MES Wadia College of Engineering Pune-01

Department of Computer Engineering

Name of Student:	**Class: TE Comp**
Semester/Year: 6th	**Roll No:**
Date of Performance:	**Date of Submission:**
Examined By: Prof(Dr.)S.K.Wagh	**Experiment No: Part 2-IS-02**

PART 2- LPII-ELII-IS-ASSIGNMENT NO: 02

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

OBJECTIVES:

1. **Understanding Cryptography Basics**: Learn the fundamental principles of cryptography, including the distinction between symmetric and asymmetric encryption, and the role of encryption and decryption in securing information.
2. **Algorithm Implementation**: Gain hands-on experience in implementing cryptographic algorithms, enhancing understanding of how theoretical concepts are translated into practical applications.
3. **Problem-Solving Skills**: Develop problem-solving and algorithmic thinking skills by devising methods to rearrange characters in a systematic way for encryption and then correctly revert to the original arrangement for decryption.
4. **Encryption Technique Application**: Understand how the Transposition technique can be applied to encrypt data by rearranging its order according to a certain system, making the data unreadable to unauthorized parties without the key.

APPRATUS:

- Operating System recommended: 64-bit Open source Linux or its derivative.
- Java, C, C++, or Python

THEORY:

Transposition technique is an encryption method which is achieved by performing **permutation over the plain text**. Mapping plain text into cipher text using transposition technique is called **transposition cipher**.

In this section, we will discuss variations of transposition technique, and we will also observe how the transposition technique is different from the substitution technique.

On the one hand, the substitution technique substitutes a plain text symbol with a cipher text symbol. On the other hand, the transposition technique executes permutation on the plain text to obtain the cipher text.

Transposition Techniques

1. Rail Fence Transposition
2. Columnar Transposition
3. Improved Columnar Transposition
4. Book Cipher/Running Key Cipher

1. Rail Fence Cipher

The rail fence cipher is the simplest transposition cipher. The steps to obtain cipher text using this technique are as follow:

Step 1: The plain text is written as a sequence of diagonals.

Step 2: Then, to obtain the cipher text the text is read as a sequence of rows.

To understand this in a better way, let us take an example:

Plain Text: meet me Tomorrow

Now, we will write this plain text sequence wise in a diagonal form as you can see below:

Looking at the image, you would get it why it got named rail fence because it appears like the rail fence.

Once you have written the message as a sequence of diagonals, to obtain the cipher text out of it you have to read it as a sequence of rows. So, reading the first row the first half of cipher text will be:

m e m t m r o

reading the second row of the rail fence, we will get the second half of the cipher text:

e t e o o r w

Now, to obtain the complete cipher text combine both the halves of cipher text and the complete cipher text will be:

Cipher Text: M E M T M R O E T E O O R W

Rail fence cipher is easy to implement and even easy for a cryptanalyst to break this technique. So, there was a need for a more complex technique.

2. Columnar Transposition Technique

The columnar transposition cipher is more complex as compared to the rail fence. The steps to obtain cipher text using this technique are as follow:

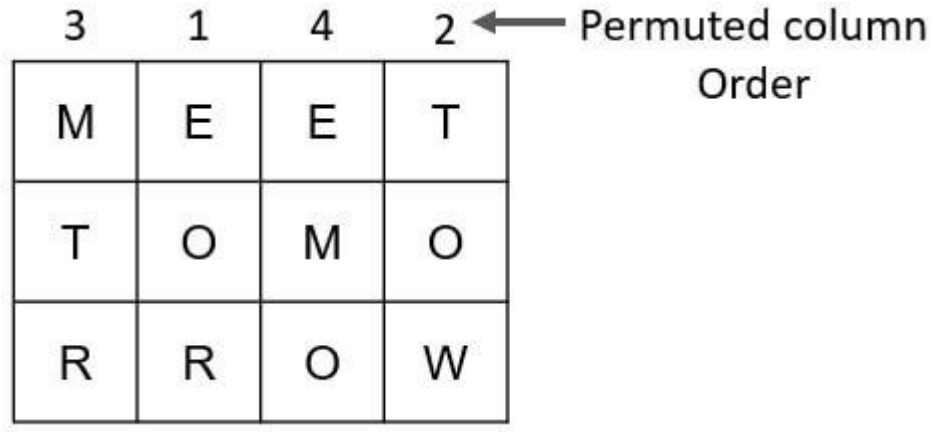
Step 1: The plain text is written in the rectangular matrix of the initially defined size in a row by row pattern.

