ST. FRANCIS INSTITUTE OF TECHNOLOGY
DEPARTMENT OF INFORMATION TECHNOLOGY

SECURITY LAB

Experiment – 2: Implementation of Playfair Cipher

Aim: To implement Playfair Cipher Technique and understand cryptanalysis of the same.

Objective: After performing the experiment, the students will be able to –

- To understand the encryption and decryption using polyalphabetic substitution technique.
- To understand that secure encryption is not possible with a small keyspace.

Lab objective mapped: L502.1: Students should be able to apply the knowledge of symmetric cryptography to implement simple ciphers.

Prerequisite: Basic knowledge of cryptography.

Requirements: JAVA/PYTHON

Pre-Experiment Theory:

Playfair Cipher:

1. WHAT IS PLAYFAIR CIPHER?

Playfair cipher is the first and best-known digraph substitution cipher, which uses the technique of symmetry encryption. Invented in 1854 by Charles Wheatstone, the cipher got its name from Lord Playfair, who promoted its use. Unlike single letters in a simple substitution cipher, the Playfair cipher technique encrypts digraphs or parts of letters.

The Playfair cipher is relatively fast and doesn't require special equipment. British Forces used it for tactical purposes during World War I and the Second Boer War, and Australians utilized it during World War II. The primary use of the cipher was for protecting vital but non-critical secrets during actual combat. By the time the enemy cryptanalysts could decrypt the information, it was useless for them.

2. **PLAYFAIR CIPHER'S RELEVANCE**

The Playfair cipher was significantly popular in the World War I and II era because of its complexity level compared to the then available ciphers. Further, it didn't need any special tools or equipment to encrypt or decrypt the information. However, after the invention of computers, the Playfair cipher was no longer used, as the computers can solve Playfair ciphers in a few seconds using break codes. Due to this reason, with the advancement of digital encryption and the passage of time, Playfair cipher was no more an acceptable form of encoding messages as there was a risk of data getting into the wrong hands. Thus, Playfair cipher cannot be recommended for business organizations.

3. ALGORITHM

Generating the Key Square

- The 'key square' is a 5×5 grid consisting of alphabets that helps encrypt the plain text.
- All these 25 letters should be unique.

- Since the grid can accommodate only 25 characters, there is no 'J' in this table. Any 'J' in the plaintext is replaced by 'I'.
- Remove any characters or punctuation that are not present in the key square. Instead, spell out the numbers, punctuations, and any other non-alphabetic text.
- The key square will start with the key's unique alphabet in the order of appearance, followed by the alphabet's remaining characters in order.
  Ref: https://www.youtube.com/watch?v=U_J2xnhblPg

Rules for Playfair Cipher Encryption:

- **Case I – Both the letters in the digraph are in the same row –** Consider the letters right of each alphabet. Thus, if one of the digraph letters is the rightmost alphabet in the grid, consider the leftmost alphabet in the same row.
- **Case II – Both the letters in the digraph are in the same column –** Consider the letters below each alphabet. Thus, if one of the digraph letters is the grid's bottommost letter, consider the topmost alphabet in the same column.
- **Case III – Neither Case I or II is true** – Form a rectangle with the two letters in the digraph and consider the rectangle's horizontal opposite corners.

Ref: https://www.youtube.com/watch?v=O8MxWNfrzho
Ref: https://www.youtube.com/watch?v=66K1tplwYqg

Rules for Playfair Cipher Decryption:

- **Case I – Both the letters in the digraph are in the same row –** Consider the letters left of each alphabet. Thus, if one of the digraph letters is the leftmost letter in the grid, consider the rightmost alphabet in the same row.
- **Case II – Both the letters in the digraph are in the same column –** Consider the letters above each alphabet. Thus, if one of the digraph letters is the topmost letter in the grid, consider the bottommost alphabet in the same column.
- **Case III – Neither Case I or II is true** – Form a rectangle with the two letters in the digraph and consider the rectangle's horizontal opposite corners.

Ref: https://www.youtube.com/watch?v=2PUInSjhxNs

Breaking of Playfair Cipher:

Ref: https://www.youtube.com/watch?v=n6ljkcJXVFY

Output:

1. Attach complete program (with detailed comments explaining each step) performing encryption and decryption of playfair cipher.
2. Display the key matrix created out of a given keyword.
3. Display the output of code for plaintext "the key is hidden under the door pad" with keyword "GUIDANCE" and its decryption.
4. Display the output of code (encryption as well as decryption) for plaintext given in post experiment exercise.

Post Experimental Exercise-

Solve the following exercise on the journal sheets.

1. Encrypt message using playfair cipher : THE WORLD OF CRYPTOGRAPHY
   Key: MONARCHY *[theoretical result and code output attached should match]*

Conclusion:

The basic features of classical cryptographic technique: Playfair Cipher are understood by implementing a code for encryption and decryption when key is known and also understood breaking of key when key space is very small by performing cryptanalysis of ciphertext.