**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**

**«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ СІКОРСЬКОГО»**

**Інститут прикладного системного аналізу**

**Кафедра системного проектування**

Лабораторна робота №1

з дисципліни

“Безпека інформаційних систем”

Виконала:

студентка групи ДА-81

Желєзнова Валерія

Київ – 2020

1. Результати ручного шифрування і дешифрування ПІБ шифром Цезаря.

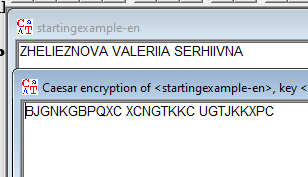
K = (N + n + c) mod 26 = (81 + 10 + 15) mod 26 = 2

ZHELIEZNOVA VALERIIA SERHIIVNA ->

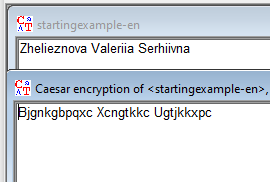
BJGNKGBPQXC XCNGTKKC UGTJKKXPC

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

1. Кодування шифром Цезаря за допомогою CrypTool (uppercase)

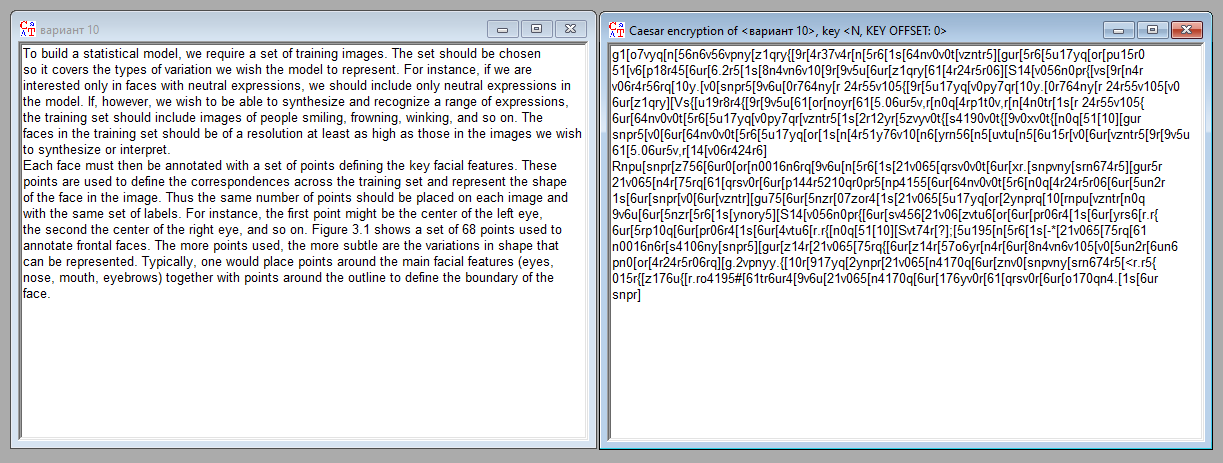


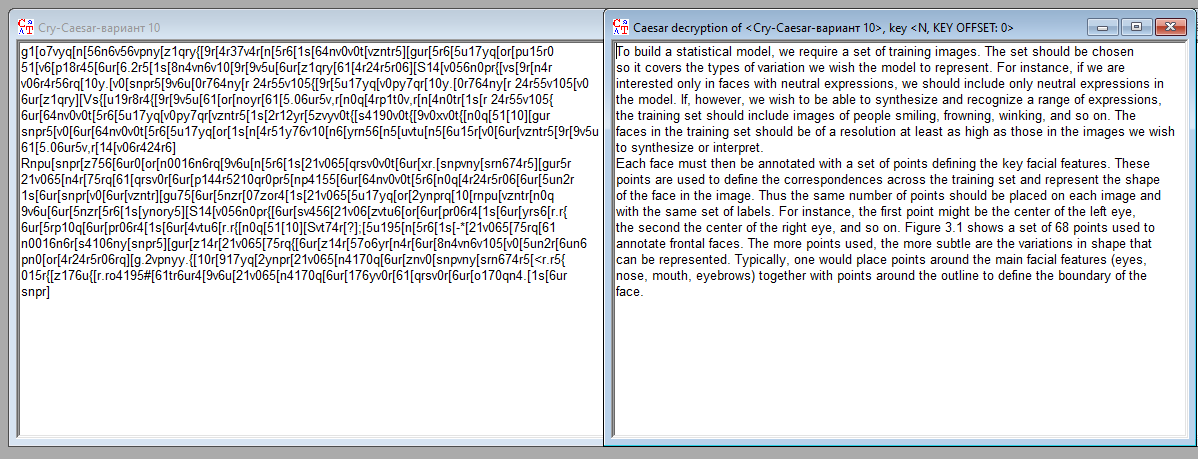
Кодування шифром Цезаря за допомогою CrypTool (різного регістру)