Step 2: To obtain the cipher text read the text written in a rectangular matrix column by column. But you have to permute the order of column before reading it column by column. The obtained message is the cipher text message.

To understand the columnar transposition let us take an example:

Plain text: meet Tomorrow

Now, put the plain text in the rectangle of a predefined size. For our example, the predefined size of the rectangle would be 3×4. As you can see in the image below the plain text is placed in the rectangle of 3×4. And we have also permuted the order of the column.



Now, to obtain the cipher text we have to read the plain text column by column as the sequence of permuted column order. So, the cipher text obtained by the columnar transposition technique in this example is:

Cipher Text: MTREOREMOTOW.

Similar to the rail fence cipher, the columnar cipher can be easily broken. The cryptanalyst only has to try few permutation and combination over the order of column to obtain the permuted order of column and the get the original message. So, a more sophisticated technique was required to strengthen the encryption.

3. Columnar Transposition Technique with Multiple Rounds

It is similar to the basic columnar technique but is introduced with an improvement. The basic columnar technique is performed over the plain text but more than once. The steps for columnar technique with multiple rounds are as follow:

Step 1: The plain text is written in the rectangle of predetermined size row by row.

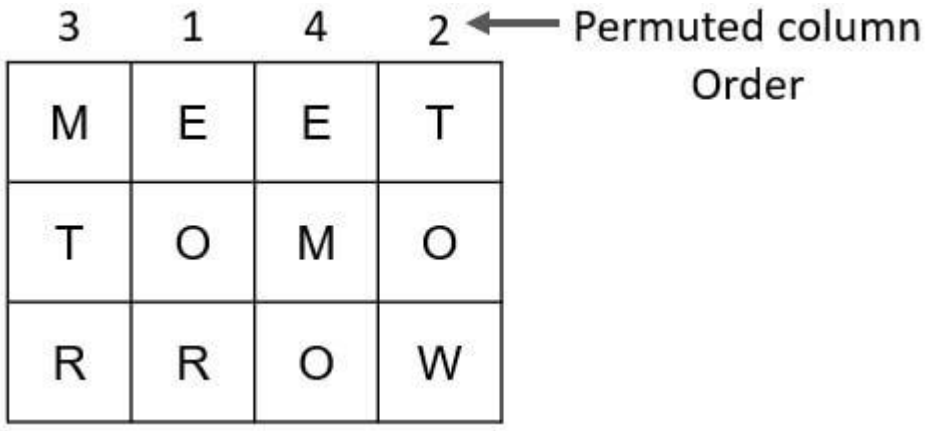
Step 2: To obtain the cipher text, read the plain text in the rectangle, column by column. Before reading the text in rectangle column by column, permute the order of columns the same as in basic columnar technique.

Step 3: To obtain the final cipher text repeat the steps above multiple time.

Let us discuss one example of a columnar transposition technique for better understanding. We will consider the same example of a basic columnar technique which will help in understanding the complexity of the method:

Plain Text: meet Tomorrow

Let us put this plain text in the rectangle of predefined size of 3×4. Proceeding with the next step, the order of the columns of the matrix is permuted as you can see in the image below:



Now after the first round the cipher text obtained is as follow:

Cipher Text round 1: MTREOREMOTOW

Now, again we have to put the cipher text of round 1 in the rectangle of size 3×4 row by row and permute the order of columns before reading the cipher text for round 2. In the second round, the permuted order of the column is 2, 3, 1, 4.

So, the obtained **cipher text for round 2** is MOOTRTREOEMW. In this way, we can perform as many iterations as requires. Increasing the number of iterations increases the complexity of the techniques.

