**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**

**«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ СІКОРСЬКОГО»**

**Інститут прикладного системного аналізу**

**Кафедра системного проектування**

Лабораторна робота №1

з дисципліни

“Безпека інформаційних систем”

Виконав:

студент групи ДА-81

Дєрюгін Єгор Олександрович

Київ – 2020Результати ручного шифрування і дешифрування ПІБ шифром Цезаря.

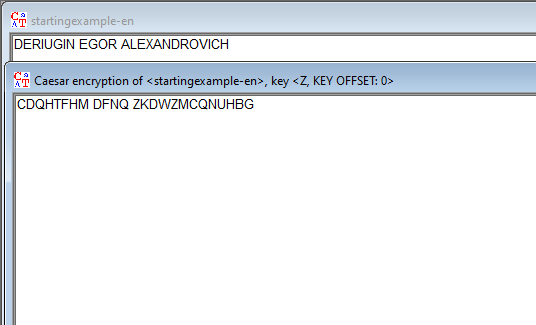
K = (N + n + c) mod 26 = (81 + 7 + 15) mod 26 = 25

DERIUGIN EGOR ALEXANDROVICH ->

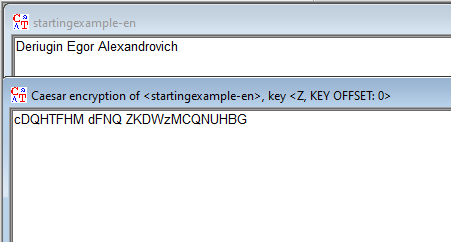
CDQHTFHM DFNQ ZKDWZMCQNUHBG

A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z -> Z, A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y

1. Кодування шифром Цезаря за допомогою CrypTool (uppercase)



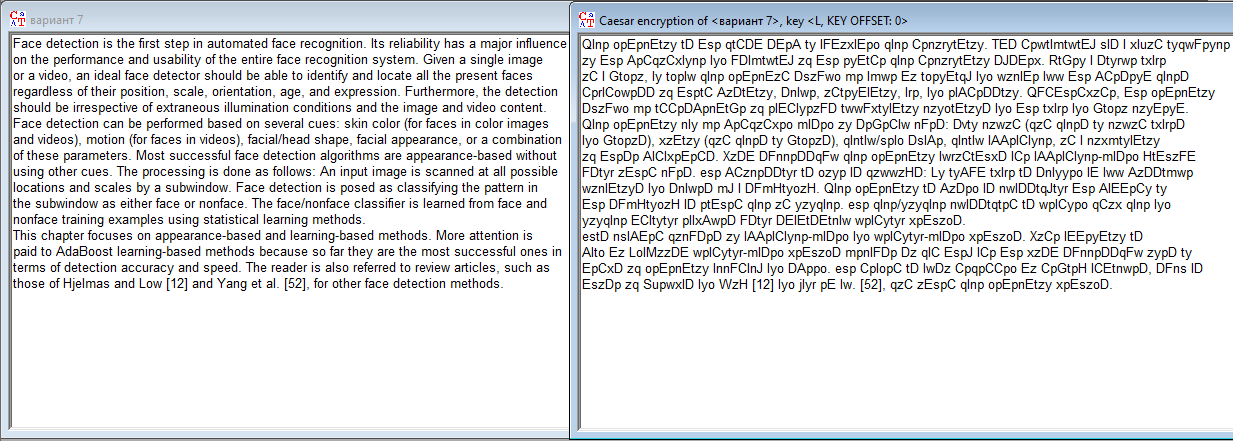
Кодування шифром Цезаря за допомогою CrypTool (різного регістру)