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

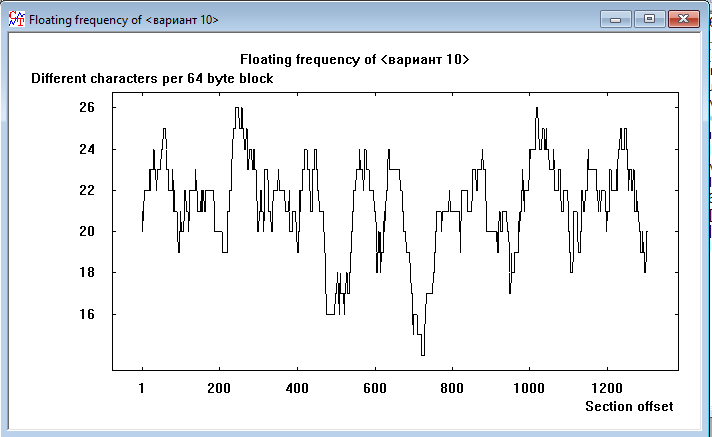
K = (N + n + c) mod 26 = (81 + 10 + 26) mod 26 = 13

Дешифрування:

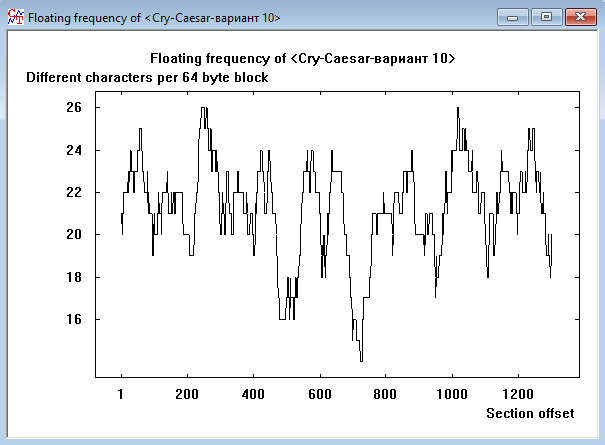


Аналіз початкового та зашифрованого тексту

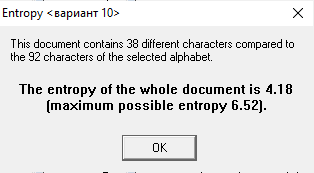
Частотний аналіз початкового тексту:



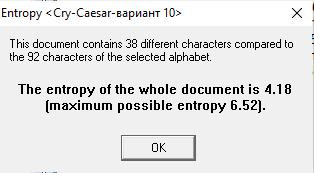
Частотний аналіз зашифрованого тексту:



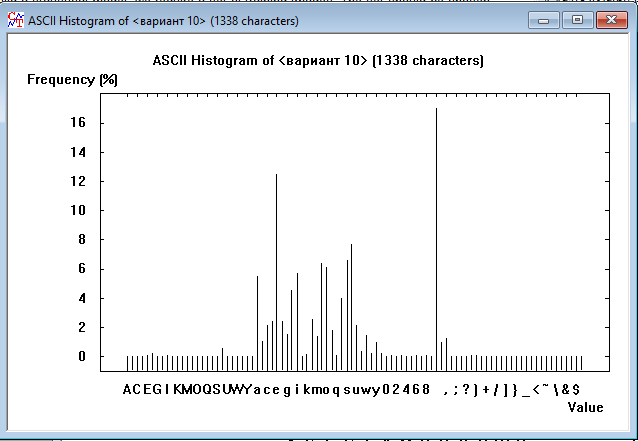
Ентропія початкового тексту:



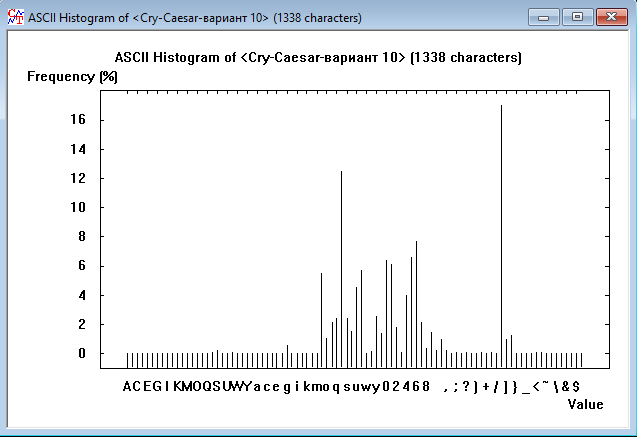
Ентропія зашифрованого тексту:



Гістограма розподілу частоти початкового тексту:

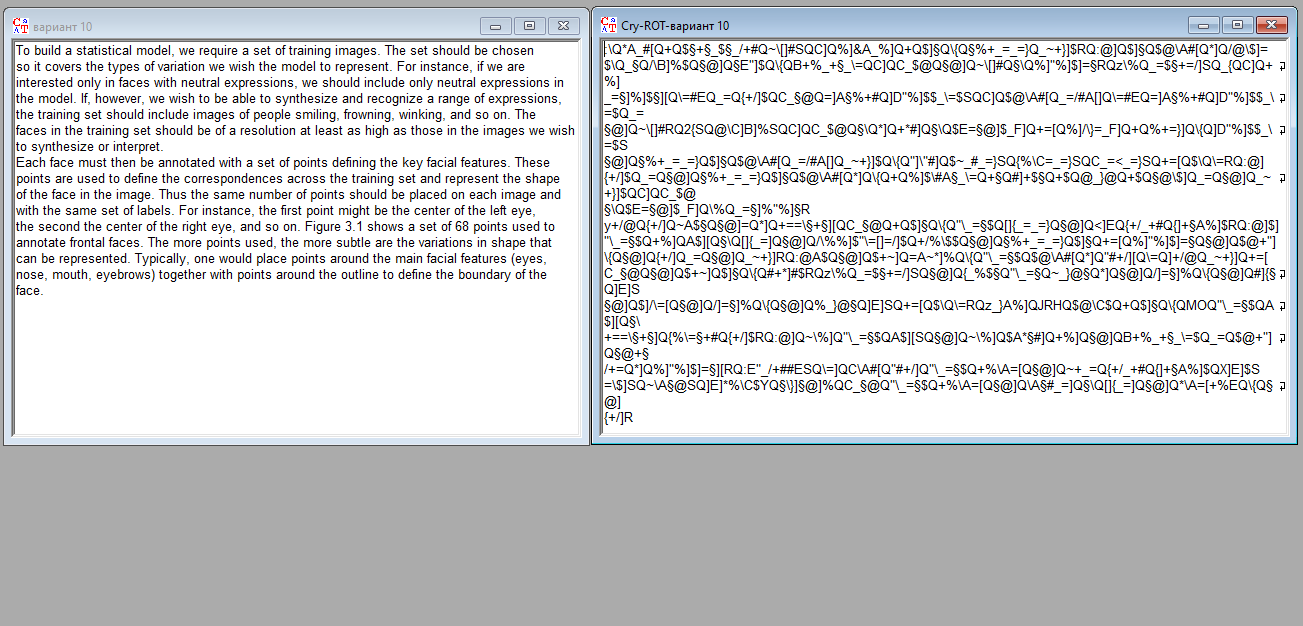


Гістограма розподілу частоти зашифрованого тексту:

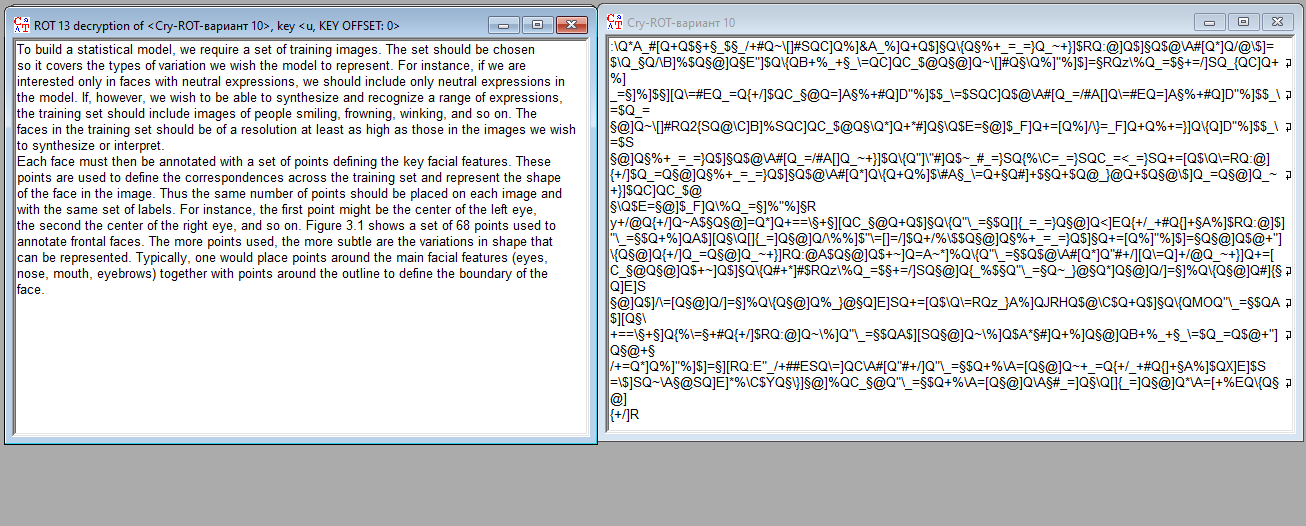


1. Результати шифрування і дешифрування текстового файлу шифром Rot-13 з використанням пакета CrypTool.

Шифрування:



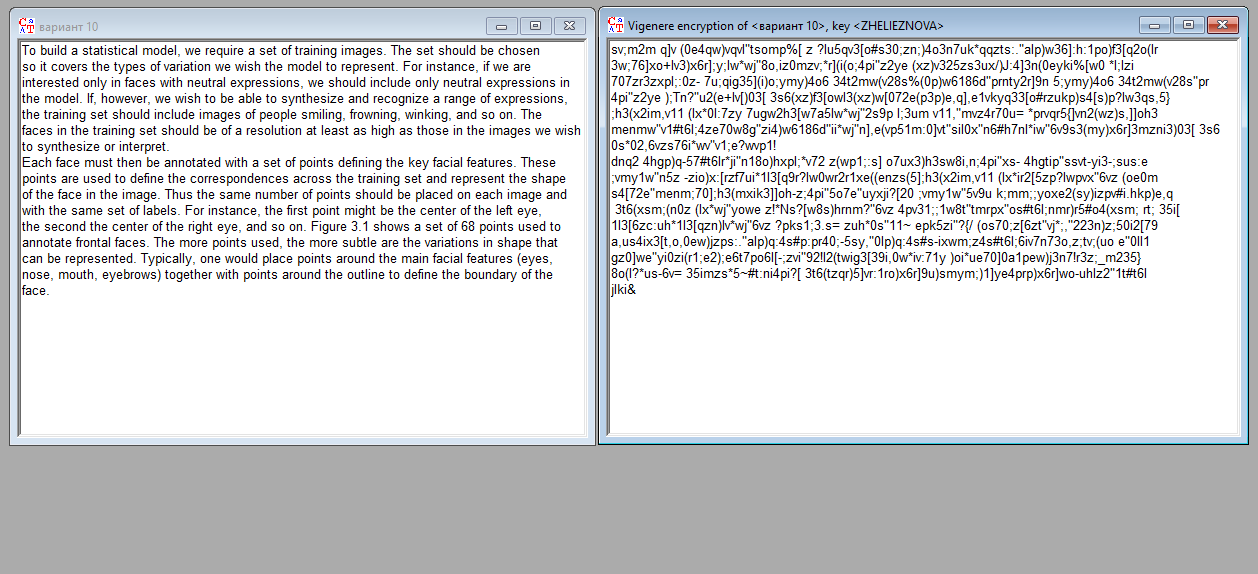
Дешифрування:



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

Ключ: ZHELIEZNOVA

Шифрування:



Дешифрування:

