Національний технічний університет України
«Київський політехнічний інститут»

Інститут Прикладного системного аналізу
Кафедра Системного проектування

Лабораторна робота № 1

з дисципліни «Безпека інформаційних систем»

«Дослідження шифрів підстановки »

Виконав:
студент групи ДА-82
факультету «ІПСА»
Муравльов А. Д.

Київ – 2020

Хід роботи

Завдання 1

Зашифрувати і дешифрувати вручну свої прізвище, ім'я та по батькові, написані великими літерами латинського алфавіту, за допомогою шифру Цезаря. Ключ K обчислюється за формулою K = (N + n + c) mod 26, де N - номер групи, n - номер студента за списком, c = 15 - константа.

Ключ K = (82 + 17 + 15) % 26 = 10

Вихідний алфавіт:
ABCDEFGHIJKLMNOPQRSTUVWXYZ
Зсунутий алфавіт:
KLMNOPQRSTUVWXYZABCDEFGHIJ

Вихідний текст:
MYRAVLYOVANDRIYDMYTROVYCH
Зашифрований текст:
WEBKFVYFKXNBSSNWIDBYFIMR

Завдання 2

Виконати шифрування і дешифрування шифром Цезаря свого прізвища, імені та по батькові, записаними великими літерами, а також малими і великими літерами латинського алфавіту за допомогою засобів пакету CrypTool. Зберегти отримані результати шифрування і дешифрування у відповідні файли за допомогою засобів пакету CrypTool. Порівняти результати ручного та автоматичного шифрування і дешифрування.

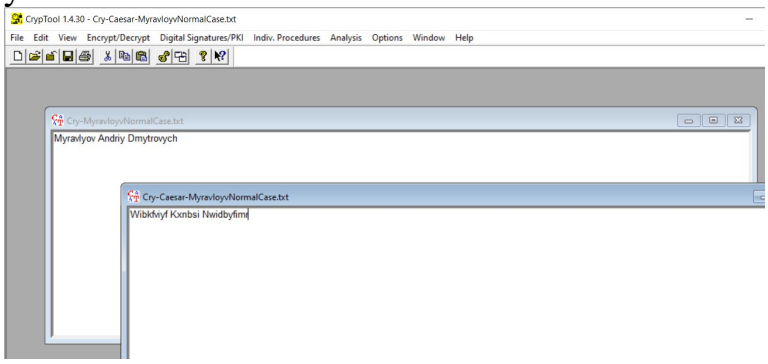


Рис. 1 Шифрування ПІБ

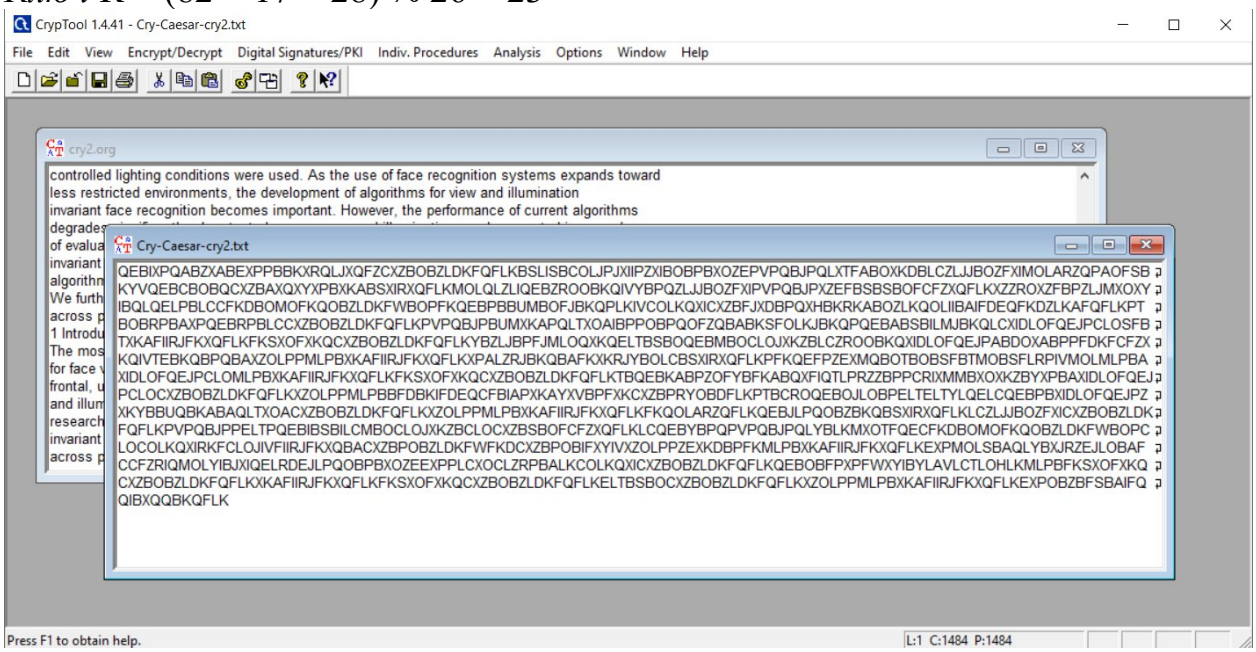
Бачимо, що отримано такий самий результат, як і при ручному шифруванні лише з тою різницею, що CrypTool зберіг великі літери та символи, що не входять до алфавіту.

