Green University of Bangladesh

Department of Computer Science and Engineering (CSE)

Semester: (Spring, Year: 2024), B.Sc. in CSE (Day)

KSA - 01

Implementation of Playfair Cipher on a Webpage

Course Title: Computer and Cyber Security

Course Code: CSE 323

Section: 213D1

Students Details

Name	ID
Md.Shakil Mia	213002147
Saydur Rahman	213002144

Submission Date: 24/12/2024

Course Teacher's Name: Sakhaouth Hossan

[For teachers use only: Don't write anything inside this box]

Contents

Project Status

Marks: Signature:

Comments: Date:

Introduction

Key Matrix Creation

The Playfair cipher relies on the creation of a key matrix, a 5x5 grid constructed using a keyword. Each letter of the keyword appears only once in the matrix, and the letters 'I' and 'J' are treated as equivalent to fit the 25-character grid. Any remaining unused letters of the alphabet are added to complete the matrix. This key matrix serves as the foundation for the encryption and decryption processes.

Text Preparation

Text preparation is a critical step in using the Playfair cipher. The plaintext is first processed to fit the digraph structure of the cipher, meaning it is divided into pairs of letters. If a pair contains repeated letters, an 'X' is inserted between them to separate them (for example, "BALLOON" becomes "BA LX LO ON"). If the plaintext has an odd number of letters, an 'X' is added to the end to ensure even pairing.

Encryption and Decryption Rules

The encryption and decryption rules of the Playfair cipher are straightforward yet effective. For letters that are in the same row of the key matrix, each letter is replaced by the letter immediately to its right, wrapping around to the start of the row if necessary. Similarly, letters in the same column are replaced by the letters immediately below them, wrapping around to the top of the column if necessary. If the letters form a rectangle in the matrix, they are replaced by the letters on the same row but at the opposite corners of the rectangle.

Implementation

In implementing the Playfair cipher, JavaScript functions are employed to handle the creation of the key matrix, preparation of the text, and the core encryption and decryption logic. The user-friendly interface, designed with HTML and CSS, allows users to interactively generate the key matrix, input plaintext, and observe the resulting encrypted and decrypted messages. This visualization aids in comprehending each step of the encryption and decryption processes, highlighting the practical application of classical cryptographic methods.

Objectives

The primary objective of this project is to implement and demonstrate the functionality of the Playfair cipher using a web-based interface. The specific goals include:

- Interactive Key Matrix Generation: Provide users with the ability to input a custom key, which will be used to generate the Playfair cipher's key matrix dynamically.
- Text Encryption and Decryption: Allow users to input plaintext, which will be encrypted using the Playfair cipher. Additionally, the interface will decrypt the ciphertext back to plaintext, showcasing the full encryption-decryption cycle.
- Visualization of Encryption Process: Offer a detailed, step-by-step visualization of the text preparation, encryption, and decryption processes to enhance user understanding of the Playfair cipher mechanism.
- User-Friendly Interface: Design a responsive and intuitive interface that is easy to use, with clear instructions and feedback mechanisms to guide users through the encryption and decryption processes.

Motivation

The key motivations for implementing this project are:

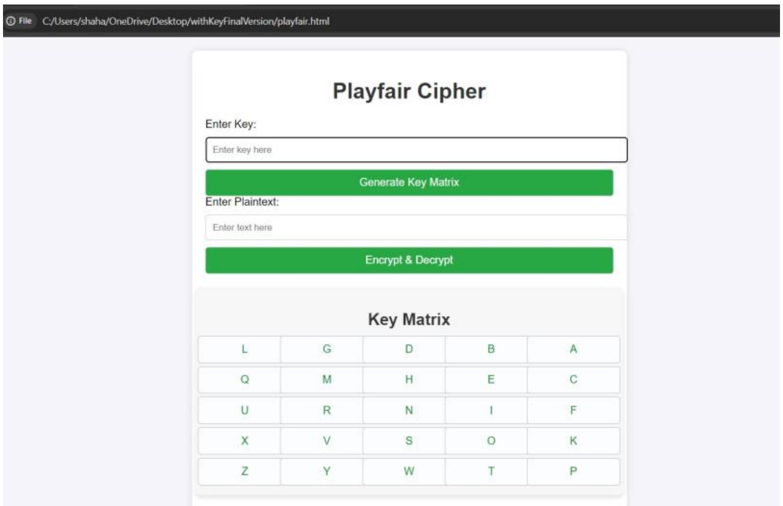
- Educational Tool: To serve as an educational resource that helps students and enthusiasts understand the principles of classical cryptography through hands-on interaction.
- Historical Appreciation: To foster an appreciation for historical cryptographic methods and their evolution, providing context for modern encryption techniques.
- Practical Demonstration: To demonstrate the practical application of the Playfair cipher, including key matrix generation, text preparation, and the actual encryption and decryption processes.
- Interactive Learning: To leverage modern web technologies to create an interactive learning environment that makes cryptographic concepts accessible and engaging.

