­­МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ “ЛЬВІВСЬКА ПОЛІТЕХНІКА”

Інститут прикладної математики та фундаментальних наук

Кафедра прикладної математики

**ЗВІТ**

про виконання лабораторної роботи № 2  
з дисципліни

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

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

Львів 2023

­­ **Лабораторна робота №2**

***Тема:***

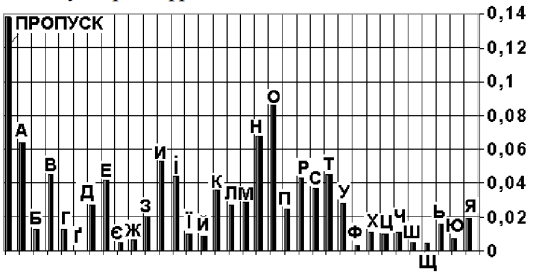
Гомофонний шифр: процедура шифрування

***Мета:***

Отримати навики практичної реалізації процедури шифрування для гомофонного шифру.

***Постановка задачі:***

1. використовуючи наведені на рис. дані про частоту літер в українській мові, запропонувати свою таблицю пропорційної заміни; пропуск вважати як ще одну додаткову літеру алфавіту; числа у таблиці використовувати або усі двоцифрові, або усі трицифрові;



Частота літер в українській мові (%/100)

2. програмно реалізувати процедуру шифрування для шифру пропорційної заміни, використовуючи свою таблицю;

3. написати текст про місцевість, у якій живуть батьки (довжиною біля 100 літер – відкритий текст; пробіли можна використовувати; розділові знаки та цифри не використовувати), і записати його у файл відкритого тексту;

4. зашифрувати цей текст шифром пропорційної заміни;

5. вихідний текст (криптограму) записати у файл, який буде використовуватися у лабораторній роботі №3;

6. 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:***

import random  
  
  
def writeToFile(*line*, *fileName*):  
 with *open*(*fileName* + '.txt', "w", *encoding*='utf-8') as file:  
 file.write(*line*)  
 file.close()  
  
  
def writeTableToFile(*table*):  
 for i in *range*(*len*(*table*)):  
 for j in *range*(*len*(*table*[i])):  
 with *open*("table.txt", "a") as file: file.write(  
 f"{*table*[i][j]} ")  
 with *open*("table.txt", "a") as file:  
 file.write(f"\n")  
 file.close()  
  
  
def createTable(*frequency*):  
 table, data = [[] for \_ in *range*(*len*(*frequency*))], []  
 for i in *range*(*len*(*frequency*)):  
 for k in *range*(*frequency*[i]):  
 while True:  
 cipheredSymbol = random.randint(100, 999)  
 if cipheredSymbol not in data:  
 table[i].append(cipheredSymbol)  
 data.append(cipheredSymbol)  
 break  
 return table  
  
  
def encrypt(*textToEncrypt*, *table*, *alphabet*):  
 encrypt\_line = ''  
 for letter in *textToEncrypt*:  
 index = *alphabet*.index(letter.lower())  
 encrypt\_line += f"{random.choice(*table*[index])}" + ' '  
 return encrypt\_line[:-1]  
  
  
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"  
  
writeToFile(text, 'text')  
table = createTable(frequency\_ukrainian\_letter)  
writeToFile(encrypt(text, table, ukrainian\_alphabet), 'encrypt')  
writeTableToFile(table)

***Опис реалізації:***

writeToFile - записує текст в файл, writeTableToFile - записує таблицю частот в файл, createTable - створює таблицю частот, encrypt – шифрує наш текст нашою таблицею частот

***Результати виконання:***