Завдання 3

Обрати текстовий файл (див. Додаток до даної роботи) для шифрування шифром Цезаря. Зашифрувати файл і зберегти його як текстовий документ.

Файл з текстом обирається за номером варіанту, а ключ шифрування - (№ групи + № списку + день народження) % 26.

Ключ K = (82 + 17 + 28) % 26 = 23



Завдання 4

За допомогою засобів аналізу пакету CrypTool провести частотний аналіз початкового і зашифрованого тексту. Визначити ентропію і максимально можливу ентропію зашифрованого файлу, побудувати гістограму розподілу частоти символів в аналізованих файлах. Зробити висновки про можливість криптоаналізу зашифрованого тексту з використанням тільки шифротексту. Порівнявши гістограми, визначити ключ шифрування і застосувати його для дешифрування зашифрованого тексту. Порівняти початковий текст з дешифрованим. Зробити висновки.

На наступних скрішнотах зашифрований файл знаходиться зліва, вихідний – справа.

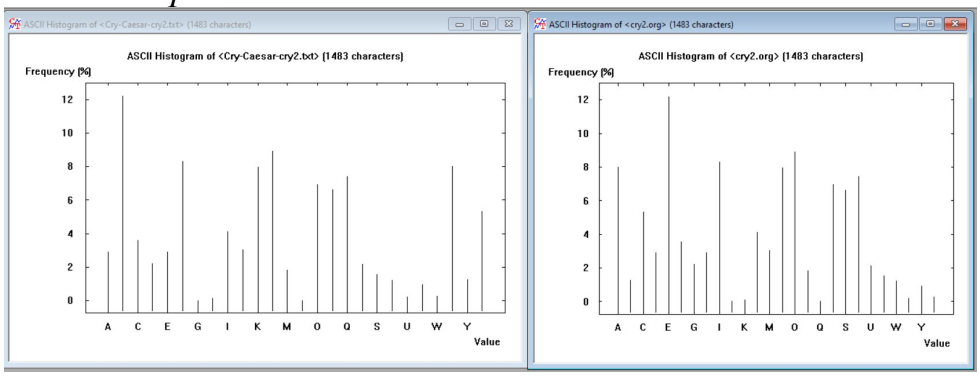


Рис.2 Гістограми розподілу частоти

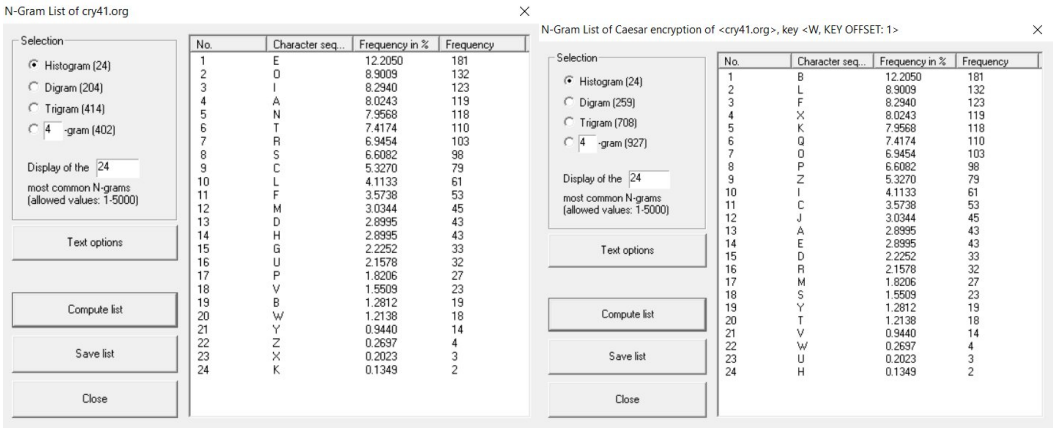


Рис. 3 Частотний аналіз

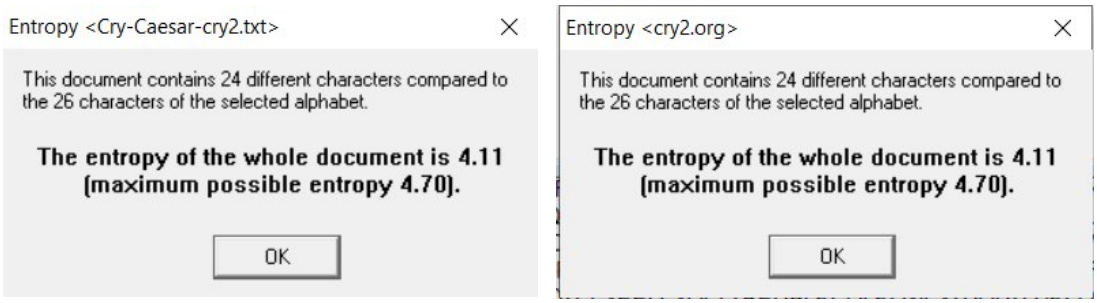


Рис. 4 Ентропія та максимальна ентропія

Виходячи з припущення, що вихідний текст містить лише букви англійського алфавіту, можемо легко віднайти ключ шифрування, знайшовши середньостатистичну гістрограму частот літер та порівнявши її з гістограмою зашифрованого тексту:

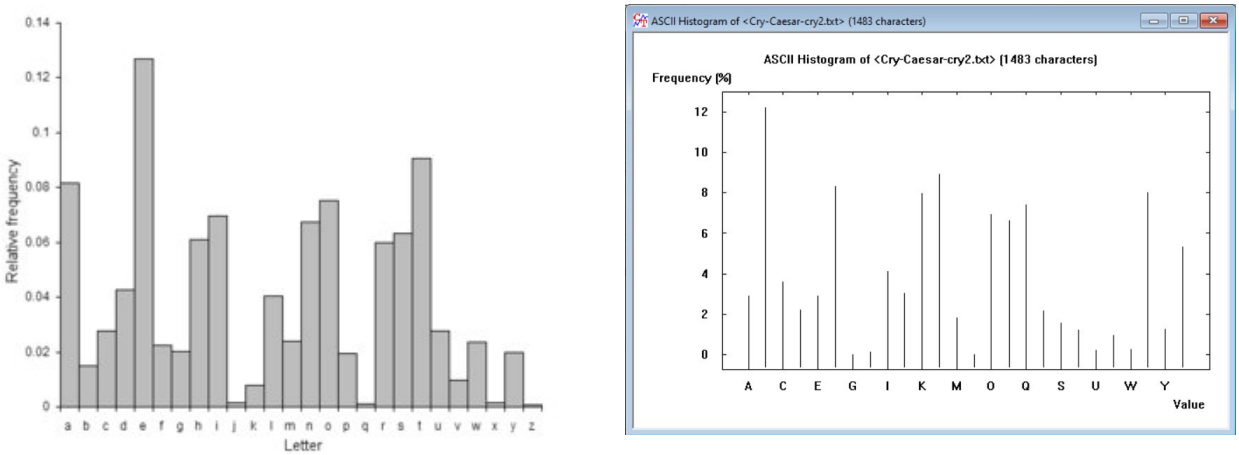


Рис. 5 Частоти літер англійського алфавіту

Бачимо, що частота літери B у зашифрованому тексті майже збігається з частотою літери E. Таким чином, зсув становить 26 – 3 = 23.

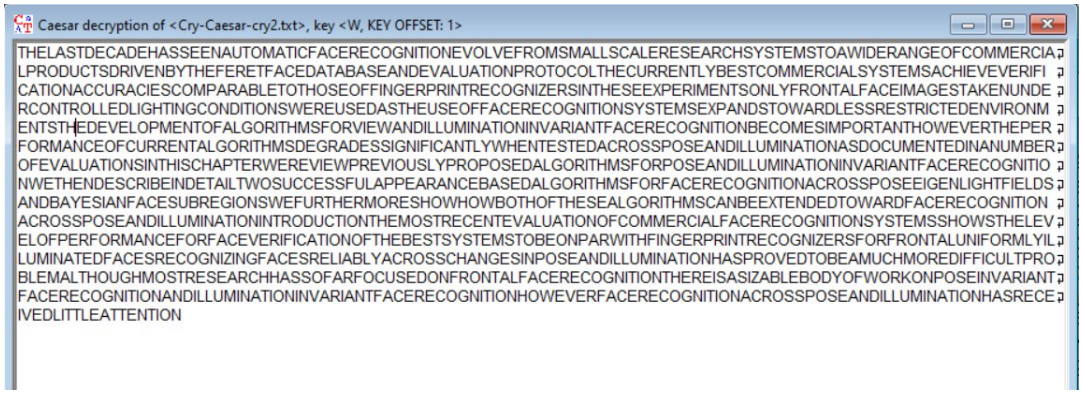


Рис.6 Дешифрований текст

Бачимо, що текст принаймні читаємий, але спеціальні символи(новий рядок, пробіл) не збережено, а також всі літери стали великими.

Завдання 5