4. Book Cipher or Running Key Cipher

The book cipher or the running key cipher works on the basic principle of one-time pad cipher. In onetime pad cipher the key is taken as long as the plain text and is discarded after the use. Every time a new key is taken for a new message.

The improvement to the onetime pad in Book cipher is that the key or the onetime pad is taken from the book. Let us discuss the steps:

Step 1: Convert the plain text in numeric form consider A=0, B=1, C=3 …, Z=25.

Step 2: Take an onetime pad or key from any of the books and convert it in the numeric form also. But the key must be as long as the length of plain text.

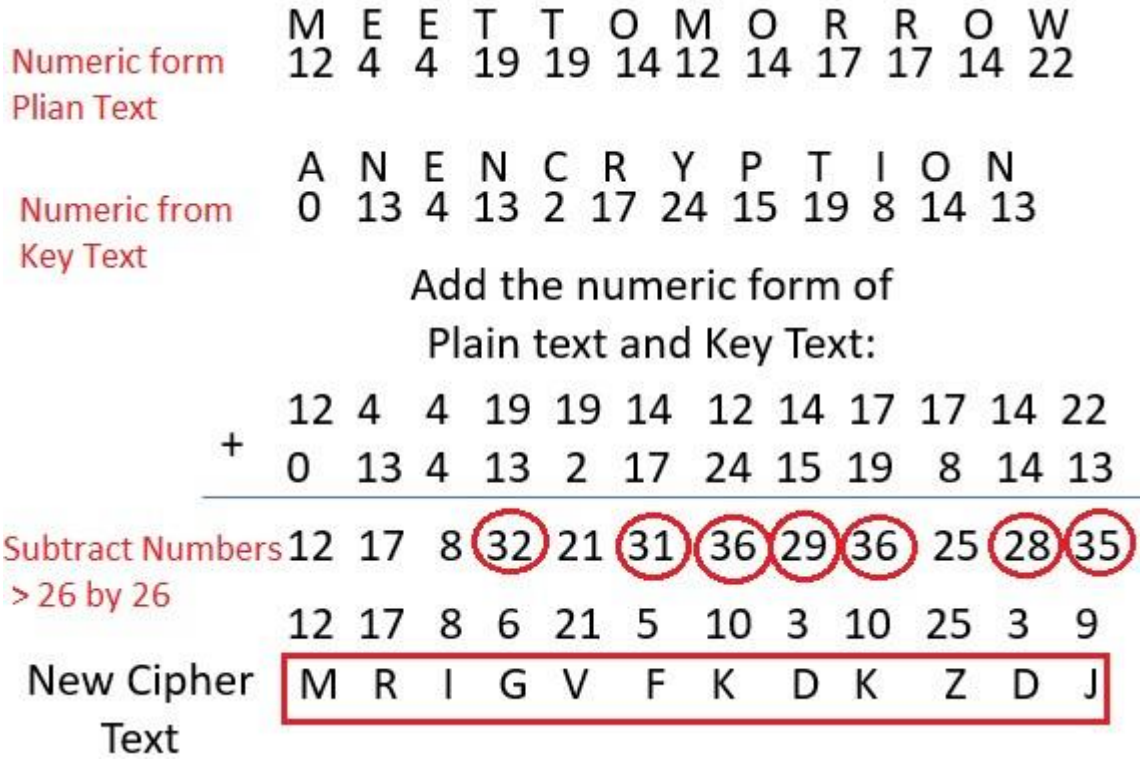
Step 3: Now add the numeric form of both plain text and key, each plain text letter with corresponding key text letter. If the addition of any plain text letter with corresponding key text letter is >26, then subtract it with 26.

Let us understand with the example:

Plain text: Meet Tomorrow

Key taken from the book: ANENCRYPTION.

Now we have to convert this plain text and key text in numeric form and add them to get cipher text as shown in the image below:



The **cipher text** obtained is MRIGVFKDKZDJ.

So, this is all about the Transposition technique, which involves the permutation over the plain text for converting plain text into the cipher text.

CONCLUSION:

We have studied the Transposition technique, which involves the permutation over the plain text for converting plain text into the cipher text.

QUESTIONS:

1. What is substitution techniques in cryptography? Explain with examples.