Algorithm

Algorithm 1 Playfair Cipher Encryption and Decryption

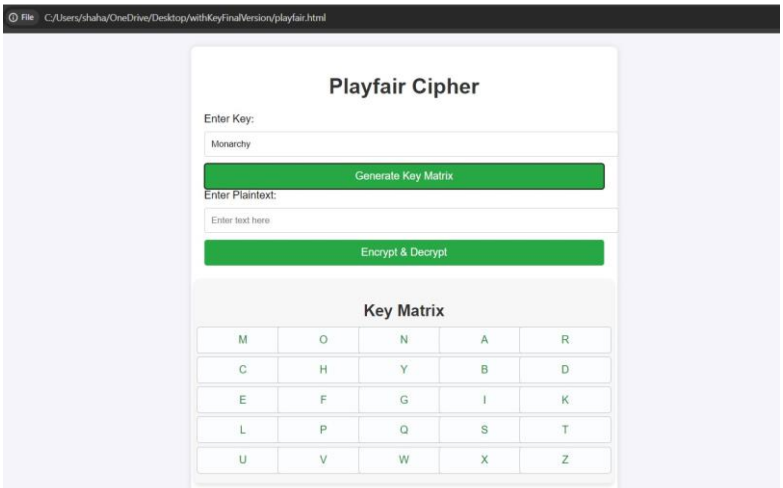
```
Step 1: Key Matrix Creation
Initialize a default key matrix with predefined letters.
if key $K$ is provided then
    Convert $K$ to uppercase and remove non-letter characters.
    Replace 'I' with 'J'.
    Create a 5x5 matrix with $K$ and remaining alphabet letters.
    Use a USED[26] array to ensure no duplicate characters in the key matrix. end
if
Step 2: Plaintext Preparation
Take plaintext input $P$ from the user.
Convert $P$ to uppercase and remove non-letter characters.
Replace ’I’ with ’J’.
Initialize an empty string $P_{prepared}$.
for each character $c$ in $P$ do if $c$ is equal to
    the next character then
        Append $c$ and ’X’ to $P_{prepared}$. else
        Append $c$ to $P_{prepared}$.
    end if
end for if length of $P_{prepared}$ is
odd then Append ’X’ to
$P_{prepared}$.
end if
Step 3: Encryption and Decryption
Set encrypt flag to true for encryption and false for decryption. Initialize
empty strings $C$ and $D$.
for each pair of characters $(a,b)$ in $P_{prepared}$ do Find
    positions $(i_1, j_1)$ and $(i_2, j_2)$ in the key matrix.
    if $i_1 = i_2$ then          Same row if encrypt is true then
            Replace $a$ and $b$ with characters to their immediate right.
        else
            Replace $a$ and $b$ with characters to their immediate left.
        end if
    else if $j_1 = j_2$ then          Same column if encrypt is true then
            Move $a$ and $b$ to characters below them.
        else
            Move $a$ and $b$ to characters above them.
        end if
    else                                                     Forming a rectangle
        Swap $a$ and $b$ to the ends of the columns.
    end if
    Append the result to $C$ if encrypt is true, otherwise append to $D$.
end for
```