Виконати шифрування і дешифрування файлу, обраного відповідно до п.3, використовуючи алгоритм Rot-13. Зберегти результати.

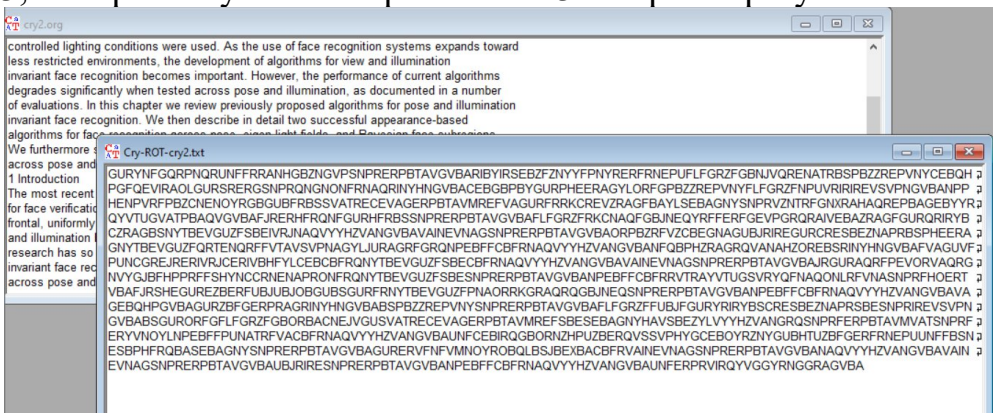


Рис. 7 Зашифрований та дешифрований текст алгоритмом Rot-13

Завдання 6

Вибрати зашифрований файл з додатку до лабораторної роботи, що відповідає номеру варіанта. Використовуючи можливості пакета CrypTool, дешифрувати файл. Результати дешифрування і всі проміжні результати зберегти, провести аналіз отриманих даних.

