Assignment No: 10A

Name of student:

Roll No:

Practical Batch:

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

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

Objective:

To understand the working of Transposition Cipher technique.

To implement Transposition Cipher technique.

Theory:

Cryptography probably dates back close to the beginnings of writing. One of the earliest known examples is the Caesar cipher, named for its purported use by Julius Caesar in ancient Rome. The Caesar cipher, which can not be considered secure today, replaced each letter of the alphabet with the letter occurring three positions later or 23 positions earlier in the alphabet: A becomes D, B becomes E, X becomes A, and so forth.

A)Substitution Cipher : A generalized version of the Caesar cipher is an alphabetic substitution cipher. As an example, a simple *substitution cipher* might use the following secret key to provide a substitution between characters of the original message and characters of the encrypted message.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

F R O A H I C W T Z X L U Y N K E B P M V G D S Q J

Using this key, a sample encrypted message is:

IEQ IBQDXMBQ FX RMBFQW MOWQB IEQ QLT IBQQ.

As is evident from even such a short example, this simple method does not disguise patterns in the text such as repeated letters and common combinations of letters. In fact, if the encrypted message is known to be English text, it is usually quite easy to determine the original message, even without the knowledge of the secret key, by using letter frequency analysis, guessing and checking, and maybe a little intuition and luck. Such substitution ciphers are commonly used today as puzzles in newspapers and puzzle books, but are not secure when used alone as cryptosystems. Polyalphabetic substitution ciphers, developed by Len Battista in 1568, improved on regular substitution ciphers by changing the substitution scheme partway through a message. Although substitution is not secure when used alone, it can be useful when used in conjunction with other techniques, and in fact, many cryptosystems used today benefit from substitution when it is carefully used as part of their encryption algorithms.

B) 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**.

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

Rail Fence Transposition
Columnar Transposition
Improved Columnar Transposition

i) 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.

ii) 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:

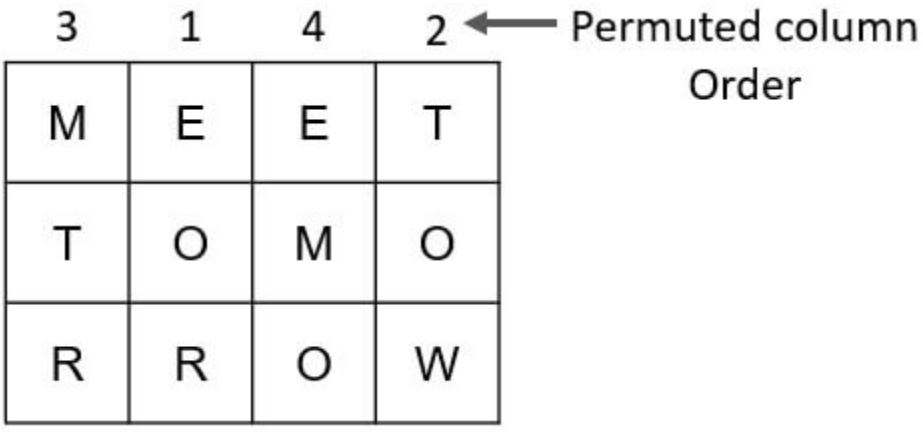
Step 1: The plain text is written in the rectangular matrix of the initially defined size in a row by row pattern.

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.

iii) 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.

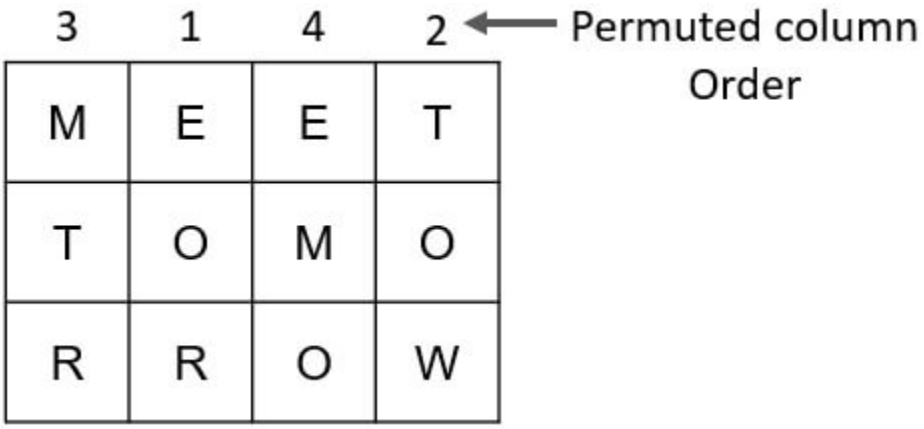
Step 2: To obtain the cipher text, read the plain text in the rectangle, column by column. Before reading the text in rectangle column by column, permute the order of columns the same as in basic columnar technique.

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.

Algorithm :

Encryption

In a transposition cipher, the order of the alphabets is re-arranged to obtain the cipher-text.

1. 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.
2. Width of the rows and the permutation of the columns are usually defined by a keyword.
3. For example, the word HACK is of length 4 (so the rows are of length 4), and the permutation is defined by the alphabetical order of the letters in the keyword. In this case, the order would be “3 1 2 4”.
4. Any spare spaces are filled with nulls or left blank or placed by a character (Example: _).
5. Finally, the message is read off in columns, in the order specified by the keyword.

Decryption

1. To decipher it, the recipient has to work out the column lengths by dividing the message length by the key length.
2. Then, write the message out in columns again, then re-order the columns by reforming the key word.

Conclusion : Thus transposition cipher method is studied and implemented.

Questions :

1. What is the meaning of cipher in computer terminology?

a) an algorithm that performs encryption
b) an algorithm that generates a secret code
c) an algorithm that performs encryption or decryption

d) a secret code
View Answer
Answer: c
Explanation: Cipher can be defined to be an algorithm that performs encryption or decryption. In cryptography, a set of defined steps are followed to generate ciphers.

2. Which of the following cipher is created by shuffling the letters of a word?
a) substitution cipher
b) transposition cipher
c) mono alphabetic cipher
d) poly alphabetic cipher
View Answer
Answer: b
Explanation: Types of traditional ciphers- Transposition and substitution cipher. In transposition cipher the letters of the given message are shuffled in a particular order, fixed by a given rule.

3. Which of the following is not a type of transposition cipher?
a) Rail fence cipher
b) Columnar transposition cipher
c) One time pad cipher
d) Route cipher
View Answer
Answer: c
Explanation: Out of the given options only One time pad cipher is not a type of transposition cipher. It is a type of substitution cipher.

3. **What is cryptography?**
4. **What is cryptanalysis?**
5. **What do you mean by cipher text?**
6. **What is encryption and decryption?**
7. **List various services of security?**