**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**

**«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ СІКОРСЬКОГО»**

**Інститут прикладного системного аналізу**

**Кафедра системного проектування**

Лабораторна робота №2

з дисципліни

“Безпека інформаційних систем”

Виконала:

студентка групи ДА-81

Желєзнова Валерія

# Київ – 2020Мета роботи

Дослідження алгоритмів симетричного шифрування і дешифрування даних з використанням шифрів DES (ECB), DES (CBC), TripleDES (ECB), TripleDES (CBC), AES за допомогою програмних засобів CrypTool та їх практична реалізація.

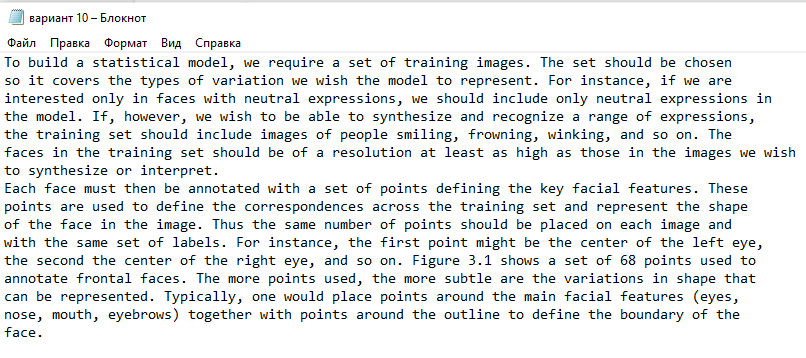
Завдання

1. Обрати текстовий файл (див. Додаток до даної роботи) відповідно до порядкового номеру студента в списку академічної групи в таблиці
2. Сформувати ключ для шифрування і дешифрування файлу відповідно до вимог для кожного шифру (DES (ECB), DES (CBC), TripleDES (ECB), TripleDES (CBC), AES), використовуючи при цьому своє прізвище, ім’я та по батькові, задані кирилицею в кодовій таблиці Windows 1251.
3. За допомогою засобів пакету CrypTool провести шифрування і дешифрування обраного файлу з використанням алгоритмів DES (ECB), DES (CBC), TripleDES (ECB), TripleDES (CBC), AES. Результати шифрування зберегти. За допомогою засобів аналізу пакета CrypTool визначити ентропію і максимально можливу ентропію зашифрованих файлів, а також побудувати гістограми розподілу частот символів у файлах, які було проаналізовано. Результати зберегти. Зробити висновки про можливість криптоаналізу зашифрованого тексту з використанням статистичних методів криптоаналізу.
4. За допомогою засобів аналізу пакету CrypTool оцінити час, необхідний для розшифрування зашифрованих файлів, отриманих при виконанні п.3, методом «грубої сили». Результати зберегти.
5. За допомогою засобів аналізу пакету CrypTool дослідити залежність тривалості «взлому» шифрів, що досліджуються, від довжини ключа. Для цього необхідно виконати криптоаналіз зашифрованих файлів при зменшеній довжині ключа, вважаючи, що частина символів ключа є відомими. Це дозволяє зменшити простір підбору ключів і, як результат, зменшити час виконання криптоанализу. Результати зберегти і проаналізувати. Написати програму для шифрування і дешифрування файлів за допомогою шифрів DES (ECB) і TripleDES (ECB). При розробці програми можна скористатися можливостями простору імен System.Security.Cryptography в середовищі .NET Security Framework, або будь-яку бібліотеку для роботи з комп’ютерною криптографією.
6. Зашифрувати файл, обраний із додатка до лабораторної роботи відповідно до свого варіанту за допомогою розробленої програми. Порівняти результати шифрування, отримані за допомогою пакету CrypTool, з результатами роботи власної програми. Зробити висновки щодо коректності роботи програми.
7. Дешифрувати файли п.8 за допомогою своєї програми.
8. Оформити звіт по роботі.

