FR. CONCEICAO RODRIGUES COLLEGE OF ENGINEERING
Department of Computer Engineering

1. **Course , Subject & Experiment Details**

Academic Year	2021-22	Estimated Time	03 - Hours
Course & Semester	T.E. (CMPN)- Sem VI	Subject Name & Code	CSS - (CSC602))
Chapter No.	02 – Mapped to CO- 1	Chapter Title	Basics of Cryptography

Practical No:	1
Title:	Design and Implementation of a product cipher using Substitution and Transposition ciphers
Date of Performance:	25/01/2022
Date of Submission:	01/02/2022
Roll No:	8875
Name of the Student:	Upmanyu D Jha

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: Design and Implementation of a product cipher using Substitution and Transposition Ciphers.

Lab Objective :

This lab provides insight into:

- How different types of Substitution Ciphers and Transposition Ciphers like Hill cipher, Verman cipher, Playfair cipher, Vigenere cipher works and their advantages and disadvantages.

Reference : "Cryptography and Network Security" B. A. Forouzan
"Cryptography and Network Security" Atul Kahate

Pre-requisite : Any Programming language and Knowledge of Ciphering .

Theory:

Cryptography is the practice and study of hiding information. It is the process of converting ordinary information (plain text) into cipher text and converting cipher text again to plain text, A cipher is a pair of algorithms which create the encryption and decryption.

Substitution Cipher: In cryptography, a **substitution cipher** is a method of encryption by which units of plaintext are replaced with cipher text according to a regular system; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing an inverse substitution.

Types of substitution cipher:

- **Monoalphabatic Cipher:** A *monoalphabetic substitution cipher*, also known as a simple substitution cipher, relies on a fixed replacement structure. That is, the substitution is fixed for each letter of the alphabet. Thus, if "a" is encrypted to "R", then every time we see the letter "a" in the plaintext, we replace it with the letter "R" in the ciphertext.

Ex. If **a** is substituted by **'x'** and **b** is substituted by **'y'** and so on than

"starbucks at three" encrypted as
PQXOYRHPXQQEOBB

1) Caesar Cipher/Additive/ Shift: It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a shift of 3, A would be replaced by D, B would become E, and so on. The method is named after Julius Caesar, who used it to communicate with his generals.

Example

Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: DEFGHIJKLMNOPQRSTUVWXYZABC

Like Plaintext: the quick brown fox jumps over the lazy dog
Cipher text: WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ

- **Polyalphabetic Cipher :** In this cipher, we are using no. of substitutions at different positions in the message.

1) Vigenere Cipher
2) Hill Cipher

1) **Hill Cipher** : It is a block cipher.

Key: An invertible m*m matrix (where m is the block length) i.e the sender & receiver must first agree upon a key matrix A of size m*m. A must be invertible mod 26.
Encryption: To encrypt a message using a message using the Hill Cipher we must first turn our keyword into a key matrix (a 2*2 matrix for working with digraphs). We also turn the PT into digraphs and each of these into a column vector. We then perform matrix multiplication modulo the length of the alphabet (i.e 26) on each vector. These vectors are then converted back into letters to produce the ciphertext.
Decryption:
To decrypt a ciphertext encoded using the Hill Cipher, we must find the inverse matrix. Once we have the inverse matrix, the process is the same as encrypting. That is we multiply the inverse key matrix by the column vectors that the ciphertext is split into, take the results modulo the length of the alphabet, and finally convert the numbers back to letters.

2) **Verman Cipher:** it is a stream, polyalphabetic cipher in which the plaintext is XORed with a random or pseudorandom stream of data to generate the ciphertext. If the stream of data is truly random and used only once, this is the one-time pad.

Ex.	H	E	L	L	O message
	7 (H)	4 (E)	11 (L)	11 (L)	14 (O) message
+	23 (X)	12 (M)	2 (C)	10 (K)	11 (L) key
=	30	16	13	21	25 message + key
=	4 (E)	16 (Q)	13 (N)	21 (V)	25 (Z) message + key (mod 26)
	E	Q	N	V	Z → ciphertext

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 Proposed Product Cipher :

1. Take key and plain text inputs from users.
2. ~~convert~~ generate a Cipher Key Matrix with Key input.
3. Convert plaintext into digraphs (i.e, into pair of two letters)
4. Encrypt plaintext using Cipher Key Matrix and get ciphertext.
5. Follow All the playfair rules for Encryption.
6. Take the previous key and Encrypted text by playfair as a input for single columnar transposition cipher.
7. use ceil to adjust the count of rows according to length of ~~matrix.~~ message
8. Convert the given message into a Matrix.
9. get the indices as the key numbers instead of alphabets in the key for appending the elements of matrix formed earlier, columnwise.
10. give the column index and get the cipher text.
11. Now take the cipher text generated by single columnar & its key as input to repeat the single columnar again to get double columnar outputs so follows step from 7 to 10 again

(11) And now Final out put is generated in message.

Example of Product Cipher

Playfair

Key:- MONK

Key Matrix :-

$$\begin{bmatrix} m & o & n & k & a \\ b & c & d & e & f \\ g & h & i & l & p \\ q & r & s & t & u \\ v & w & x & y & z \end{bmatrix}$$

message : I am Upmanyu Jha and this is my product cipher,

plain text : Iamupmanyujhaandthisismyproductcipher

cipher text : pnaqgamkztognzmkesilxsqnzlwefserdhgict

Single columnar

key :- MONK

The message:-

$$\begin{bmatrix} p & n & a & q \\ g & a & m & k \\ z & t & o & g \\ n & z & m & k \\ e & s & i & l \\ x & s & q & n \\ z & l & w & e \\ f & s & e & r \\ d & h & g & i \\ c & t & \_ & \_ \end{bmatrix}$$

Cipher text:- qkgklncri_pgznexzfdcamomiqweg_natzsslsht.

Double colomnar transposition cipher. (i.e redoing sigle columnar transposition cipher)

Key : MONK

The message matrix is :

$$\begin{bmatrix} q & k & g & k \\ l & n & c & r \\ i & \_ & p & j \\ z & n & e & x \\ a & m & o & m \\ i & q & w & e \\ g & \_ & n & a \\ t & z & s & s \\ l & s & h & t \end{bmatrix}$$

Cipher text : krgxcmeostqlizzaigtlgcpedownshkn_nfmq_zs ,

A

Practical & Real-Time Application

- encryption and decryption of stream cipher and block cipher

Conclusion:

The program was tested for different sets of inputs.
Program is working SATISFACTORY NOT SATISFACTORY
(Tick appropriate outcome)

Post Lab :

1. To break the Caesar cipher using brute force attack, how many attempts are needed?
2. Compare Substitution and Transposition techniques.

Postlab

1 Ans] At the Most ~~Mostly~~ One or two attempts is only needed to break Caesar cipher.

2 Ans]

Substitution	Transposition
① In Substitution cipher technique the letter of plain text are replaced by another letters or number or symbols.	① In Transposition cipher technique does not substitute one symbol for another instead it changes the location of the symbol.
② In this the letter with low frequency can detect plaintext.	② In this, the keys which are nearer to the correct key can disclose plain text.
③ In this character's Identity is changed while its position remains unchanged.	③ In this the position of the charater is changed but character's identity is not changed.
④ Example :- Caesar cipher	④ Example :- Reil Fence cipher.