­­МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ “ЛЬВІВСЬКА ПОЛІТЕХНІКА”

Інститут прикладної математики та фундаментальних наук

Кафедра прикладної математики

**ЗВІТ**

про виконання лабораторної роботи № 6  
з дисципліни

***«*АЛГОРИТМИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ МЕРЕЖАХ*»***

Виконав:  
студент  
групи ПМ-43  
Павло Гутковський  
Прийняв:   
Ліснічук А. Є.

Львів 2023

­­ **Лабораторна робота №6**

***Тема:***

Шифр Плейфера: процедура дешифрування

***Мета:***

Отримати навики практичної реалізації процедури дешифрування для шифру Плейфера

***Постановка задачі:***

1. Програмно реалізувати процедуру дешифрування шифром Плейфера, використовуючи свою, запропоновану у лабораторній роботі №5, таблицю-ключ;

2. Дешифрувати криптограму, отриману у результаті виконання лабораторної роботи №5, і перевірити чи отримано правильний відкритий текст про свій любимий напиток;

3. Підготувати опис/звіт про виконану роботу.

***Короткі теоретичні відомості:***

Базові теоретичні відомості про шифр Плейфера і засади реалізації процедури шифрування наведено у описі до лабораторної роботи №5. При дешифруванні використовуємо ту саму матрицю-ключ, що і при шифруванні. При дешифруванні використовуємо також ті самі три правила, як і при шифруванні (див. опис до лабораторної роботи №5), тільки виконуємо протилежні дії.

**Правило 1:** якщо дві літери криптограми окреслюють прямокутник, то вибираємо відповідні літери з протилежних кутів цього прямокутника, причому лівій літері прямокутника відповідає ліва, а правій – права.

**Правило 2:** якщо дві літери криптограми знаходяться в одному рядку матриці, то вибираємо відповідні літери лівіше від них (у кільці).

**Правило 3:** якщо дві літери криптограми знаходяться в одному стовпці матриці, то вибираємо відповідні літери, які знаходяться у матриці вище від них (у кільці).

Винятком із цих правил є випадок, коли у блоці для дешифрування є дві однакові літери. У такому випадку домовляємося вибирати дві однакові літери, що розміщені у матриці лівіше (у кільці).

***Програмна реалізація:***

def readFromFileMatrix(*fileName*):  
 matrix = []  
 with *open*(*fileName*, "r", *encoding*="utf-8") as file:  
 lines = file.readlines()  
 for line in lines:  
 row = *list*(line.strip())  
 row = [char for char in row if char != ' ']  
 matrix.append(row)  
 return matrix  
  
  
def readFromFile(*fileName*):  
 with *open*(*fileName*, 'r', *encoding*="utf-8") as file:  
 lines = file.read()  
 file.close()  
 return lines  
  
  
def findInMatrix(*el*, *table*):  
 for i in *range*(4):  
 for j in *range*(8):  
 if *el* == *table*[i][j]:  
 return i, j  
  
  
def decrypt(*text*, *table*):  
 out = ''  
 for i in *range*(0, *len*(*text*), 2):  
 two\_letters = *text*[i:i + 2]  
 i1, j1 = findInMatrix(two\_letters[0], *table*)  
 i2, j2 = findInMatrix(two\_letters[1], *table*)  
 *# По прямокутнику* if i1 != i2 and j1 != j2:  
 out += *table*[i2][j1] + *table*[i1][j2]  
 *# По рядку* elif i1 == i2:  
 out += *table*[i1][-1] if j1 - 1 < 0 else *table*[i1][j1 - 1]  
 out += *table*[i1][-1] if j2 - 1 < 0 else *table*[i1][j2 - 1]  
 *# По стовпцях* elif j1 == j2:  
 out += *table*[-1][j1] if i1 - 1 < 0 else *table*[i1 - 1][j1]  
 out += *table*[-1][j1] if i2 - 1 < 0 else *table*[i2 - 1][j2]  
 return out  
  
  
line = readFromFile('text.txt')  
table = readFromFileMatrix('matrix.txt')  
*print*(line)  
for i in table:  
 *print*(i)  
*print*(decrypt(line, table))

***Опис реалізації:***

writeToFile() функція запису у файл, cipherTable() генерація матриці Плейфера

decrypt() функція дешифрування, findInMatrix() функція пошуку елемента в матриці

writeToFileMatrix() функція запису матриці у файл, readToFileMatrix() функція зчитування

матриці з файлу

***Результати виконання:***

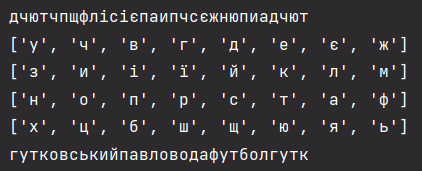


Рисунок 1 Зашифрована стрічка виведена в консоль з матрицею