**Варіант 10**

Хід роботи

Текст за варіантом 10



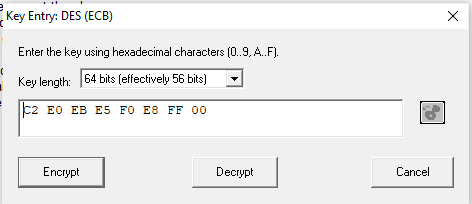
Ключі в Windows – 1251

Железнова – C6 E5 EB E5 E7 ED EE E2 E0

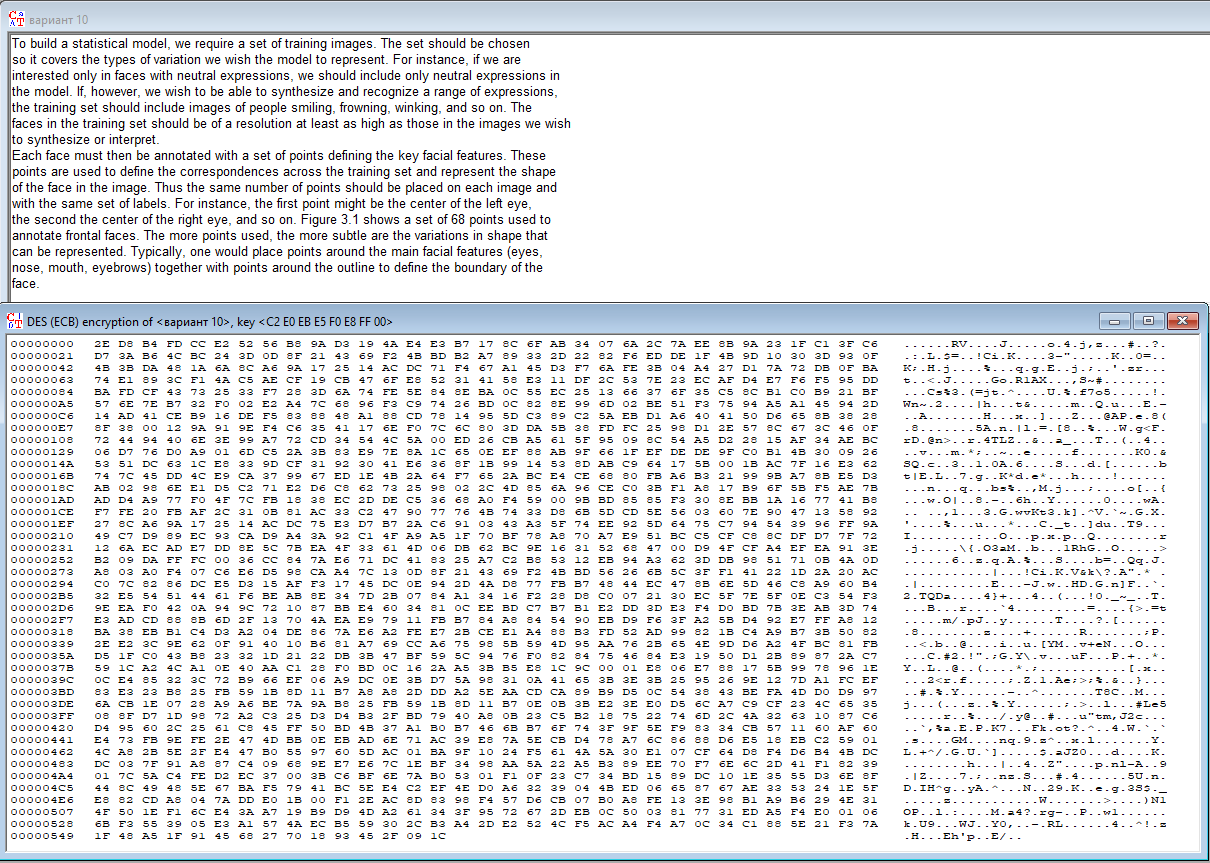
Валерия – C2 E0 EB E5 F0 E8 FF

Сергеевна - D1 E5 F0 E3 E5 E5 E2 ED E0

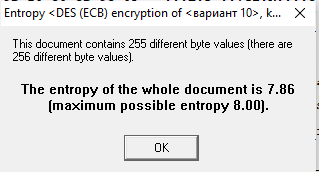
За допомогою CrypTool проводимо DES(ECB) шифрування



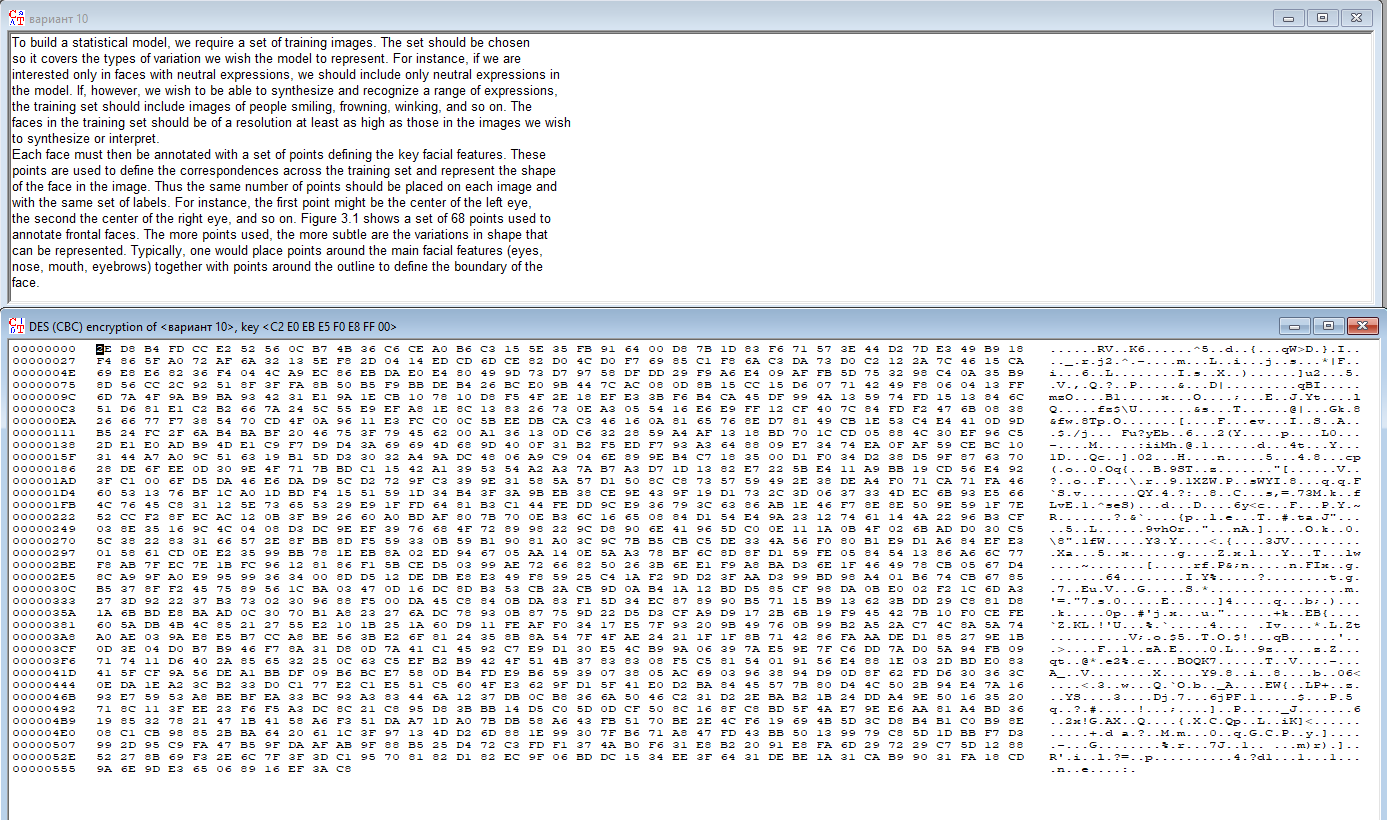
Результат:



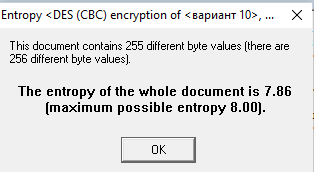
Ентропія та максимальна можлива ентропія в зашифрованому файлі DES (ECB)



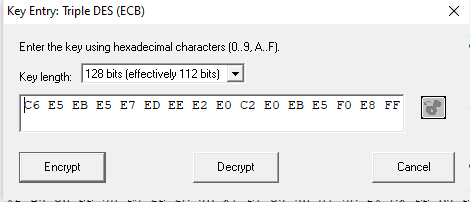
За допомогою CrypTool проводимо DES(CBC) шифрування

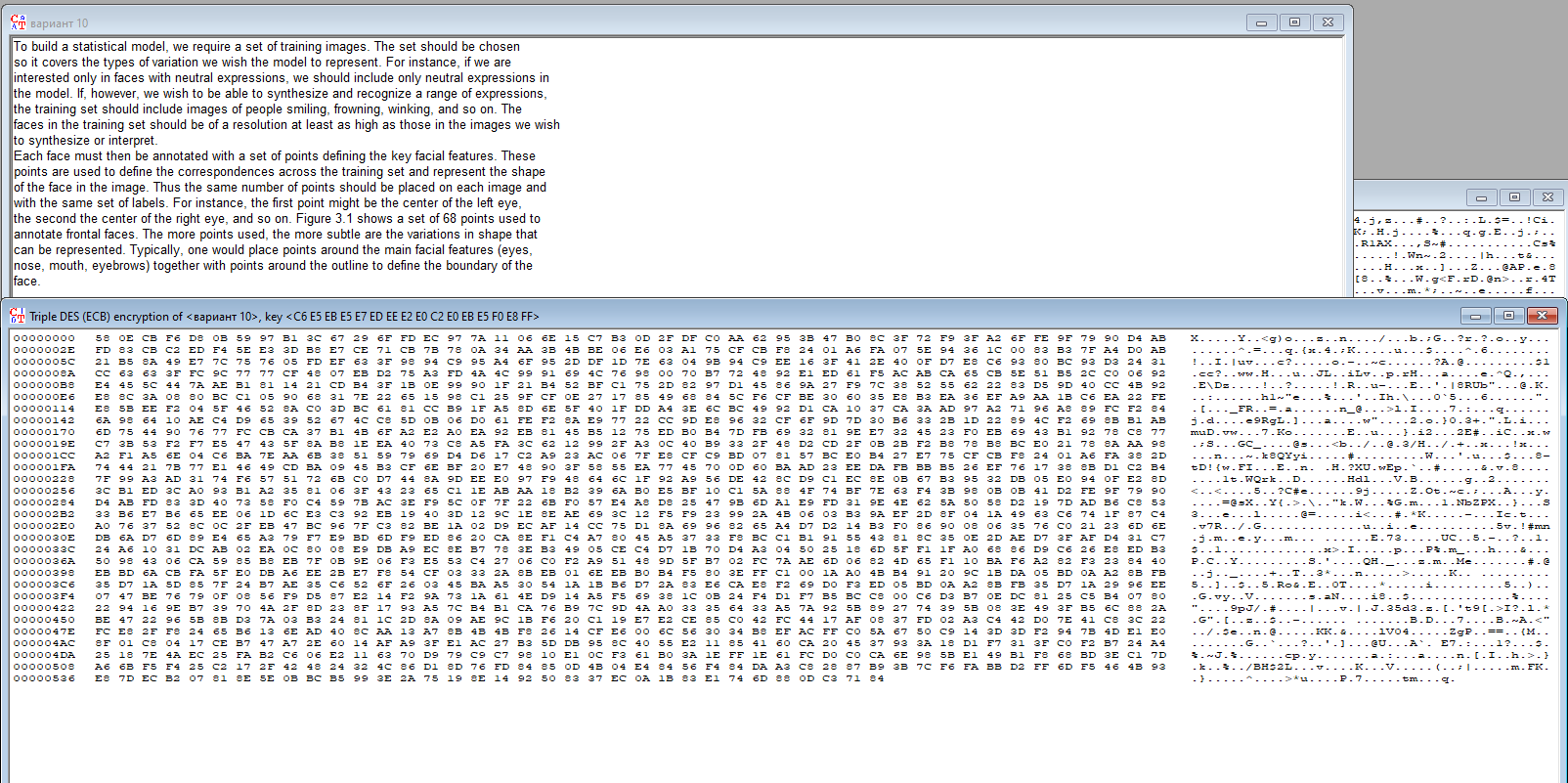


Ентропія та максимальна можлива ентропія в зашифрованому файлі DES (CBC)

