

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

Інститут комп'ютерних наук та інформаційних технологій

Кафедра інформаційних систем та мереж



Лабораторна робота №1

з дисципліни: «Технології захисту інформації»

на тему: «Симетричні методи шифрування інформації»

Варіант №6

Виконала:

студентка групи ІТ-32

Моляща Ю.А.

Прийняв:

Табачишин Д.Р.

Львів - 2023

Лабораторна робота №1

«Симетричні методи шифрування інформації»

Мета роботи: навчитися опрацьовувати (шифрувати та дешифрувати) файли на основі методів симетричного шифрування.

Завдання на лабораторну роботу.

Завдання 1. Написати програму на мові C++ (чи іншій за згодою викладача) яка виконує криптографічні перетворення (шифрування та дешифрування) над файлами за одним з методів симетричного шифрування відповідно до заданого варіанту приведенного в таблиці.

Варіант 6. Шифр Цезаря, що передбачає зсув на 8 символів даних англійської абетки. Результат представити у рядковому представленні.

Хід роботи.

Код програми:

```
# Define shift value
shift = 8
def encrypt(text):
    # Define empty string for encrypted text
    encrypted_text = ""
    for char in text:
        # Check if character is letter
        if char.isalpha():
            if char.islower():
                # Get encrypted character for lowercase letter
                encrypted_char = chr(((ord(char) - ord('a') + shift) % 26) +
ord('a'))
            else:
                # Get encrypted character for uppercase letter
                encrypted_char = chr(((ord(char) - ord('A') + shift) % 26) +
ord('A'))
            # Add encrypted character to encrypted text
            encrypted_text += encrypted_char
        else:
            # If character is not letter, add it to encrypted text
            encrypted_text += char
    return encrypted_text
# Define decrypt function
def decrypt(encrypted_text):
    # Define empty string for decrypted text
    decrypted_text = ""
    for char in encrypted_text:
        # Check if character is letter
        if char.isalpha():
            if char.islower():
```

```

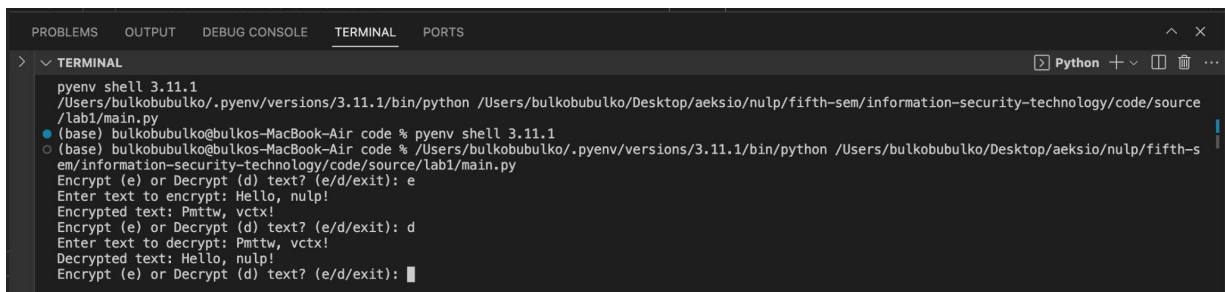
        # Get decrypted character for lowercase letter
        decrypted_char = chr(((ord(char) - ord('a') - shift) % 26) +
ord('a'))
    else:
        # Get decrypted character for uppercase letter
        decrypted_char = chr(((ord(char) - ord('A') - shift) % 26) +
ord('A'))

    # Add decrypted character to decrypted text
    decrypted_text += decrypted_char
else:
    # If character is not letter, add it to decrypted text
    decrypted_text += char
return decrypted_text
def main():
    while True:
        choice = input("Encrypt (e) or Decrypt (d) text? (e/d/exit):
").strip().lower()
        if choice == 'e':
            text = input('Enter text to encrypt: ')
            text_encrypted = encrypt(text)
            print('Encrypted text:', text_encrypted)
        elif choice == 'd':
            text = input('Enter text to decrypt: ')
            text_decrypted = decrypt(text)
            print('Decrypted text:', text_decrypted)
        elif choice == 'exit':
            break
        else:
            print('Invalid choice. Please select a valid option (e/d/exit).')

if __name__ == "__main__":
    main()

```

Приклад виконання зображено на Рис. 1.



```

pyenv shell 3.11.1
/Users/bulkobubulko/.pyenv/versions/3.11.1/bin/python /Users/bulkobubulko/Desktop/aeksio/nulp/fifth-sem/information-security-technology/code/source
/lab1/main.py
(base) bulkobubulko@bulkos-MacBook-Air code % pyenv shell 3.11.1
(base) bulkobubulko@bulkos-MacBook-Air code % /Users/bulkobubulko/.pyenv/versions/3.11.1/bin/python /Users/bulkobubulko/Desktop/aeksio/nulp/fifth-s
em/information-security-technology/code/source/lab1/main.py
Encrypt (e) or Decrypt (d) text? (e/d/exit): e
Enter text to encrypt: Hello, nulp!
Encrypted text: Pmttw, vctx!
Encrypt (e) or Decrypt (d) text? (e/d/exit): d
Enter text to decrypt: Pmttw, vctx!
Decrypted text: Hello, nulp!
Encrypt (e) or Decrypt (d) text? (e/d/exit): 

```

Рис. 1. Приклад виконання

Посилання на GitHub-репозиторій: <https://github.com/bulkobubulko/nulp-ist>

Висновок: під час виконання лабораторної роботи було вивчено опрацювання (шифрування та дешифрування) файлів на основі методів симетричного шифрування.