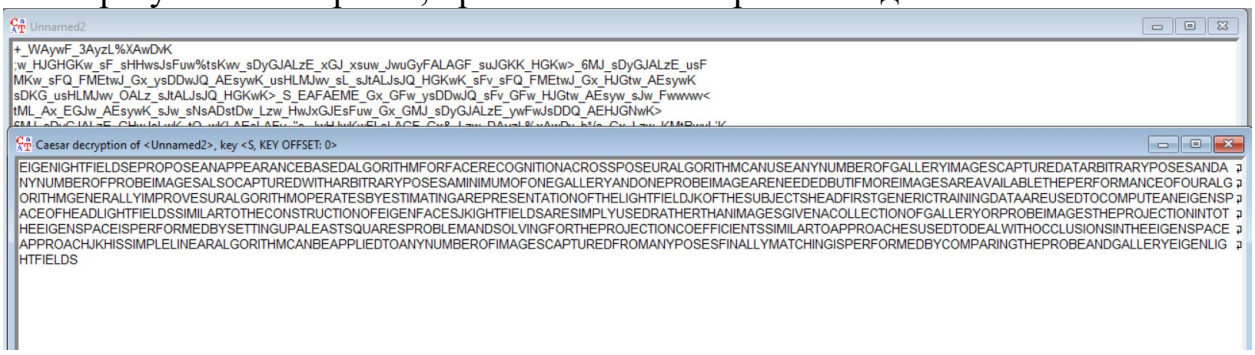


Рис. 8 Зашифрований та дешифрований текст

Користуючись підходом, описаним у завданні 4 та порівнявши гістограми розподілу літер у англійській мові та в заданому тексті, можемо визначити ключ K, що дорівнює 18 та розшифрувати текст. Для шифрування було використано шифр Цезаря.

Завдання 7

Виконати шифрування і дешифрування файлу, обраного відповідно до п.3, використовуючи алгоритм Віженера і ключове слово у вигляді прізвища студента, за допомогою пакета CrypTool. Дослідити можливості пакета CrypTool для злому шифру Віженера.

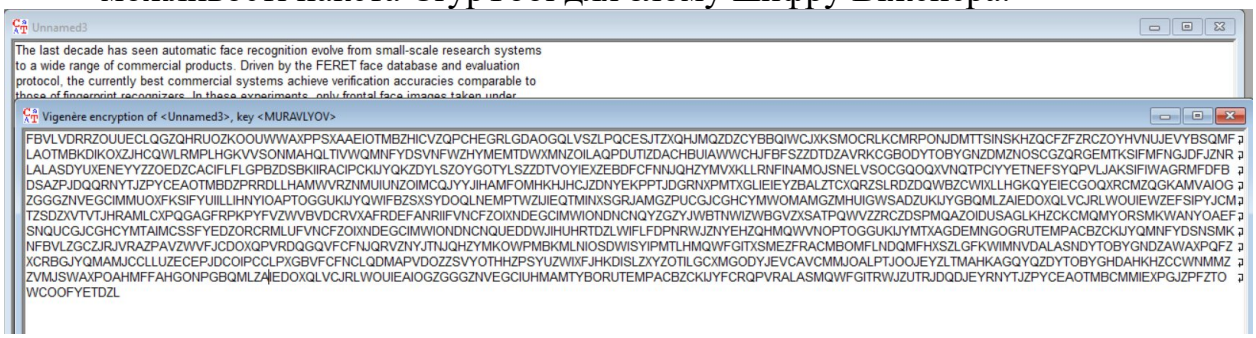


Рис. 9 Зашифрований та оригінальний тексти

Проаналізувати шифр Віженера можна з використанням пакету Cryptool, відкривши відповідне меню:

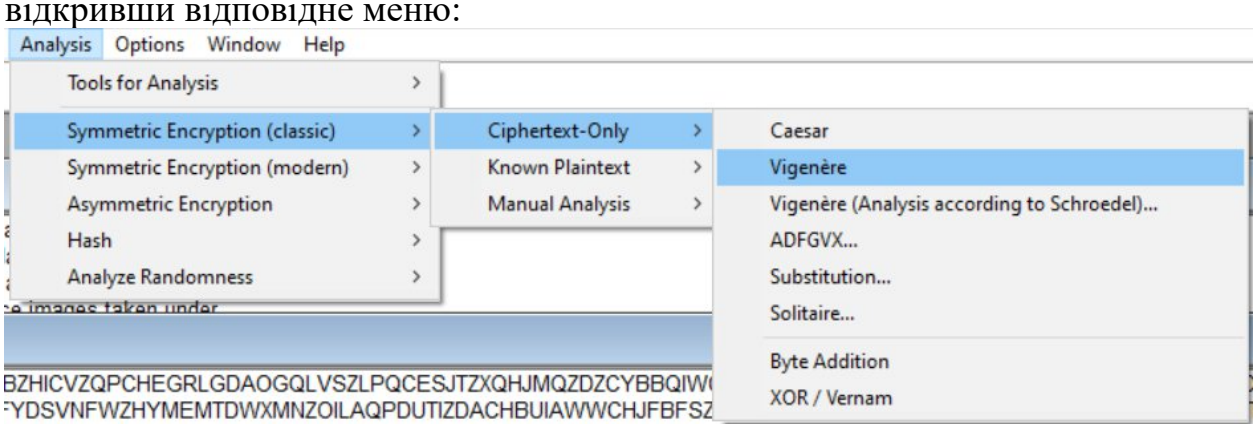


Рис. 10 Меню аналізу шифру Віженера в Cryptool

Пакет здатен автоматично віднайти ключ та його довжину.

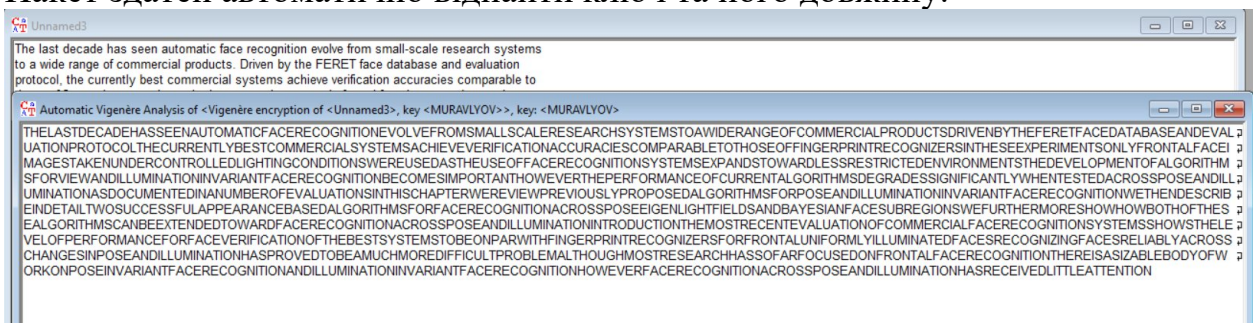


Рис. 11 Розшифрований та оригінальний тексти

Завдання 8

Написати програму для шифрування і дешифрування файлів за допомогою шифру Віженера. Зашифрувати файл, вибраний з додатка до лабораторної роботи згідно свого варіанту, за допомогою розробленої програми. Порівняти результати шифрування, отримані за допомогою пакета CrypTool, з результатами роботи власної програми. Зробити висновки про коректність роботи програми.