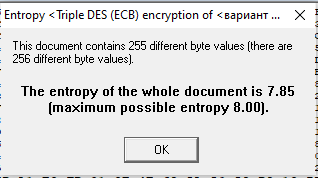


За допомогою CrypTool проводимо TripleDES(ECB) шифрування

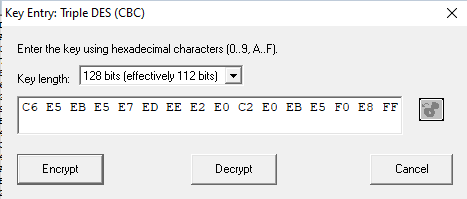


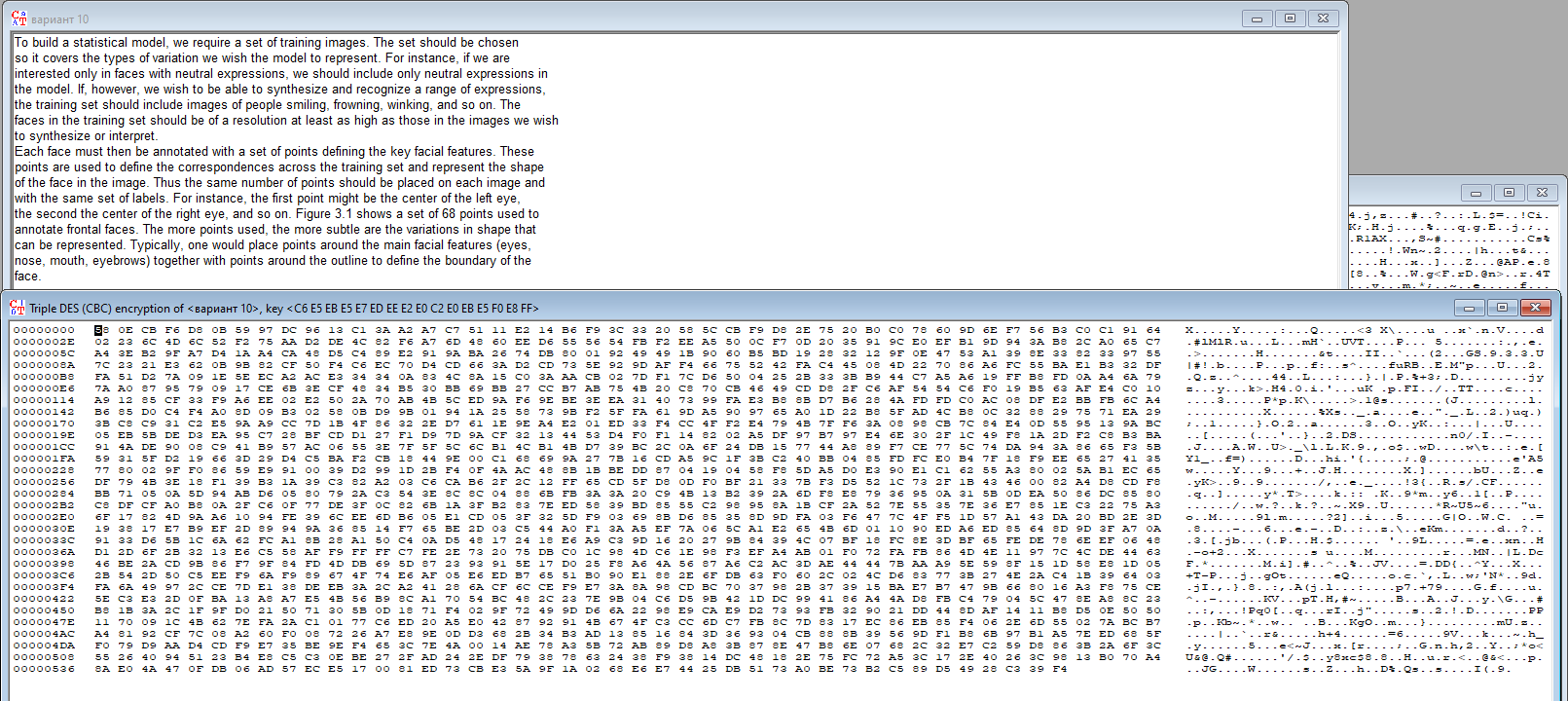


Ентропія та максимальна можлива ентропія в зашифрованому файлі

