Національний технічний університет України
«Київський політехнічний інститут»

Інститут Прикладного системного аналізу
Кафедра Системного проектування

Лабораторна робота №2

з дисципліни «**ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ**»

«Дослідження сучасних симетричних систем шифрування»

Виконав:
студент групи ДА-82
факультету «ІПСА»
Муравльов Андрій
Варіант 17

Київ – 2020

Хід роботи

Завдання 1. 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.

Оскільки кодування Windows 1251 не є актуальним на даний момент, будемо використовувати кодування UTF-8.

Отримаємо ключі для шифрування, взявши за оригінал строку *«Муравльов Андрій Дмитрович»*

64-бітний ключ для алгоритму DES*:*

63 45 58 4A 83 A0 C4 D7

128-бітний ключ для алгоритмів TripleDES та AES*:*

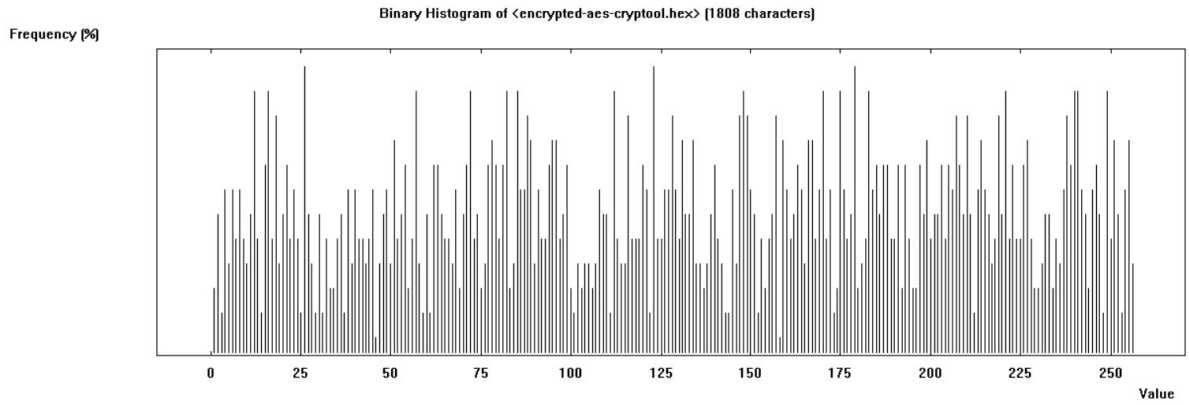
63 45 58 4A 83 A0 C4 D7 BA 3A B6 A6 95 25 C0 5E

Завдання 2. 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.

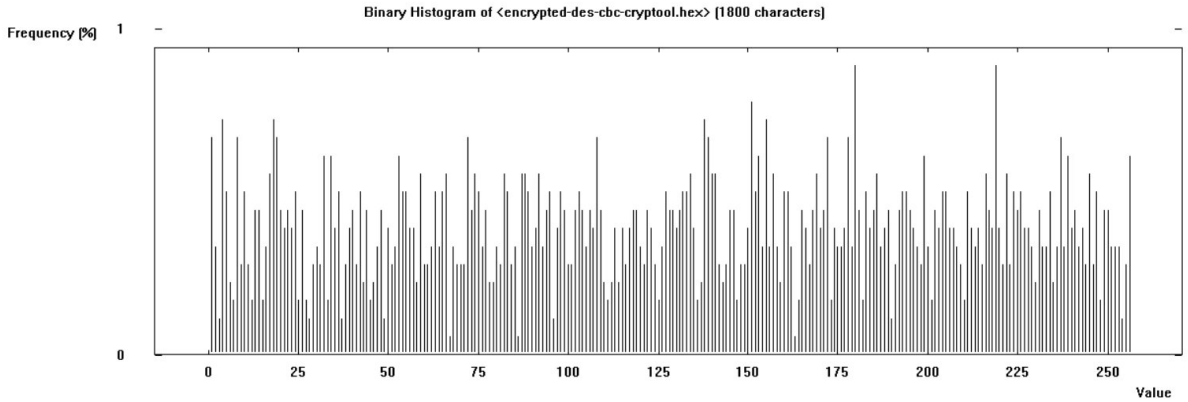
Зведена таблиця ентропій

Назва алгоритму	*Ентропія файлу*	*Максимальна ентропія*
DES (CBC)	7.88	8.00
DES (ECB)	7.86	8.00
TripleDES (ECB)	7.87	8.00
TripleDES (CBC)	7.89	8.00
AES	7.90	8.00