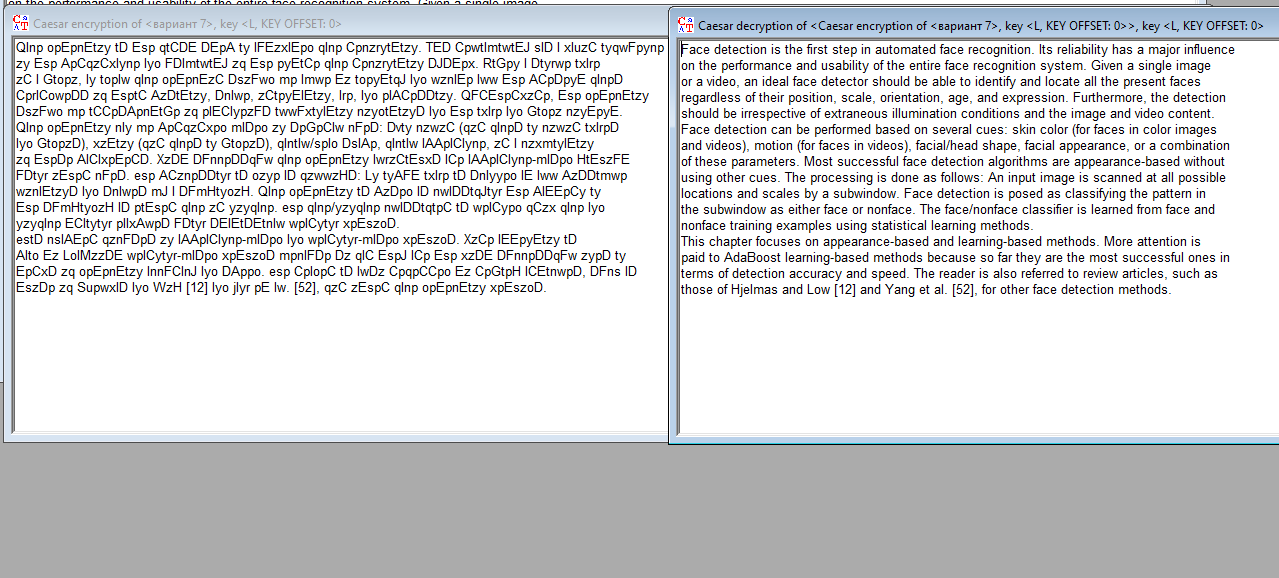


1. Результати шифрування і дешифрування текстового файлу шифром Цезаря з використанням пакету CrypTool, ентропія і максимально можлива ентропія, гістограма розподілу частоти символів.

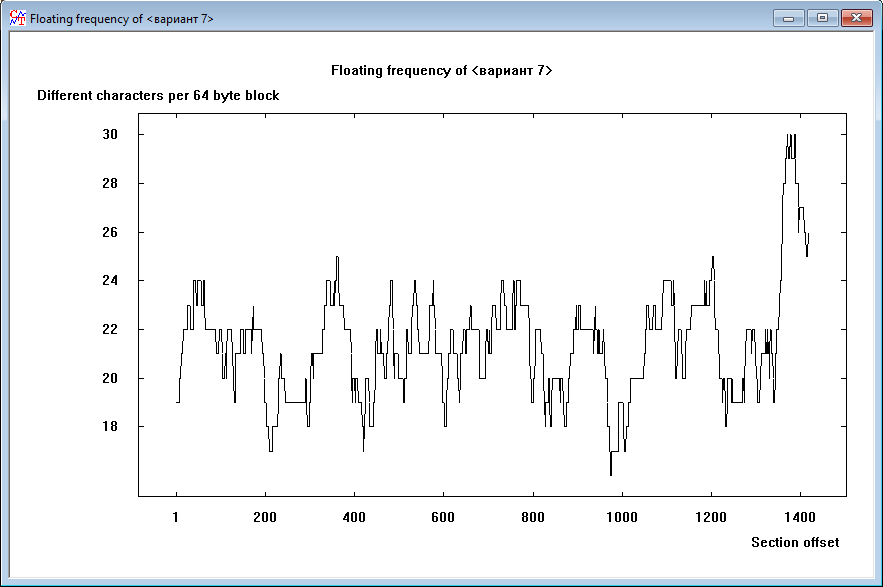
K = (N + n + c) mod 26 = (81 + 7 + 27) mod 26 = 11