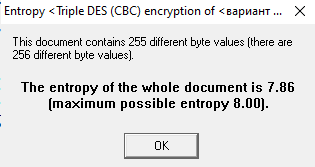


За допомогою CrypTool проводимо TripleDES(CBC) шифрування

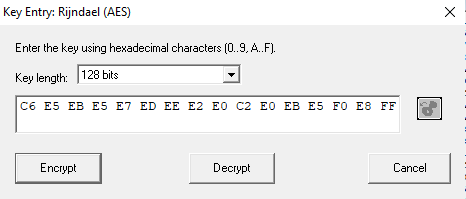


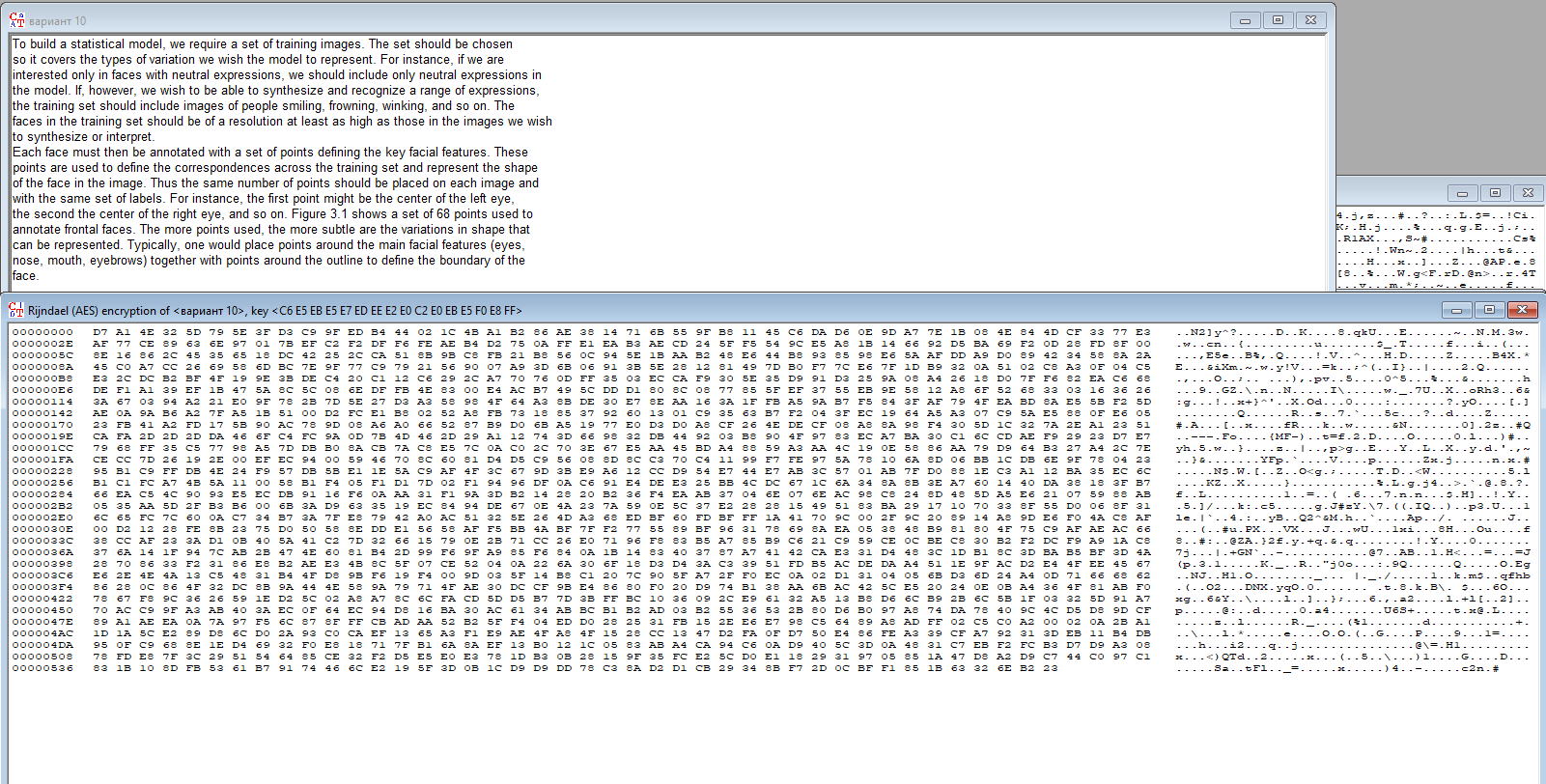


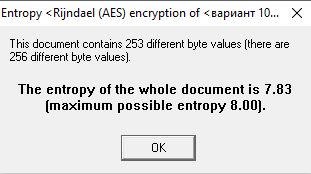
Ентропія та максимальна можлива ентропія в зашифрованому файлі



