Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Факультет інформатики та обчислювальної техніки

Кафедра інформатики програмної інженерії

Основи захисту інформації

Лабораторна робота № 1

Тема: Прості шифри

**Виконав:**

Студент гр. ІТ-82

Фолькін Д. О.

**Перевірив:**

ст. вик. Ісаченко Г. В.

Оцінка:\_\_\_\_\_\_\_\_\_\_\_

(\_\_)\_\_\_\_\_\_\_\_\_\_2021

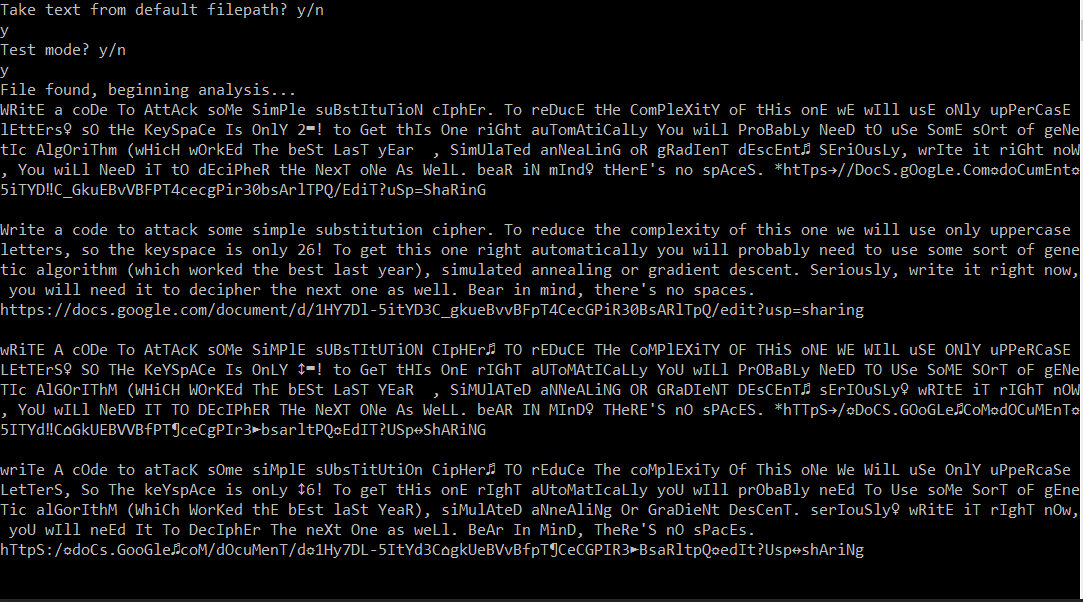
Київ – 2021

**Хід роботи**

У файлі був набір байтів у бінарному вигляді. За допомогою веб-калькулятора було отримано набір символів. Набір символів мав у кінці два «=», що є ознакою кодування based64. Після розкодування тексту засобами мови С# було отримано текст завдання.

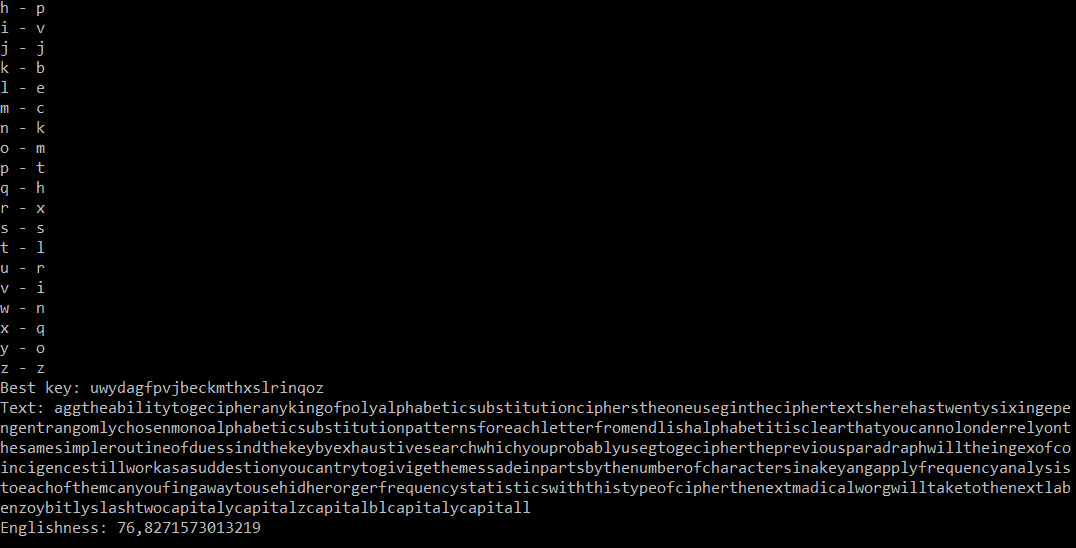
Перше завдання – шифр Цезаря із XOR. Для цього було створено програму на С#. Методом частотного аналізу було встановлено символ-зміщення і розшифровано текст.

Друге завдання – шифр Віженера. Програму було доповнено кількома методами для визначення довжини ключа та самого ключа за допомогою частотного аналізу. Після визначення ключа розшифрували текст:



Третє завдання – шифр підстановки. Програму було доповнено методами для підбору алфавіту заміни, за допомогою якого можна розшифрувати шифр. Використовувався генетичний алгоритм, хромосомами якого були алфавіти заміни, ними розшифровувався текст, для тексту рахувалася ознака схожості на природню мову. Це була сума різниць між частотами триграм у розшифрованому тексті та еталонними значеннями. Алфавіт заміни, що показував найменшу ознаку, вважався вдалим і розшифрований ним текст виводився на консоль.

Приклад роботи програми при розшифруванні шифру простої підстановки:



Даний текст можна розібрати і вручну виправити дрібні неточності.