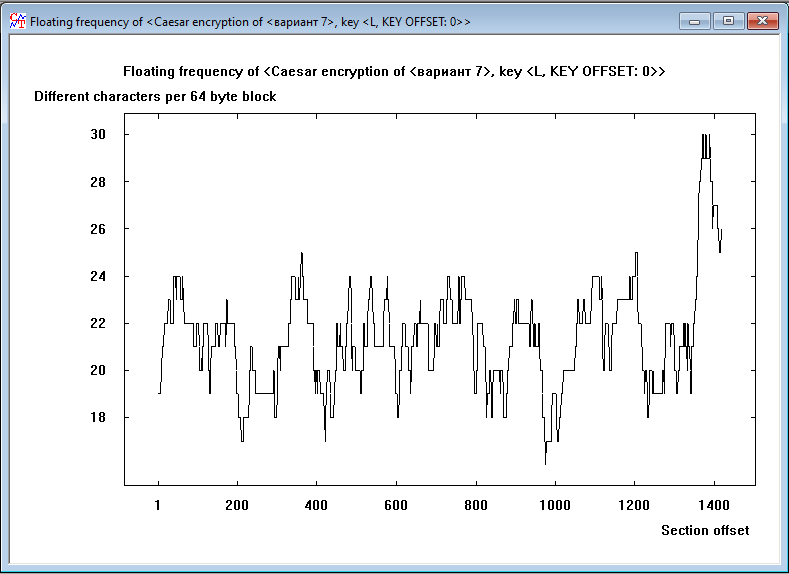
Шифрування:



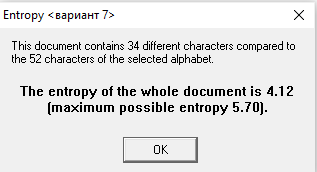
Дешифрування

Аналіз початкового та зашифрованого тексту

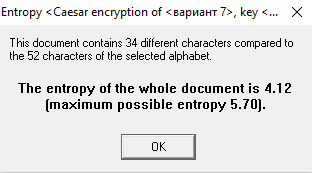
 Частотний аналіз початкового тексту:

Частотний аналіз зашифрованого тексту:

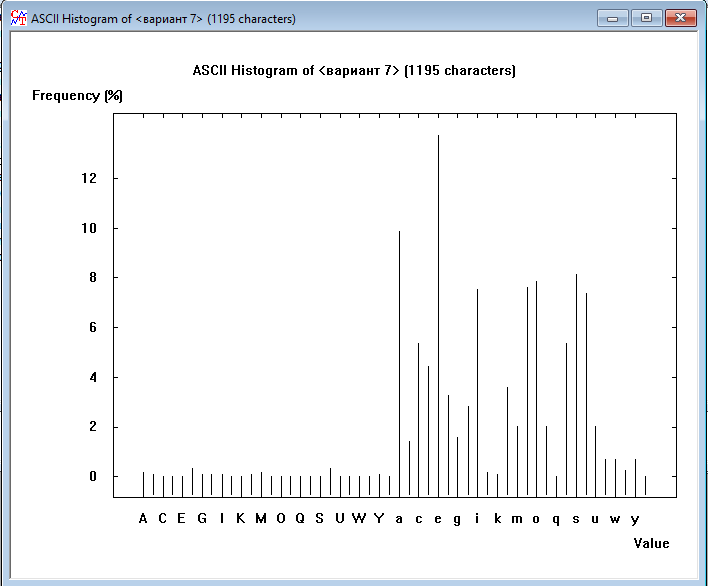
Ентропія початкового тексту:



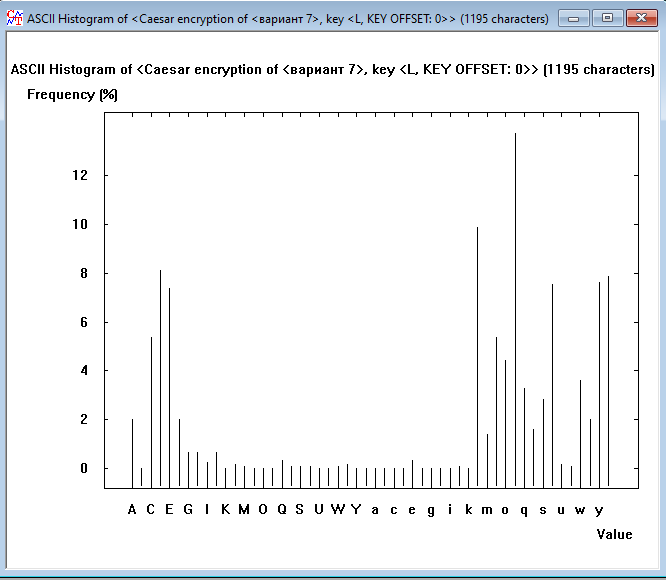
Ентропія зашифрованого тексту:



Гістограма розподілу частоти початкового тексту:

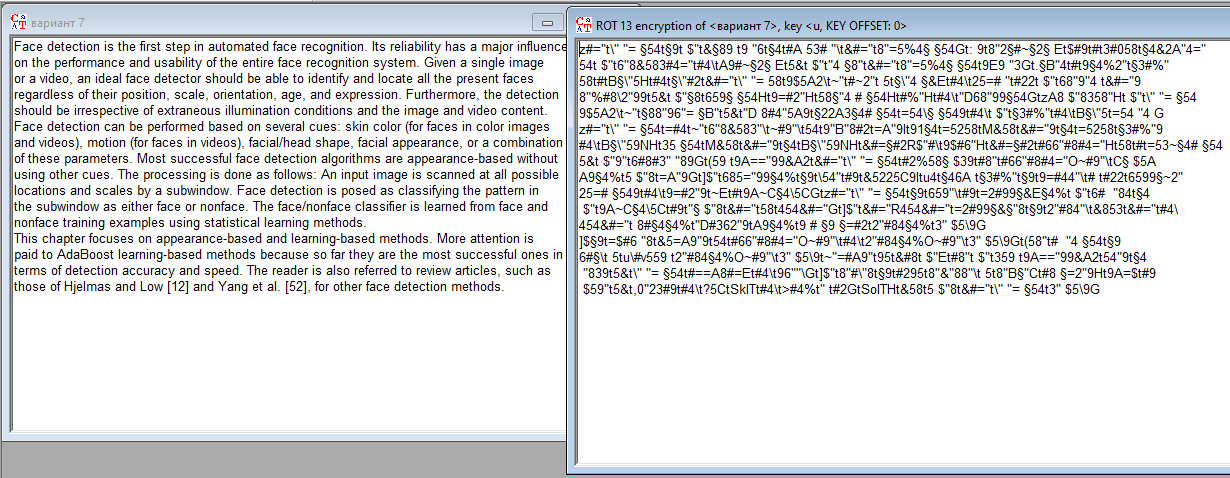


Гістограма розподілу частоти зашифрованого тексту:

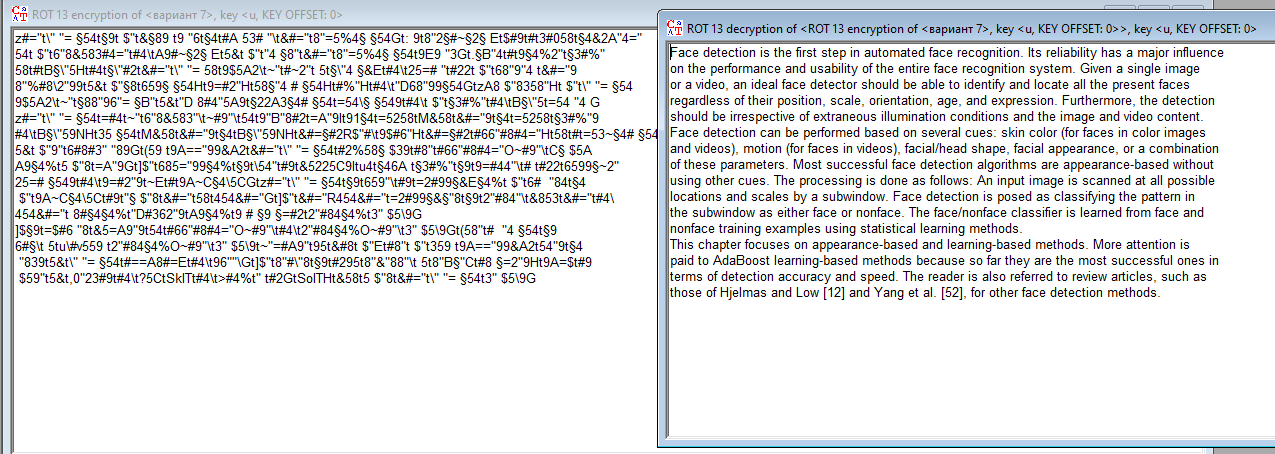


1. Результати шифрування і дешифрування текстового файлу шифром Rot-13 з використанням пакета CrypTool.