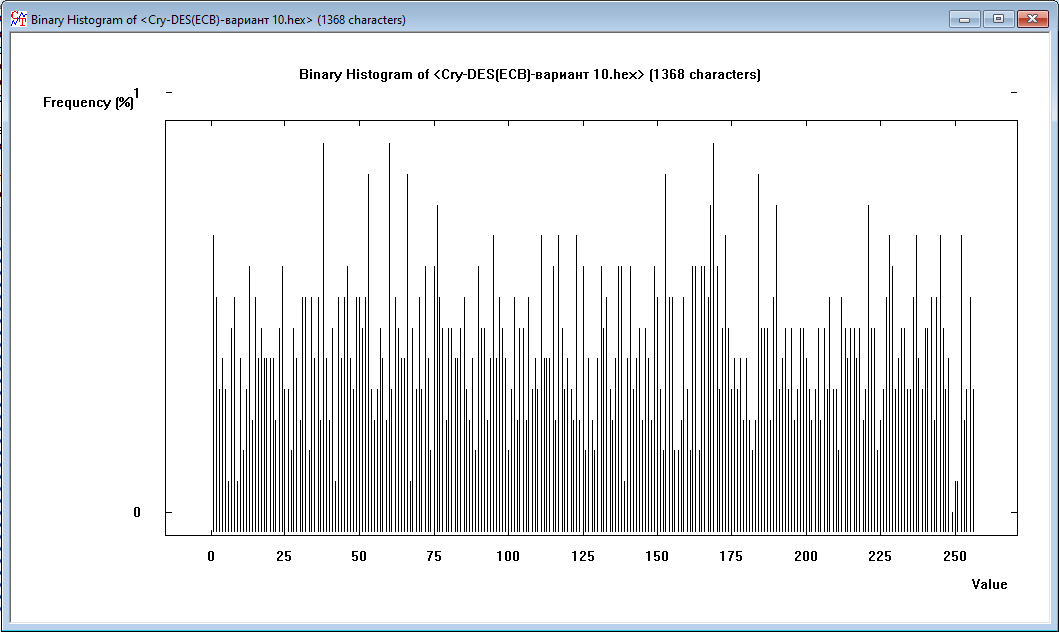
AES

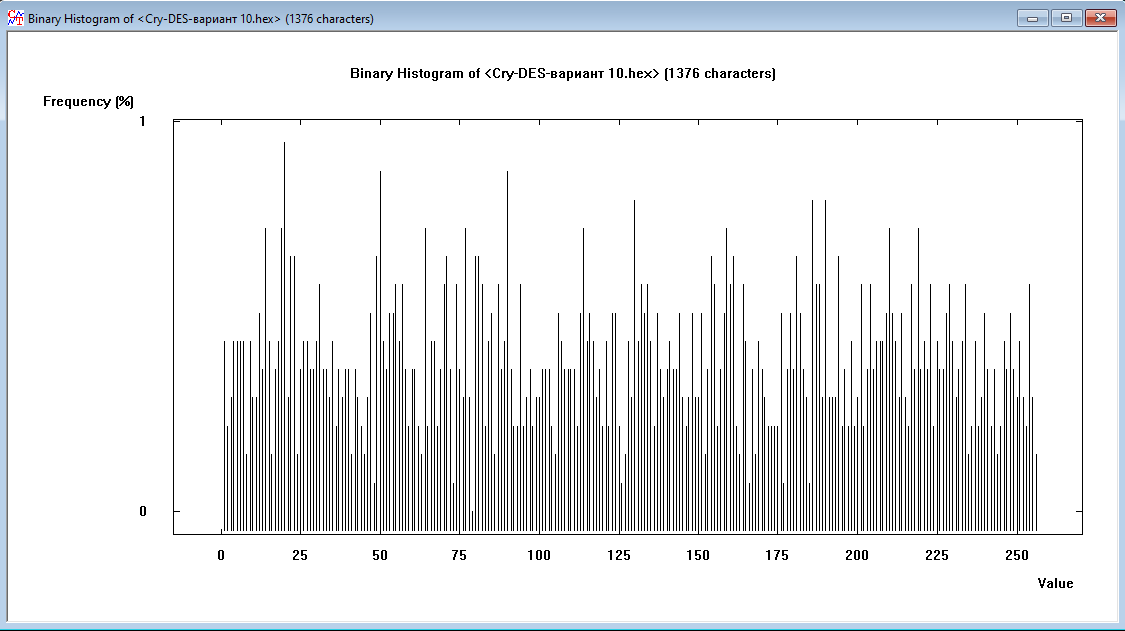




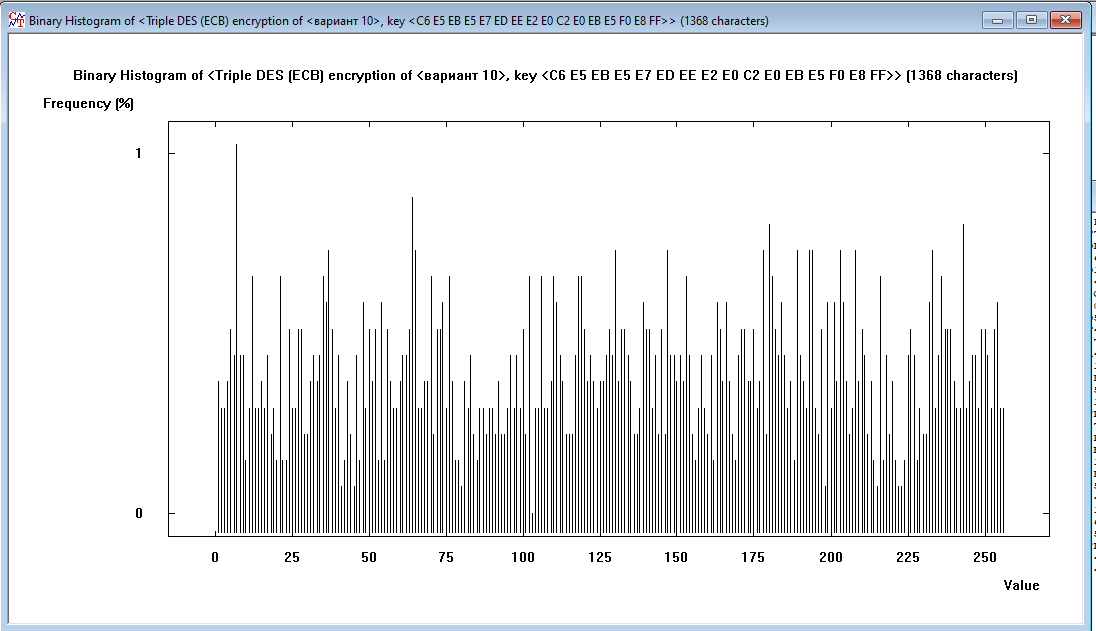


