

# REPORT

Laboratory work No. 3

Course: Cryptography and Security

Theme: Polyalphabetic ciphers

*Author:* Corneliu Catlabuga  
FAF-213

*Checked by:* univ. assist.  
Cătălin Mîțu

## Objective:

Study and implement the Playfair algorithm in a programming language.

## Task:

Implement the Playfair algorithm in a programming language which supports text encryption and decryption supporting the Romanian alphabet. The script should take in a message/ciphertext containing [A-Za-z], including “Ăă, Ââ, Îî, Șș, Țț” and spaces and a keyword respecting the same requirements.

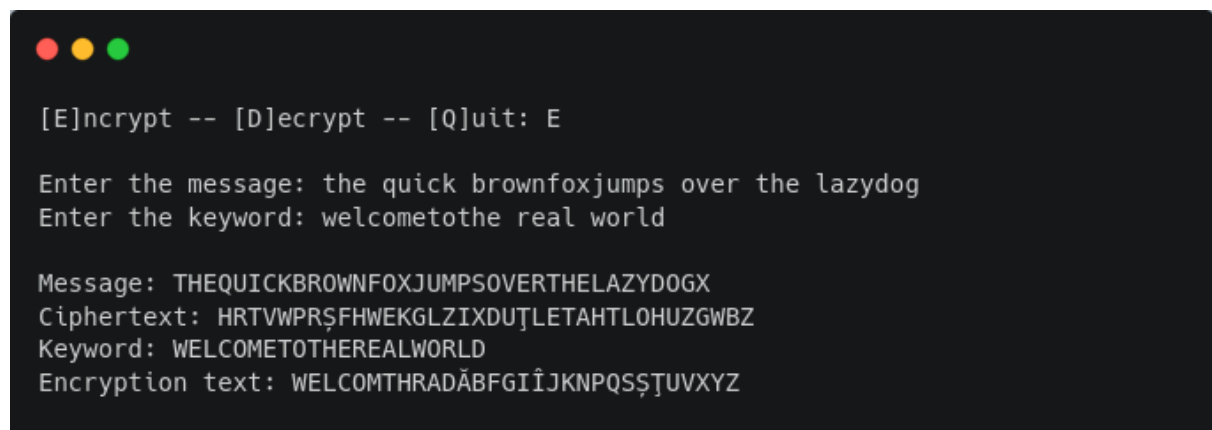
## Theoretical considerations:

The technique encrypts pairs of letters (bigrams or digrams), instead of single letters as in the simple substitution cipher and rather more complex Vigenère cipher systems then in use. The Playfair is thus significantly harder to break since the frequency analysis used for simple substitution ciphers does not work with it. The frequency analysis of bigrams is possible, but considerably more difficult.

## Implementation, practical results:

When starting the script the user is prompted to select one of the three options: E – encrypt, D – decrypt and Q – quit, selecting any other option is not supported and will print the introduction screen again.

### Playfair Encryption



```
[E]ncrypt -- [D]ecrypt -- [Q]uit: E

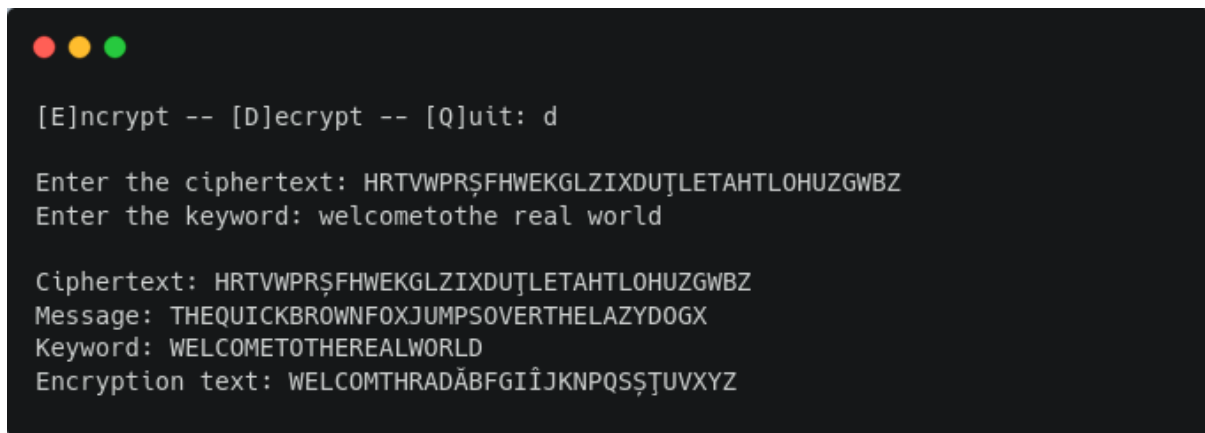
Enter the message: the quick brownfoxjumps over the lazydog
Enter the keyword: welcometothe real world

Message: THEQUICKBROWNFOXJUMPSOVERTHELAZYDOGX
Ciphertext: HRTVWPRŞFHWEKGLZIXDUȚLETAHTLOHUZGWBZ
Keyword: WELCOMETOTHEREALWORLD
Encryption text: WELCOMTHRADĂBFGIÎJKNPQŞŞTUVXYZ
```

**Figure 1:** Text encryption output

When selecting the Encrypt option the user is prompted to enter a message, in this case the message is “the quick brownfoxjumps over the lazydog” with the keyword “welcometothe real world”. The encrypted version of the text is “HRTVWPRŞFHWEKGLZIXDUȚLETAHTLOHUZGWBZ”.

## Playfair Decryption

A terminal window with a dark background and three colored window control buttons (red, yellow, green) in the top-left corner. The terminal displays the following text:

```
[E]ncrypt -- [D]ecrypt -- [Q]uit: d

Enter the ciphertext: HRTVWPRŞFHWEKGLZIXDUŦLETAHTLOHUZGWBZ
Enter the keyword: welcometothe real world

Ciphertext: HRTVWPRŞFHWEKGLZIXDUŦLETAHTLOHUZGWBZ
Message: THEQUICKBROWNFOXJUMPSOVERTHELAZYDOGX
Keyword: WELCOMETOTHEREALWORLD
Encryption text: WELCOMTHRADĂBFGIÎJKNPQSŞŦUVXYZ
```

**Figure 2:** Text decryption output

When selecting the Decrypt option the user is prompted to enter the cyphertext (note: the script will output an error if the length of the ciphertext is odd) and the keyword. When decrypting the ciphertext “HRTVWPRŞFHWEKGLZIXDUŦLETAHTLOHUZGWBZ” with the keyword “welcometothe real world” the message is “THEQUICKBROWNFOXJUMPSOVERTHELAZYDOGX”.

### Conclusions:

In summary, the Playfair cipher is a classical symmetric key cryptographic algorithm characterized by its utilization of a 5x5 (adaptable to other alphabets) key matrix to encrypt plaintext messages. Its strength lies in its ability to efficiently encrypt digraphs (pairs of letters) while providing resistance against basic frequency analysis attacks. Although it lacks the robustness of modern encryption algorithms, the Playfair cipher remains a valuable historical artifact in the field of cryptography.

### References:

1. Github repository: [https://github.com/muffindud/CS\\_Lab/tree/lab3/lab3](https://github.com/muffindud/CS_Lab/tree/lab3/lab3)