Вихідний код та результати роботи програми:

vigenere.py:

```
def vigenere(txt='', key='', typ='d'):
    if not txt:
        print('Needs text')
        return
    if not key:
        print('Needs key')
        return
    if typ not in ('d', 'e'):
        print('Type must be "d" or "e"')
        return

    k_len = len(key)
    k_ints = [ord(i) for i in key]
    txt_ints = [ord(i) for i in txt]
    ret_txt = ''
    for i in range(len(txt_ints)):
        adder = k_ints[i % k_len]
        if typ == 'd':
            adder *= -1

        v = (txt_ints[i] - 32 + adder) % 95

        ret_txt += chr(v + 32)
    return ret_txt
```

main.py:

```
from vigenere import vigenere

q = vigenere('hello world!', 'key', 'e')
print(q)
print(vigenere(q, 'key', 'd'))
```

```
tk'xu:$u-xj;
hello world!
```

Код працює більш ефективно, оскільки враховує регістр букв та взагалі не обмежений латинським алфавітом, оскільки здатен успішно кодувати навіть пунктуаційні знаки.

Завдання 9

Написати програму для злому шифру Віженера з використанням атаки Беббіджа. За допомогою розробленої програми відновити зашифрований файл, отриманий при виконанні шифрування Віженера своєю програмою.

Зашифруємо файл у програмі CrypTool та збережемо у файл hostiletext.txt:

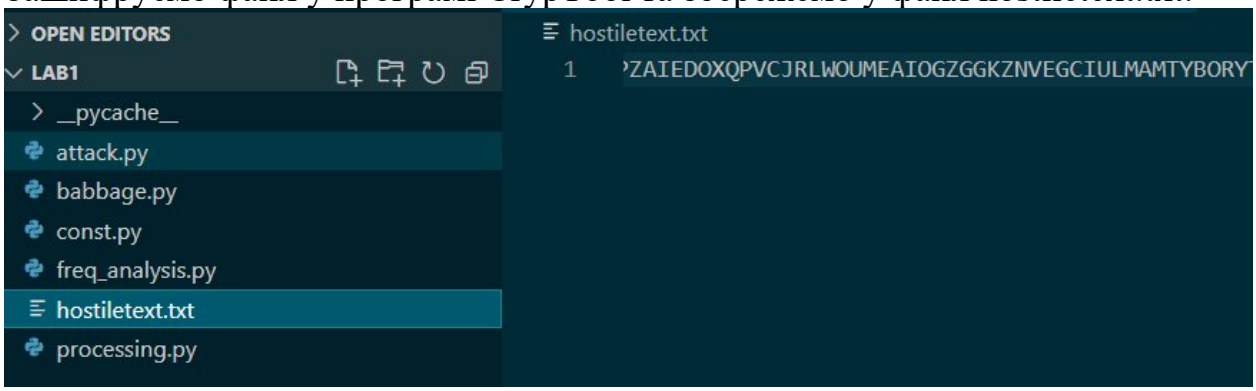


Рис.12 Структура проекту

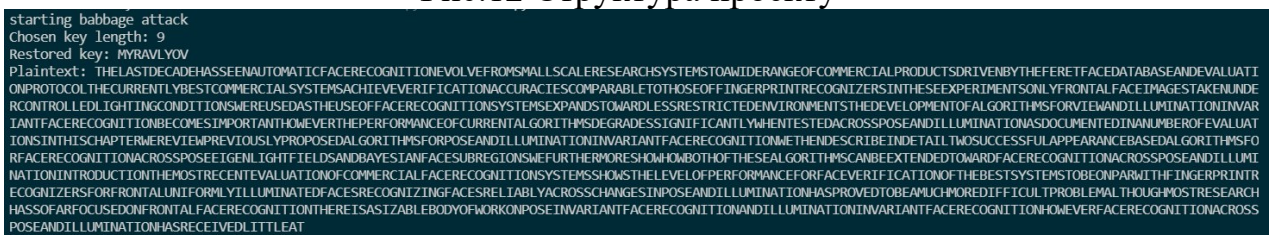


Рис. 13 Результат роботи програми

Програма розшифрувала заданий шифр аналогічно до результату, отриманого програмою CrypTool.

Висновки

В ході роботи я ознайомився з основними принципами роботи моно- та поліалфавітних шифрів, зокрема шифрами Цезаря та Віженера, навчився проводити їх аналіз та злом. Обидва шифри досить прості для зламу та не потребують значних обчислювальних потужностей для обчислення ключа, що робить їх не актуальними на наш час.