FR. CONCEICAO RODRIGUES COLLEGE OF ENGINEERING
Department of Computer Engineering

1. Course , Subject & Experiment Details

Academic Year	**2017-18**	**Estimated Time**	**02 - Hours**
Course & Semester	**B.E. (CMPN)- Sem VII**	**Subject Name & Code**	**CSS - (CPC702)**
Chapter No.	**02 – Mapped to CO- 1**	**Chapter Title**	**Basics of Cryptography**

Practical No:	**2**
Title:	To study and implement different types of transposition ciphers.
Date of Performance:	
Date of Submission:	
Roll No:	**7371**
Name of the Student:	**Flavion D'sa**

Evaluation:

Sr. No	Rubric	Grade
1	On time submission Or completion (2)	
2	Preparedness(2)	
3	Skill (4)	
4	Output (2)	

Signature of the Teacher:

Date:

Title : To study and implement any two different types transposition ciphers like rail fence, single columnar, double columnar cipher.

Lab Objective :

This lab provides insight into:

- How different types of Transposition Ciphers like rail fence, single columnar and double columnar, works and their advantages and disadvantages.

Reference : "Cryptography and Network Security" B. A. Forouzan
"Information Security Principles and Practice" Mark Stamp
"Cryptography and Network Security" Atul Kahate

Prerequisite : Java and Knowledge of Ciphering .

Theory:
A **transposition cipher** is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext. That is, the order of the units is changed.

1. **Rail Fence cipher:** The Rail Fence cipher is a form of transposition cipher that gets its name from the way in which it is encoded. In the rail fence cipher, the plaintext is written downwards on successive "rails" of an imaginary fence, then moving up when we get to the bottom. The message is then read off in rows. For example, using three "rails" and a message of 'WE ARE DISCOVERED. FLEE AT ONCE', the cipher writes out:

Example:

W . . . E . . . C . . . R . . . L . . . T . . . E
. E . R . D . S . O . E . E . F . E . A . O . C .
. . A . . . I . . . V . . . D . . . E . . . N . .

Then reads off:

WECRL TEERD SOEEF EAOCA IVDEN

2. Single Columnar transposition: In a 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. Both the width of the rows and the permutation of the columns are usually defined by a keyword. For example, the word ZEBRAS is of length 6 (so the rows are of length 6), and the permutation is defined by the alphabetical order of the letters in the keyword. In this case, the order would be "6 3 2 4 1 5".

In a regular columnar transposition cipher, any spare spaces are filled with nulls; in an irregular columnar transposition cipher, the spaces are left blank. Finally, the message is read off in columns, in the order specified by the keyword. For example, suppose we use the

keyword ZEBRAS and the message WE ARE DISCOVERED. FLEE AT ONCE. In a regular columnar transposition, we write this into the grid as:

Example:

ZEBRAS - 632415

6 3 2 4 1 5
W E A R E D
I S C O V E
R E D F L E
E A T O N C
E Q K J E U

The ciphertext is then read off as:

EVLNE ACDTK ESEAQ ROFOJ DEECU WIREE

3. Double Columnar transposition: A single columnar transposition could be attacked by guessing possible column lengths, writing the message out in its columns (but in the wrong order, as the key is not yet known), and then looking for possible anagrams. Thus to make it stronger, a double transposition was often used. This is simply a columnar transposition applied twice. The same key can be used for both transpositions, or two different keys can be used.

As an example, we can take the result of the irregular columnar transposition in the previous section, and perform a second encryption with a different keyword, STRIPE, which gives the permutation "564231"

Example:

5 6 4 2 3 1
E V L N A C
D T E S E A
R O F O D E
E C W I R E
E
This is read off column wise to give the cipher text.

CAEEN SOIAE DRLEF WEDRE EVTOC

Algorithm of Double Columnar Transposition

Encryption:

In double columnar transposition, the order of the alphabets are rearranged in form of a matrix 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 ZEBRA is of length 5 (so the rows are of length 5), and the permutation is defined by the alphabetical order of the letters in the keyword. In this case, the order would be "5 3 2 4 1".
4. Any spare spaces are filled with nulls or left blank or placed by a character (Example: X).
5. A new message is read off in columns, in the order specified by the keyword.
6. This new message is then again written in a matrix form using the same key or a different key which may have a different length.
7. Finally, the message is read off from the resulting columns.

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.
3. The above step is repeated again with the message formed therewith.

Conclusion:

The program was tested for different sets of inputs.

Program is working SATISFACTORY NOT SATISFACTORY

(Tick appropriate outcome)

Post Lab Assignment:

Multiple-choice questions

1. Transposition cipher involves

   _____

   a) replacement of blocks of text with other blocks
   b) replacement of characters of text with other characters.
   c) strictly row-to-column replacement
   d) some permutations on the input text to produce cipher text

2. The mechanism of writing text as rows and reading as columns is called as

   _____

   a) Vernam cipher
   b) Caesar cipher
   c) Simple Columnar Transpositiontechniques.
   d) Homophonic substitution cipher

3. One of the following is correct in regards to transposition cipher.

_____

a) The identity of the letters change but their positions remains the same
b) A transposition cipher is strong when there are long blocks of identical characters within the string
c) Given text with normal language characteristics, a transposition cipher can be strong against a brute force attack.
d) All of the above

4. Explain the transposition ciphers with its merits and demerits.