



Kingdom Of Saudi Arabia  
Ministry of Education  
King Faisal University  
College of Computer Science and  
Information Technology (CCSIT)



# COMPUTER SECURITY COURSE PROJECT PROGRAMMING PROJECT "PLAYFAIR"

Name	Student ID
<i>Mahdi Jameel Alzakari</i>	<b>221415196</b>
<i>Mahdi Ali AL Mutawa</i>	<b>221425942</b>
<i>Abdulrhman Albusaad</i>	<b>221434010</b>
<i>Faris Hassan ALSalmi</i>	<b>221434782</b>

## Table of Contents

<b>Introduction .....</b>	<b>2</b>
<b>System description .....</b>	<b>2</b>
<b>System scope and goals.....</b>	<b>5</b>
<b>Algorithm description.....</b>	<b>5</b>
<b>Algorithm weaknesses and limitations .....</b>	<b>7</b>
<b>References: .....</b>	<b>8</b>

## Introduction

The Playfair cipher, an encryption technique that employs a letter substitution method based on a key-guided 5x5 grid, stands as a classic cryptographic system designed to secure communications. Developed using the Dart programming language and Flutter framework, this interactive system demonstrates both the encryption and decryption processes of the Playfair cipher, providing a clear, user-friendly platform for understanding these operations. By enabling users to input a plaintext or ciphertext along with a keyword, the system efficiently transforms messages into encrypted or decrypted forms, making it an excellent educational tool for those new to the field of cryptography. The primary goal of this system is to demystify the Playfair cipher method, presenting its components and functionality in an accessible manner, thereby enhancing comprehension of basic cryptographic principles without requiring prior technical expertise.

## System description

- Purpose of the system.

This system, developed using the Dart programming language and Flutter framework, demonstrates the functionality of the Playfair cipher. The primary aim is to offer users a clear and interactive way to understand the encryption and decryption processes involved in the Playfair cipher. By transforming plaintext into ciphertext using paired letter substitution based on a specified key, this method ensures secure communication.

# Playfair Cipher

Is a polygraphic substitution cipher that employs a 5x5 grid of letters for encryption, making it more resistant to frequency analysis compared to traditional ciphers. Its strength lies in its use of digraphs, where pairs of letters are encrypted based on their positions within the grid.




## - Components of the system.

This system consists of various components. Each component is determined by the user choice Encryption or Decryption, user secret key to create the Playfair cipher grid. There is a section for inputting text, which is common to all parts of the system. Additionally, there is a component that converts the text into a readable message - Plain text -, and another component that reverses the process, turning the scrambled message back into normal text - Cipher text -.


- ❖ **Key:** A keyword or phrase used to create the Playfair cipher grid.
- ❖ **Encryption Algorithm:** An algorithm that converts plaintext into ciphertext using the Playfair grid.
- ❖ **Decryption Algorithm:** An algorithm that converts ciphertext into plaintext using the Playfair grid.


# Enter Your Key



Encrypt

Decrypt





Show Playfair Table



## - System environment “Input and output of the system”.

### ▪ Input

The Playfair cipher program requires two primary inputs: the message and the keyword. The message is the one that requires encryption or decryption, as the keyword serves as the key for both processes. The software requires the text message to only contain alphabetic letters, with no numbers or special characters included. In the same way, the keyword must consist solely of alphabetical characters.

### ▪ Output

The Playfair cipher program generates either the encrypted ciphertext or the decrypted plaintext, based on the user's chosen mode. The encrypted message contains letters and spaces, and the decrypted text is the message originally entered by the user.

## System scope and goals

The primary goal of this system is to demystify the Playfair cipher, a secure method for encrypting and decrypting messages by substituting pairs of letters based on a specific key. This system provides an interactive and intuitive platform that simplifies the cryptographic processes, making it accessible to users without prior expertise.

## Algorithm description

- Defining the problem.

The aim of the algorithm is to transform plain text into a ciphertext text (encryption) and then transform it back to plain text (decryption) according to the user, using the Playfair cipher technique.

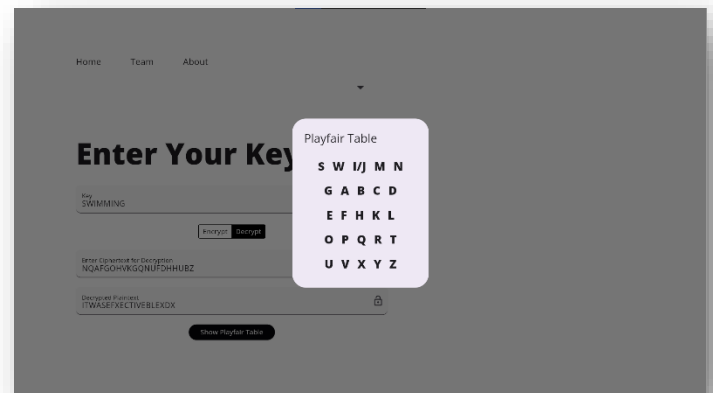
- Nature of Input and Output.

In the encryption process, the user provides a plaintext message as input, for decryption, the input is the ciphertext. For both processes, the user must also enter a key consisting of English alphabet. The output for encryption is the ciphertext, while for decryption, it's the original plaintext.

- Functions of the Algorithm.

- ❖ **Encryption function.**

The Playfair cipher transforms plain text letters into pairs based on a key rule set and a 5 x 5 grid. Each pair undergoes encryption by following specific grid-based rules:



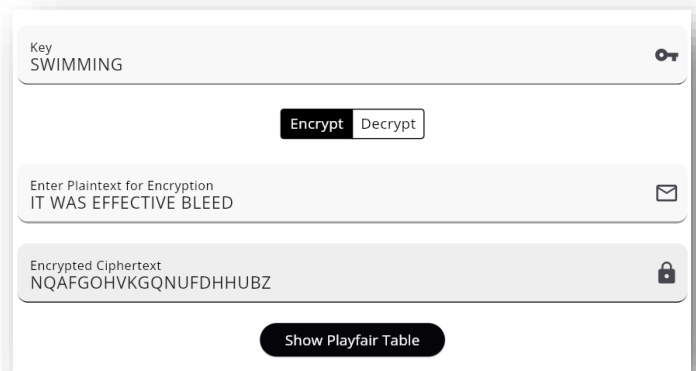
1. Same row: shift right, wrapping around if needed.
2. Same column: shift downward, wrapping around if needed.
3. Forming a Box: swap with opposite corners on the same row. These rules ensure the conversion of each letter pair into an encrypted letter.

In the Playfair cipher, handling identical consecutive letters in a word involves changing one of the letters. For example, in the word "meet", we insert a letter, typically 'X', resulting in "mXet". Then we proceed with the encryption process as usual.

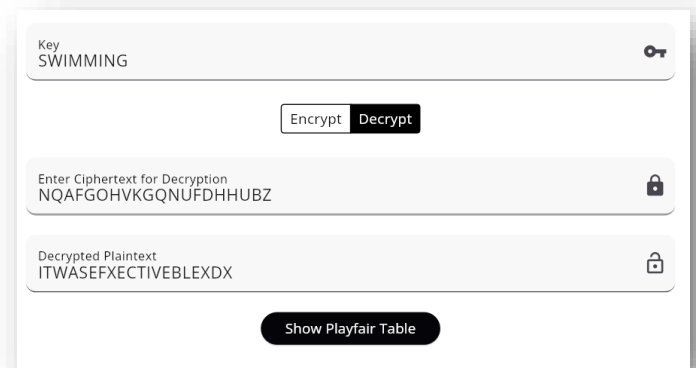
#### ❖ **Decryption function.**

The decryption function for the Playfair cipher reverses the encryption process. Given the encrypted letter pairs, each pair is decrypted by following the reverse of the encryption rules:

1. For pairs in the same row: shift left, wrapping around if needed.
2. For pairs in the same column: shift upward, wrapping around if needed.
3. For pairs forming a box: swap with opposite corners on the same row.



A screenshot of a web-based Playfair cipher encryption tool. At the top, a key 'SWIMMING' is entered next to a key icon. Below this are two buttons: 'Encrypt' (highlighted) and 'Decrypt'. The main input area is labeled 'Enter Plaintext for Encryption' and contains the text 'IT WAS EFFECTIVE BLEED' next to an envelope icon. Below the input, the 'Encrypted Ciphertext' is shown as 'NQAFGOHVKGQNUFDHHUBZ' next to a lock icon. At the bottom, there is a 'Show Playfair Table' button.



A screenshot of a web-based Playfair cipher decryption tool. At the top, the same key 'SWIMMING' is entered. The buttons are 'Decrypt' (highlighted) and 'Encrypt'. The main input area is labeled 'Enter Ciphertext for Decryption' and contains the text 'NQAFGOHVKGQNUFDHHUBZ' next to a lock icon. Below the input, the 'Decrypted Plaintext' is shown as 'ITWASEFFECTIVEBLEDX' next to a lock icon. At the bottom, there is a 'Show Playfair Table' button.

## Algorithm weaknesses and limitations

- Vulnerability to Known Plaintext Attacks:

If a large part of the original message is revealed, the Playfair cipher can be easily compromised through known plaintext attacks, resulting in reduced security.

- Limited Character Set:

The Playfair cipher can only encrypt letters and does not work with numbers or special characters.

- Key Space Limitation:

The Playfair cipher key space is restricted by the 5x5 grid size, resulting in lower security compared to newer encryption methods.

- Dependency on Keyword:

To decode messages, both the sender and recipient must share the same keyword, emphasizing the importance of effective key management for secure communication.



## References:

- [1] “Playfair cipher.” Encyclopaedia Britannica. Retrieved April 18, 2024, from <https://www.britannica.com/topic/Playfair-cipher>
- [2] “Playfair Cipher.” Boxentriq. Retrieved April 21, 2024, Retrieved from <https://www.boxentriq.com/code-breaking/playfair-cipher>
- [3] Stallings, W., & Brown, L. (2015). “Computer Security: Principles and Practice (3rd ed.)”. Prentice Hall. ISBN: 9780133773927.