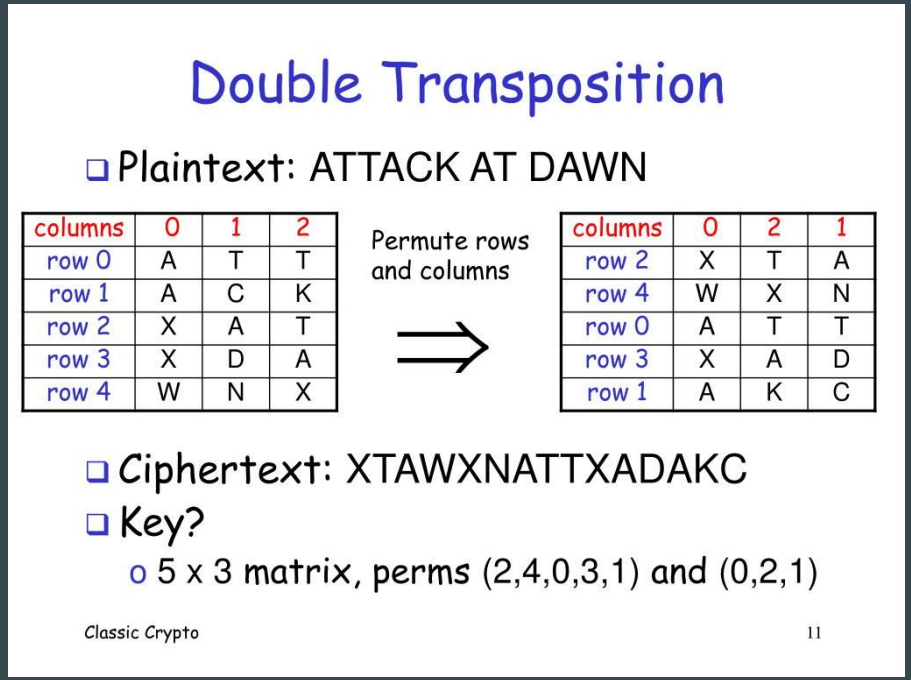
COLUMNAR TRANSPOSITION ~ DECRYPTION



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.

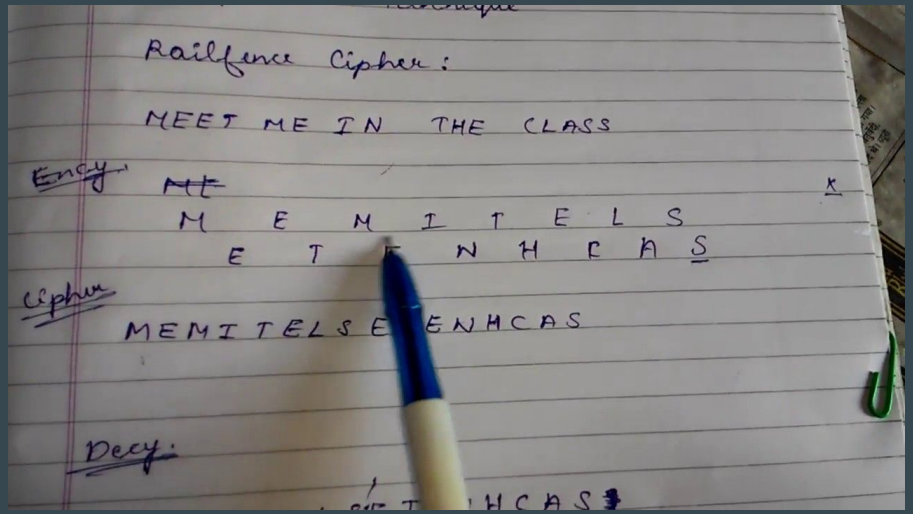
DOUBLE COLUMNAR TRANSPOSITION



Double Transposition 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.

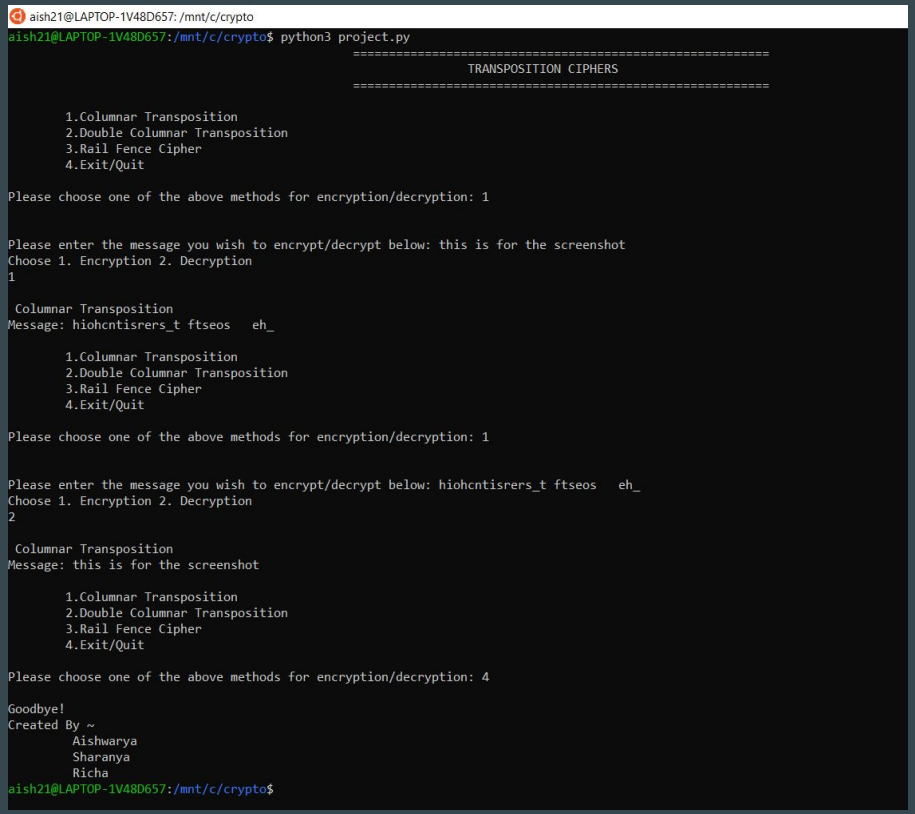
RAIL FENCE CIPHER ~ DECRYPTION

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



THANK YOU