­­МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ “ЛЬВІВСЬКА ПОЛІТЕХНІКА”

Інститут прикладної математики та фундаментальних наук

Кафедра прикладної математики

**ЗВІТ**

про виконання лабораторної роботи № 3  
з дисципліни

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

Виконав:  
студент  
групи ПМ-33  
Павло Гутковський  
Прийняв:   
Ліснічук А. Є.

Львів 2023

­­ **Лабораторна робота №3**

***Тема:***

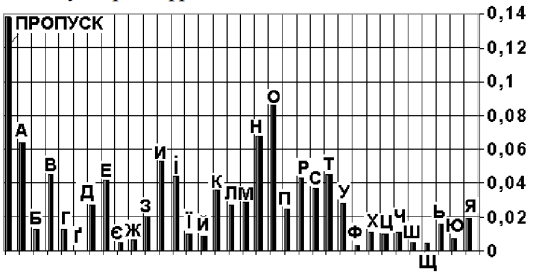
Гомофонний шифр: процедура дешифрування

***Мета:***

Отримати навики практичної реалізації процедури дешифрування для гомофонного шифру (шифру пропорційної заміни).

***Постановка задачі:***

1. використовуючи запропоновану Вами в лабораторній № 2 таблицю пропорційної заміни для української мови (отриману на основі наведених на рис. 2 даних про частоту літер в українській мові), програмно реалізувати шифр пропорційної заміни, використовуючи свою таблицю;



Частота літер в українській мові (%/100)

2. використовуючи файл зі своєю криптограмою з лабораторної № 2, дешифрувати інформацію про місцевість, у якій живуть Ваші батьки; результат записати у файл відкритого тексту;

3. перевірити правильність кінцевого тексту (тексту, який пройшов процедури шифрування і дешифрування).

4. проаналізуйте частоту символів у відкритому тексті та у криптограмі у вигляді табл. 2 та табл. 3; ці частоти повинні суттєво відрізнятися;

5. підготувати опис/звіт про виконану роботу.



***Короткі теоретичні відомості:***

Гомофонний шифр запропонував німецький математик Карл Гаус. Він відноситься до класу шифрів багатозначної заміни (одному символу відкритого тексту ставимо у відповідність один символ із певної множини символів). Цей шифр можна представити у вигляді таблиці, в якій одному символу вхідного алфавіту відповідає множина символів вихідного алфавіту, які вибираємо випадковим чином. Історично відомий різновид – шифр пропорційної заміни: чим більша частота появи символу у відкритому алфавіті, тим більше значень може відповідати цьому символу у вихідному алфавіті.

***Програмна реалізація:***

def readFromFile(*fileName*):  
 with *open*(*fileName*, 'r') as file:  
 lines = file.read()  
 file.close()  
 return lines  
  
  
def writeToFile(*line*, *fileName*):  
 with *open*(*fileName* + '.txt', "w") as file:  
 file.write(*line*)  
 file.close()  
  
  
def createTable(*frequency*):  
 table = [[] for \_ in *frequency*]  
 for i, freq in *enumerate*(*frequency*):  
 table[i] = [0] \* freq  
 return table  
  
  
def findIndex(*array*, *number*):  
 for i in *range*(*len*(*array*)):  
 if *number* in *array*[i]:  
 return i  
 return -1  
  
  
def printFrequencyTable(*arraySymbol*, *str*):  
 *print*("\n+===+========+")  
 for symbol in *arraySymbol*:  
 *print*("'{}' | {}%".format(symbol, *round*(*str*.count(symbol) / *len*(*str*) \* 100, 3)))  
 *print*("+===+========+\n")  
  
ukrainian\_alphabet = [" ", "а", "б", "в", "г", "ґ", "д", "е", "є", "ж", "з", "и", "і", "ї", "й", "к", "л", "м", "н",  
 "о", "п", "р", "с", "т", "у", "ф", "х", "ц", "ч", "ш", "щ", "ь", "ю", "я"]  
frequency\_ukrainian\_letter = [14, 7, 2, 5, 2, 1, 3, 4, 1, 1, 2, 6, 4, 1, 1, 4, 3, 3, 7, 9, 3, 4, 4, 5, 3, 1, 1, 1, 2, 1,  
 1, 2, 1, 2]  
text = "Львів це місто яке розташоване на заході України славиться своєю великою історією чарівною" \  
 " архітектурою великим культурним спадком та неймовірною гостинністю своїх мешканців"  
  
table, i = createTable(frequency\_ukrainian\_letter), 0  
readLine = readFromFile('encrypt.txt')  
numbers = readLine.split(' ')  
for line in readFromFile('table.txt').splitlines():  
 table[i] = line.split()  
 i += 1  
outputLine = ''  
for number in numbers:  
 outputLine += ukrainian\_alphabet[findIndex(table, number)]  
*print*(outputLine)  
  
printFrequencyTable(ukrainian\_alphabet, outputLine)  
printFrequencyTable([" ", "1", "2", "3", "4", "5", "6", "7", "8", "9", "0"], readLine)

***Опис реалізації:***

readFromFile – функцція що зчитує масив стрічок з файлу, writeToFile – запис в файл нашого результату, createTable – переробляємо зчитанні стрічки в readFromFile в таблицю, findIndex пошук букви по числу в таблиці, printFrequencyTable – вивід таблиці частот

***Результати виконання:***