Inputs and Outputs



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

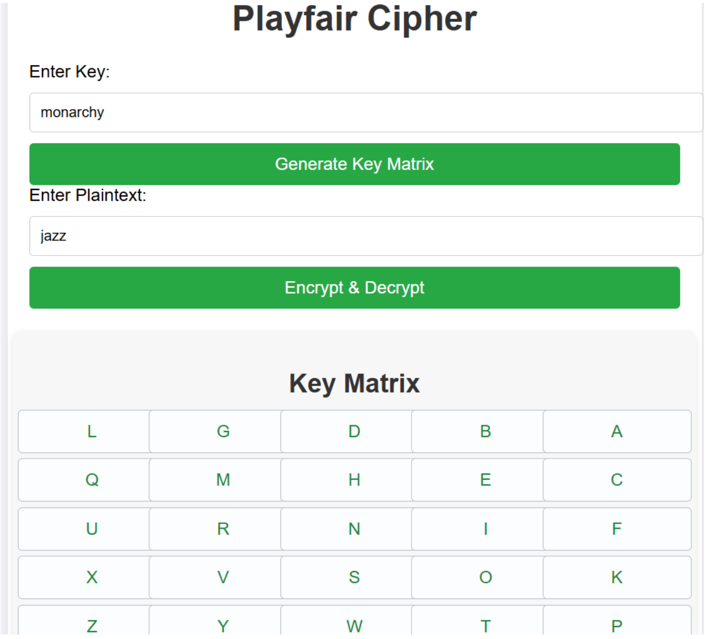
Figure 1: Default Key Matrix without any Keyword



Enter Key: Monarchy

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

Figure 2: Key Matrix with Keyword "MONARCHY"



Playfair Cipher

Enter Key:

monarchy

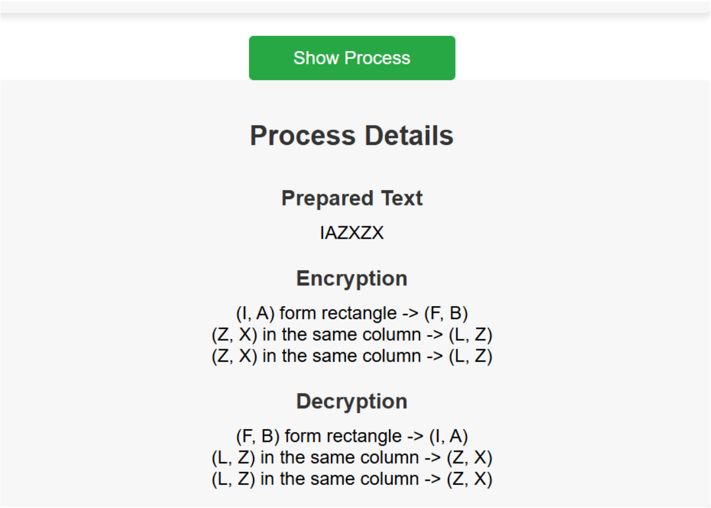
Enter Plaintext:

jazz

Key Matrix

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

Figure 3: Encryption and decrytion of text "JAZZ"



Process Details

Prepared Text

IAZXZX

Encryption

(I, A) form rectangle -> (F, B)
(Z, X) in the same column -> (L, Z)
(Z, X) in the same column -> (L, Z)

Decryption

(F, B) form rectangle -> (I, A)
(L, Z) in the same column -> (Z, X)
(L, Z) in the same column -> (Z, X)

Figure 4: Process of text preparation and Encryption and decrytion of text "jazz "

Analysis and Discussion

Reflecting on the project, our project is on demonstrating playfair cipher with webbased UI, by doing the project we have learned about the inner workings of playfair cipher, concepts like key matrix and text preparation and encryption and decryption based on the position variables.

Also seeing the projects done with parallel to ours by our friends, gave us a deeper understanding on encryption algorithm, it helped us to visulaize the process of cipher and decipherment, also we had to experience some unique UI approcahes to visualsing these projects. Abstracting the inner working and making simple visual element gave us a new perspective on encryption techniques. We had some difficulties doing it, for example translating the algorithm to appropriate environment and making it work with user interaction was quite difficult. Overall it was a practical learning experience and this can serve as a foundation for future exploration of more complex ciphers.