Тепер побудуємо гістограми розподілу частот символів зашифрованих файлів

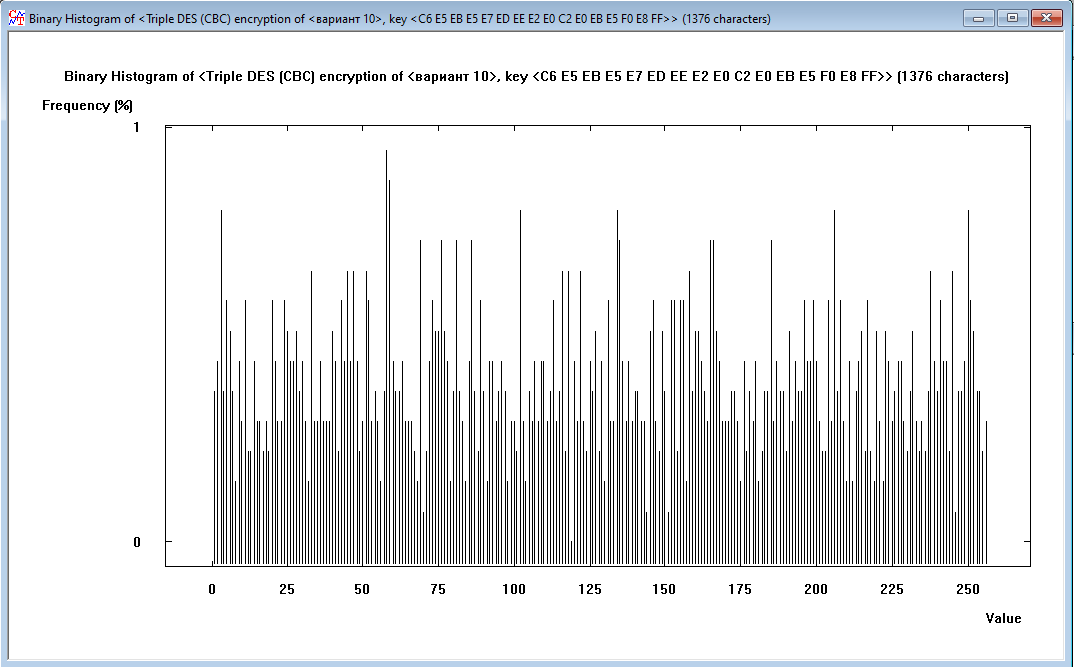
DES(ECB)  
  
DES(CBC)



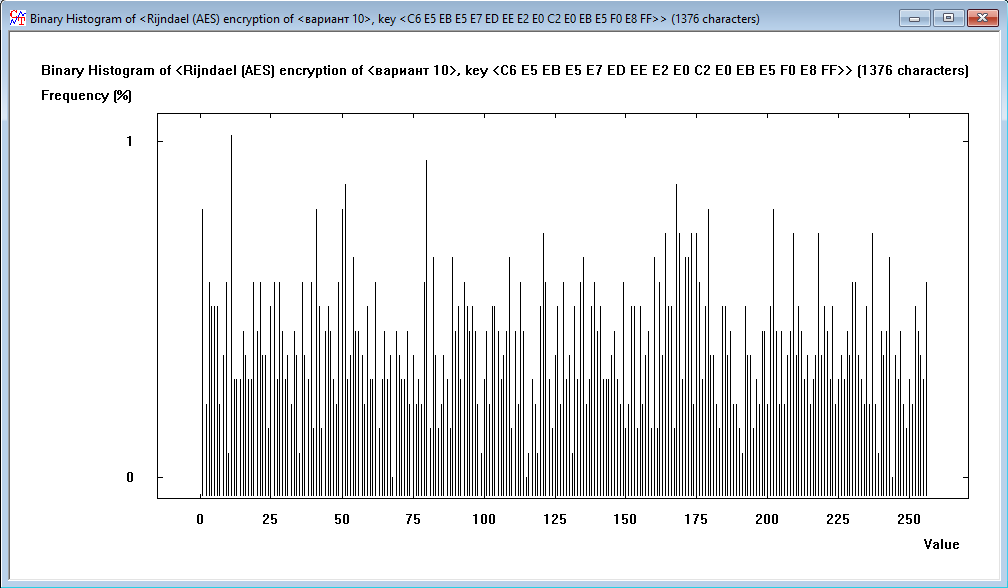
TripleDES(ECB)



TripleDES(CBC)



AES



Проведемо оцінку часу для взлому файлів методом «грубої сили»

DES(ECB): 5.2 days

DES (CBC): 7.3 days

Triple DEC (ECB): 1.6e+015years

Triple DES (CBC): 1.9e+015years

AES: 1.2e+018years

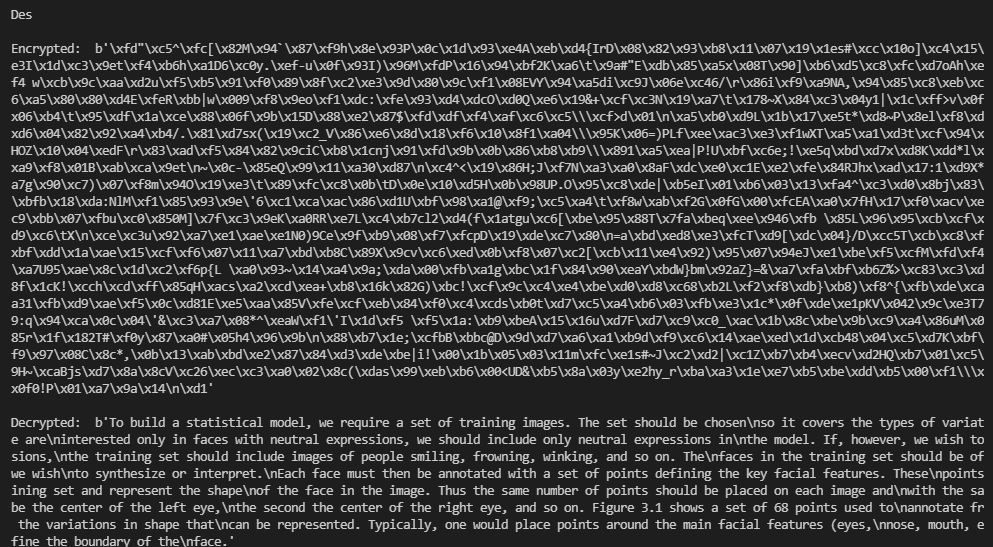
Програмна реалізація шифрування і дешифрування

Результат роботи програми:

**Triple DES(ECB)**



**DES(ECB)**



Лістинг програми

from Crypto.Cipher import DES

from Crypto.Cipher import DES3

from Crypto import Random

with open('10.txt', 'r') as file:

    data = file.read()

iv = Random.new().read(DES3.block\_size)

cipher\_triple\_des = DES3.new(

    bytes('ЖелезноваВалерия', 'windows-1251'),

    DES3.MODE\_CFB,

    iv

    )

cipher\_des = DES.new(

    bytes('Железнов', 'windows-1251'),

    DES.MODE\_CFB,

    iv

    )

decrypt\_triple\_des = DES3.new(

    bytes('ЖелезноваВалерия', 'windows-1251'),

    DES3.MODE\_CFB,

    iv

    )

decrypt\_des = DES.new(

    bytes('Железнов', 'windows-1251'),

    DES.MODE\_CFB,

    iv

    )

print('Text: ', data)

triple = cipher\_triple\_des.encrypt(str.encode(data))

common = cipher\_des.encrypt(str.encode(data))

print("\n\nDes")

print('\nEncrypted: ', common)

print('\nDecrypted: ', decrypt\_des.decrypt(common))

print("\nTripleDes")

print('\nEncrypted: ', triple)

print('\nDecrypted: ', decrypt\_triple\_des.decrypt(triple))