Experiment No. 02

Title

Write a Java/C/C++/Python program to perform encryption and decryption using the method of Transposition technique.

Objective

Learn how to Perform Encryption and Decryption using method of transposition technique.

Problem Definition:

Perform Encryption and Decryption using method of transposition technique.

Outcome

After completion of this assignment students will be able to understand the Perform Encryption and Decryption using method of transposition technique.

Software Requirements:

Python 3

Hardware Requirements:

PC, 2GB RAM, 500 GB HDD

Theory

Transposition Techniques

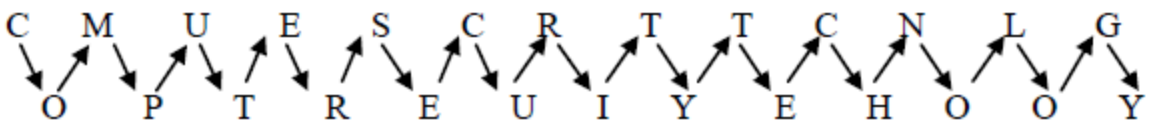
Rail Fence Technique

In Rail fence cipher, techniques are essentially Transposition Ciphers and generated by rearrangement of characters in the plaintext. The characters of the plain text string are arranged in the form of a rail-fence as follows.

Given **Plain text** is - COMPUTER SECURITY TECHNOLOGY

Rail Fence Technique algorithm:

1. Write down the plain text message as a sequence of diagonals.
2. Read the plain text written in Step-1 as a sequence of rows. Example: plain text = COMPUTER SECURITY TECHNOLOGY is converted to cipher text with this help of Rail Fence Technique with dual slope.



Cipher Text is - CMUESCRTTCNLGOPTREUIYEHOOY

Columnar Transposition

Following are two types of Columnar Transposition

Simple Columnar Transposition

The columnar transposition cipher is a transposition cipher that follows a simple rule for mixing up the characters in the plaintext to form the cipher-text. It can be combined with other ciphers, such as a substitution cipher, the combination of which can be more difficult to break than either cipher on its own.

The cipher uses a columnar transposition to greatly improve its security.

Algorithm:

1. The message is written out in rows of a fixed length.
2. Read out again column by column according to given order or in random order.
3. According to order write cipher text.

Example

The key for the columnar transposition cipher is a keyword e.g. ORANGE. The row length that is used is the same as the length of the keyword.

To encrypt a below **Plain Text** - COMPUTER PROGRAMMING

O	**R**	**A**	**N**	**G**	**E**
C	O	M	P	U	T
E	R	P	R	O	G
R	A	M	M	I	N
G	L	E	X	X	M

In the above example, the plaintext has been padded so that it neatly fits in a rectangle. This is known as a regular columnar transposition. An irregular columnar transposition leaves these characters blank, though this makes decryption slightly more difficult. The columns are now reordered such that the letters in the key word are ordered alphabetically.

5	**6**	**1**	**4**	**3**	**2**
O	**R**	**A**	**N**	**G**	**E**
C	O	M	P	U	T
E	R	P	R	O	G
R	A	M	M	I	N
G	L	E	X	X	M

The Encrypted text or **Cipher Text** is: MPMET GNMUO IXPRM XCERG ORAL (Written in blocks of five)

Double Columnar Transposition

A single Columnar Transposition can be attacked by guessing possible column lengths by writing the message from columns (with the wrong order because the key is unknown) and then trying to get the possible message.

Therefore to make it stronger, a double transposition was used. This is simple columnar transposition technique applied twice. Here the same key can be used for both transpositions or two different keys can be used.

For Example – Plain Text: - WELCOME HOME Key:-PLAYER (with length 6)

Round 1

1	2	3	4	5	6
W	E	L	C	O	M
E	H	O	M	E	

Now read it with some random order of (4,6,1,2,5,3) = “CMMWEEHOELO”

Round 2 now “CMMWEEHOELO” this will be next cipher Text

1	2	3	4	5	6
C	M	M	W	E	E
H	O	E	L	O	

Again read with the order of (4,6,1,2,5,3) = “WLECHMOEOME”

Algorithm:-

1. Write the plain text message row-by-row in a rectangle of a predefined size
2. Read the message column-by-column in any random order.
3. The message thus obtained is cipher text message of round one
4. Repeat step 1 to3 as many times as desired.

Conclusion

Thus we learn that how to Perform Encryption and Decryption using method of transposition technique.