Шифрування:



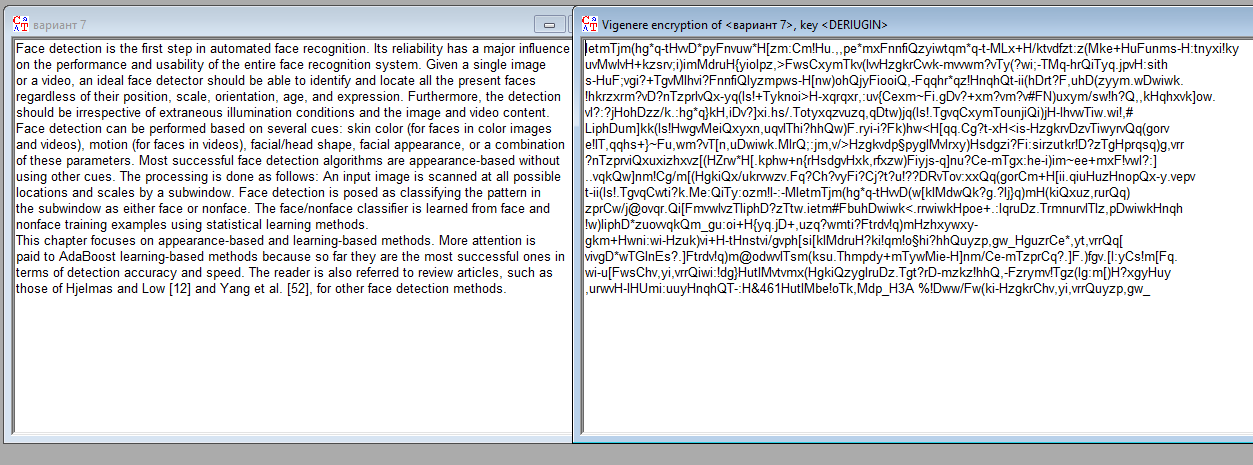
Дешифрування:



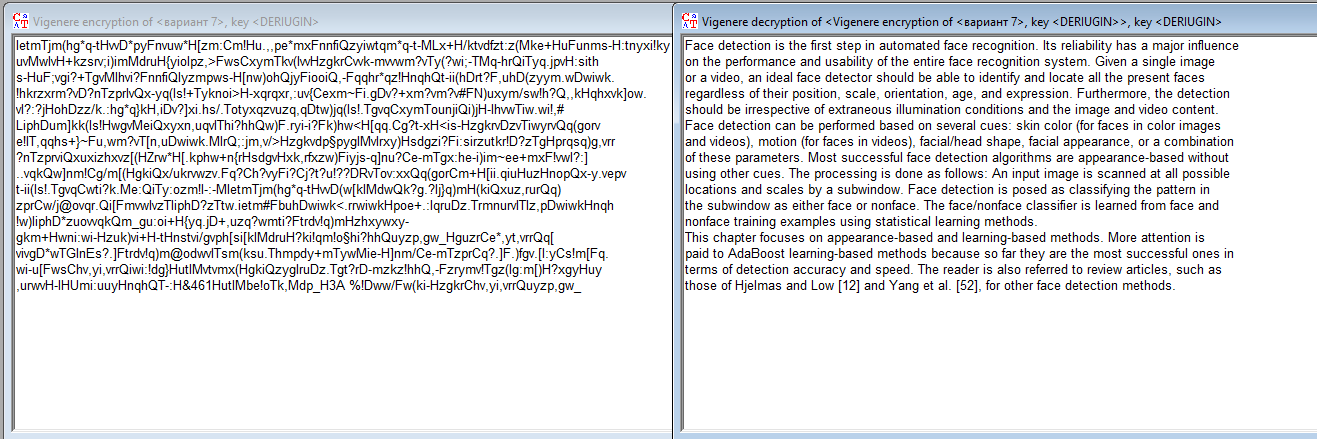
1. Результати шифрування і дешифрування текстового файлу шифром Віженера з використанням пакета CrypTool.

Ключ: DERIUGIN

Шифрування:



Дешифрування:



Висновки:

У ході виконання лабораторної роботи я вивчив шифри Цезаря, Rot-13, Віженера та атаку Бебіджа (Касіски). Вивчив можливості програми CrypTool, та виконав за її допомогою шифрування/дешифрування тексту згідно із завданням.