

Ministerul Educatiei, Culturii și Cercetarii al Republicii Moldova Universitatea Tehnic**ă** a Moldovei

Facultatea Calculatoare, Informatic**ă ş**i Microelectronic**ă** Departamentul Ingineria Software și Automatica

Report

for laboratory work No. 3

course "Cryptography and Security"

Done by:

Ciumac Alexei, gr.

FAF-212

Checked by:  
 Cǎtǎlin MÎŢU

Chișinău – 2023

**Subject:** Cryptanalysis of monoalphabetic ciphers

## Tasks:

To create a Playfair algorithm implementation in a programming language suitable for processing messages in Romanian, which consists of 31 letters, you need to ensure that the characters in the text fall within the 'A' to 'Z' and 'a' to 'z' range. Any characters outside this range should be flagged as incorrect. It's essential for the key to be at least 7 characters long. Users should have the option to choose between encryption and decryption, input their key, message, or cryptogram, and receive the decrypted cryptogram or message. Adding new spaces, as necessary, based on the chosen language and the message's logic, will be a manual step in the final stage of processing.

**Theory :**

The Playfair cipher, often associated with Lord Playfair but originally invented by Charles Wheatstone in 1854, is a historic encryption technique. This digraph substitution cipher became prominent in the 19th century. It hinges on the creation of a 5x5 key matrix derived from a secret key phrase, which could be any combination of letters, including omitting duplicates and treating 'I' and 'J' as one.

It was used for tactical purposes by British forces in the Second Boer War and in World War I and for the same purpose by the Australians during World War II. This was because Playfair is reasonably fast to use and requires no special equipment

**Implementation:**

***Step 1: Prepare the Text for Encryption***

Convert the entire plaintext to uppercase.

Replace all occurrences of "J" with "I" to treat them as the same letter.

Create letter pairs (couples) from the plaintext.

Remove any spaces and punctuation from the letter pairs.

***Step 2: Construct the Encryption Matrix (Playfair Table)***

Ensure there are no duplicate letters in the key and handle "J"s by treating them as "I."

Create the Playfair matrix by adding the key and the remaining letters of the alphabet without duplication. The key letters are placed first, and then the remaining letters are filled in, usually from left to right and top to bottom.

***Step 3: Encrypt the Message***

For the encryption process, you'll perform the following substitutions based on the position of the letters within the Playfair matrix:

**For Different Rows and Columns:**

If the two letters of a letter pair are in different rows and columns, replace each letter with the letter in the same row but from the column of the other letter.

**For the Same Rows:**

If the two letters are in the same row, replace each letter with the next letter in the same row. If a letter is at the end of the row, wrap around to the beginning of the row.

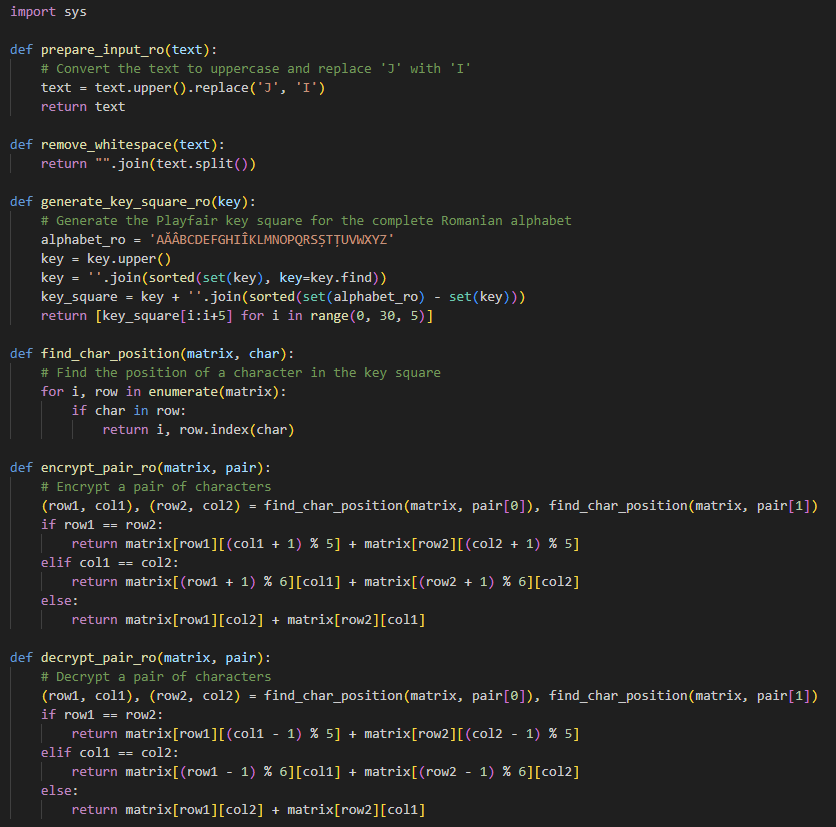
**For the Same Columns:**

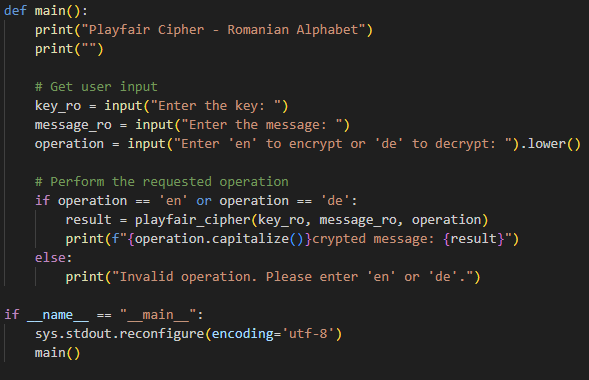
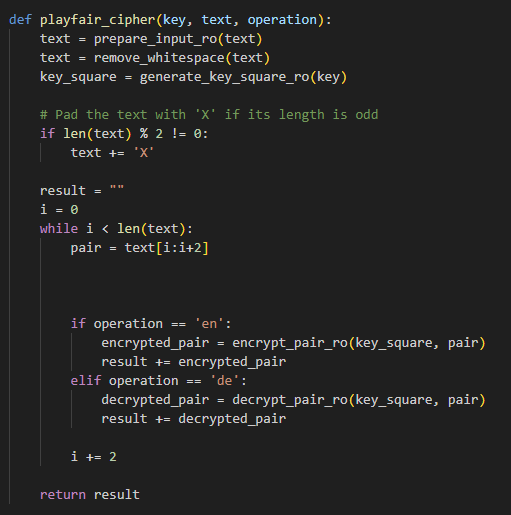
If the two letters are in the same column, replace each letter with the next letter in the same column. If a letter is at the bottom of the column, wrap around to the top of the column .

After applying these rules, you will have successfully encrypted the plaintext using the Playfair cipher.

**By applying these rules in reverse, you will successfully decrypt the ciphertext back into the original plaintext using the Playfair cipher.**

**Code Snippets:**





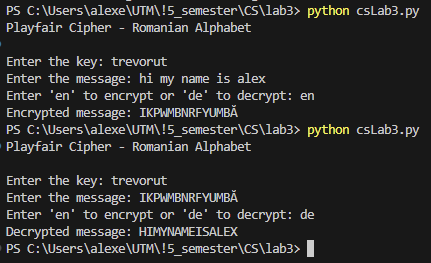


Figure 1 Example of Encryption/Decryption

**Conclusion:**

In the lab, we've learned about the Playfair cipher, an old encryption method. It showed us how to encrypt and decrypt messages following certain rules. This understanding is a building block for data security. The Playfair cipher has its place in history and connects with today's data security practices.