МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

ІКТА

кафедра ЗІ



**З В І Т**

до лабораторної роботи №1

з курсу: «Основи крипографічного захисту інформації»

на тему: «Використання класичних криптоалгоритмів підстановки та перестановки для захисту текстової інформації»

Виконав: ст. гр. УІ-42

Симоненко Д.С.

Прийняв: Шандра З.А.

Львів – 2017

**Мета роботи:** навчитися використовувати класичні крипто алгоритми підстановки та перестановки для захисту текстової інформації.

Завдання

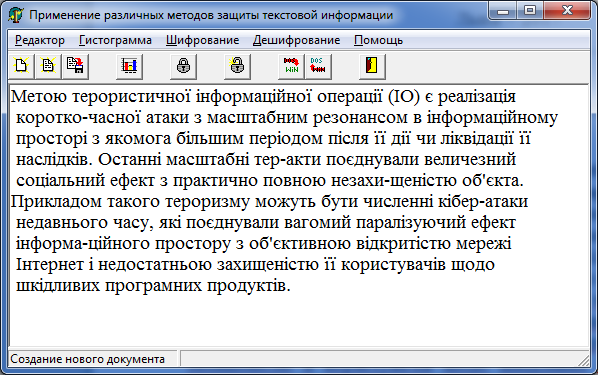
1. Для одноалфавітного методу з фіксованим зміщенням визначити встановленне в програмі зміщення. Для цього потрібно:

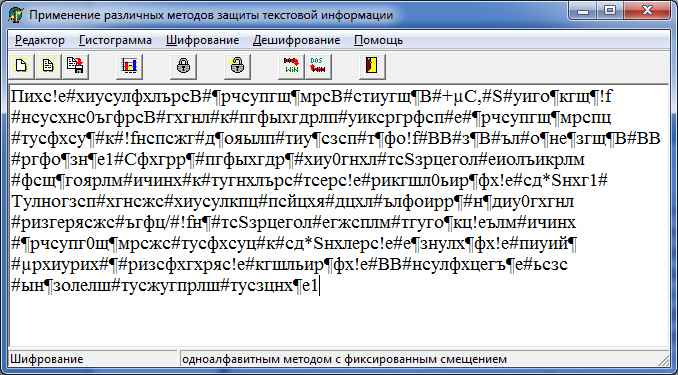
* переглянути попередньо створений за допомогою редактора свій текстовий файл;
* виконати для цього файлашифровання;
* переглянути в редакторі зашифрований файл;
* переглянути гистограми вихідного та зашифрованого текстів;
* описати гістограми (в чому подібні, в чому різняться) і визначити, з яким зміщенням 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.

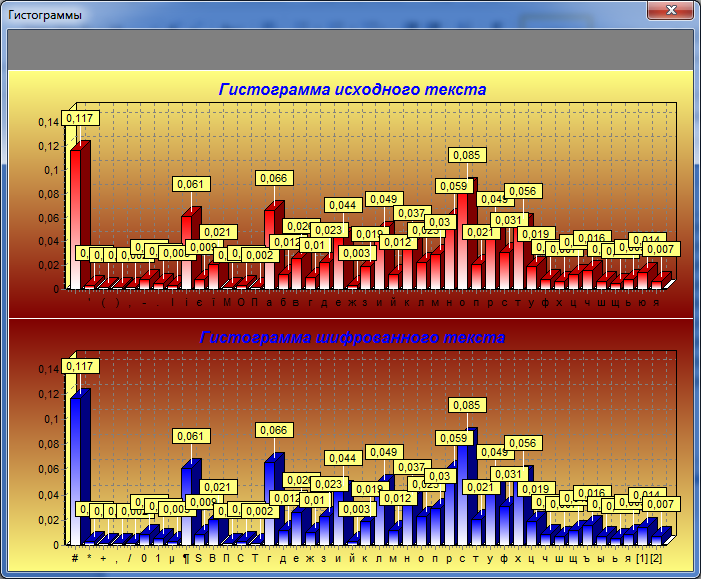
1. В звіті описати послідовність дій, імена усіх використаних файлів, отримані гістограми, вказати визначені зміщення, описати процес розшифрування.
2. Викладачеві надається звіт про виконану роботу і усі використані та створені файли.

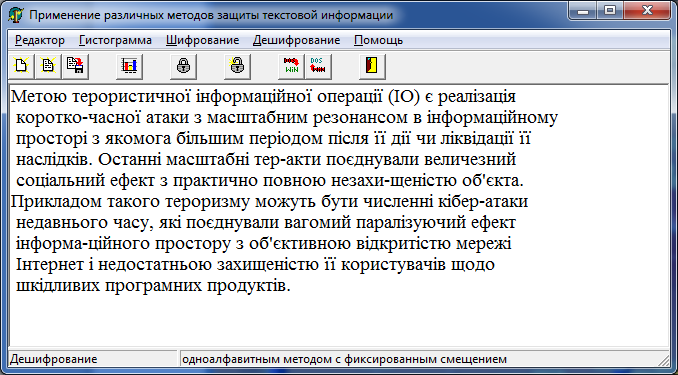
*Примітка.* Для виконання роботи потрібно запустити програму **L\_LUX.EXE**. Порядок роботи і теоретичні відомості з методів шифрування можна подивитися в пункті меню **Help.**

Виконання







Згідно гістограми ми отримали зміщення на 3 символи вправо.

**Висновок:** під час лабораторної роботи я навчився використовувати класичні криптоалгоритми підстановки та перестановки для захисту текстової інформації.