**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»**

ІКТА

Кафедра ЗІ



**З В І Т**

**до лабораторної роботи №1**

**з курсу: «Основи криптографічного захисту інформації»**

Прийняв: доц. каф. ЗІ

Шандра З. А.

**Львів – 2018**

**Мета роботи:** Використання класичних криптоалгоритмів підстановки та перестановки для захисту текстової інформації. Метод Цезаря.

Завдання

1. Для одноалфавітного методу з фіксованим зміщенням визначити встановленне в програмі зміщення. Для цього потрібно:

* переглянути попередньо створений за допомогою редактора свій текстовий файл;
* виконати для цього файла шифровання;
* переглянути в редакторі зашифрований файл;
* переглянути гистограми вихідного та зашифрованого текстів;
* описати гістограми (в чому подібні, в чому різняться) і визначити, з яким зміщенням було виконано шифрування;
* розшифрувати зашифрований текст:
* за допомогою програми, після чого перевірити в редакторі правильність розшифрування;
* вручну за допомогою гістограм:
* описати і пояснити процес розшифрування.

1. В звіті описати послідовність дій, імена усіх використаних файлів, отримані гістограми, вказати визначені зміщення, описати процес розшифрування.
2. Викладачеві надається звіт про виконану роботу і усі використані та створені файли.

**Виконання завдання**

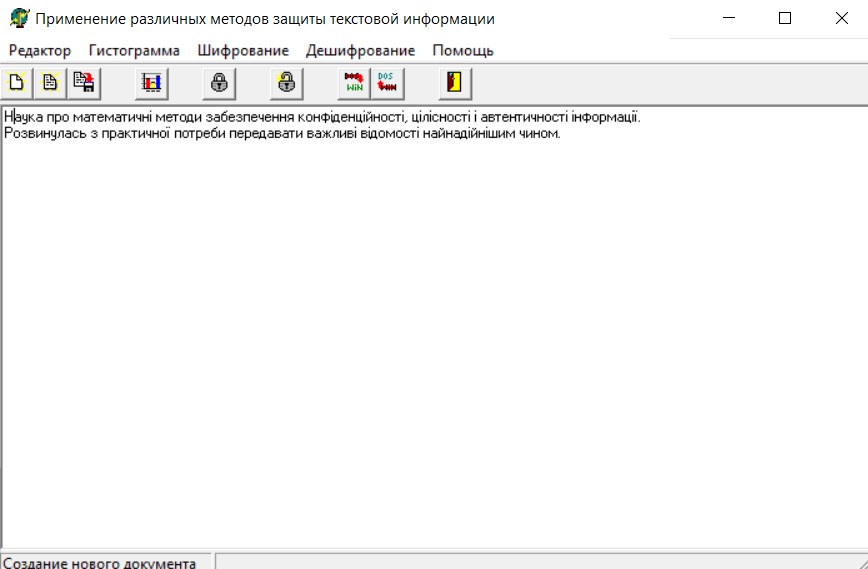
****

Рис. 1. Текст вхідного (не зашифрованого файлу)

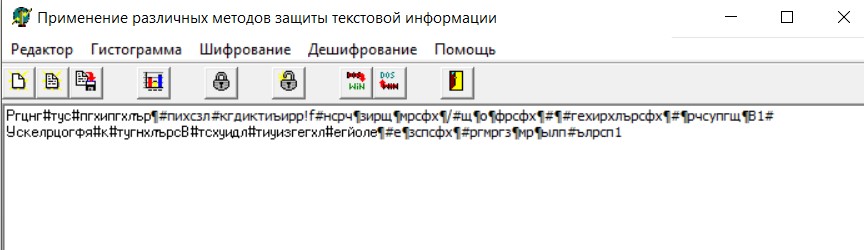


Рис. 2. Текст зашифрованого файлу

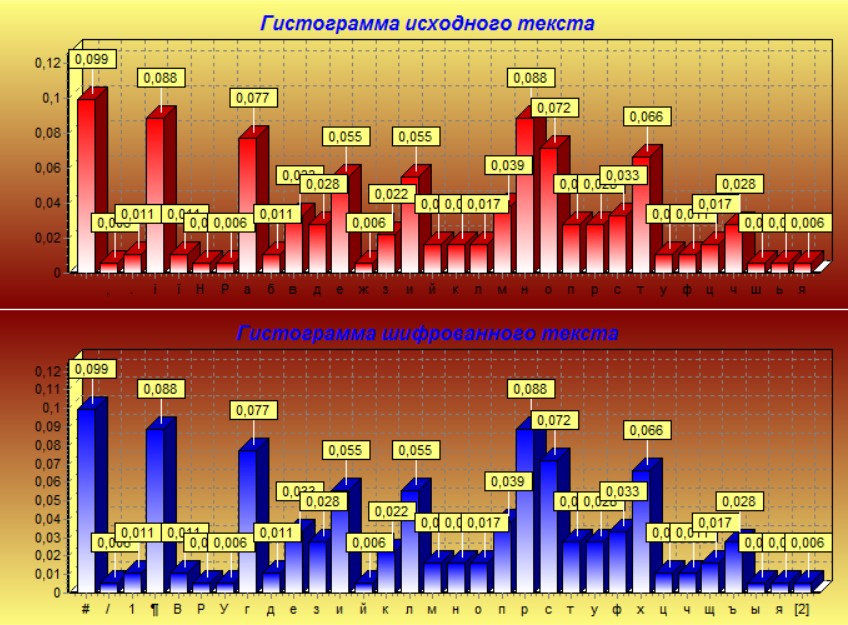


Рис. 3. Гістограма шифрування файлу

**Висновки:** під час виконання лабораторної роботи я ознайомилась із методом шифрування. Це одноалфавітний метод з фіксованим зміщенням який має досить зрозумілий алгоритм. У ході роботи мною детально була вивчена гістограма файлу, яка наведена на рис. 3, за допомогою якої я визначила зміщення шифрування яке виявилося рівним 3-ом.