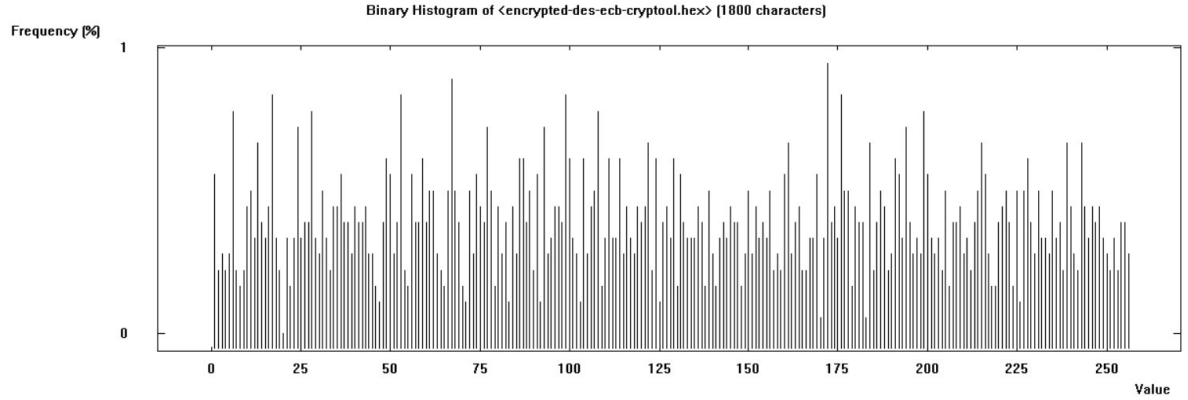
Гістограми



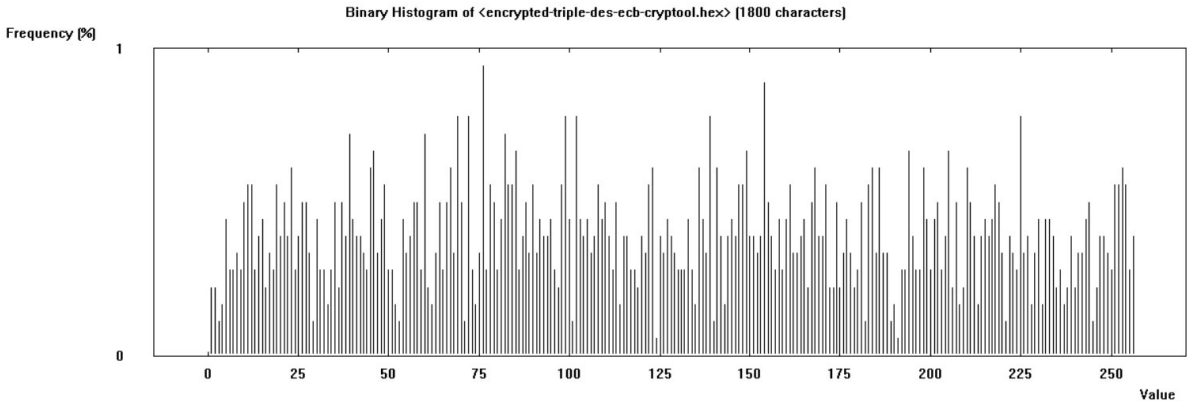
Гістограма розподілу частот для алгоритму AES



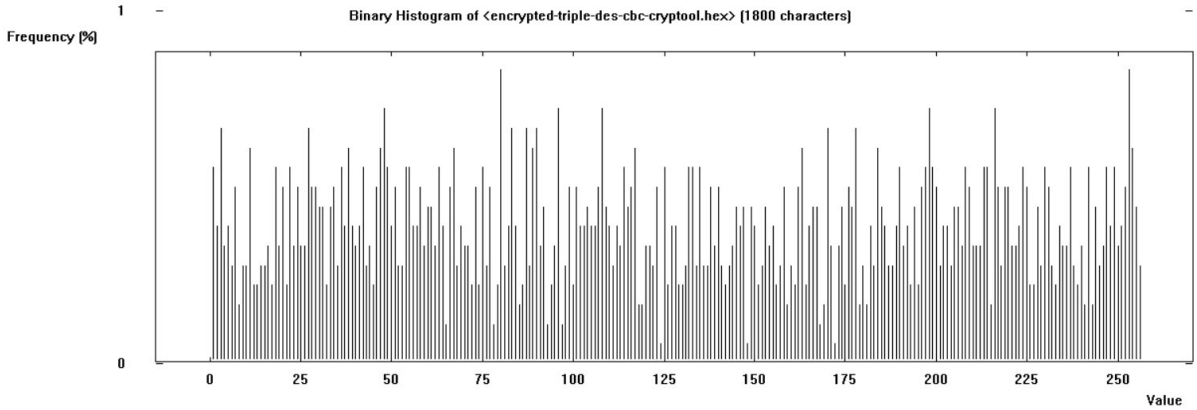
Гістограма розподілу частот для алгоритму DES (CBC)



Гістограма розподілу частот для алгоритму DES (ECB)



Гістограма розподілу частот для алгоритму TripleDES (ECB)



Гістограма розподілу частот для алгоритму TripleDES (CBC)

Маючи такі розподіли частот, можемо зробити висновок, що жоден шифр не піддається статистичному або частотному аналізу, оскільки судячи з ентропії розподіл дуже схожий на випадковий та не містить літер.

Завдання 3. 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.

Дослідимо час, який потрібен для злому ключа, в залежності від кількості відомих символів на прикладі алгоритму DES (CBC):

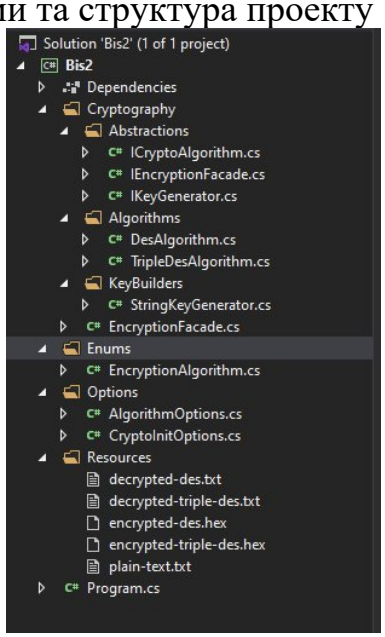
Кількість відомих байтів	Час злому, мс
0	6.3072e+14
2	4.253e+10
4	3.24e+6
6	2.23e+2

При подальшому зростанні кількості відомих байтів за допомогою алгоритму «грубої сили» ключ знаходиться за дуже короткий проміжок часу. Кожен відомий байт зменшує час на розшифровку методом грубої сили в сто разів.

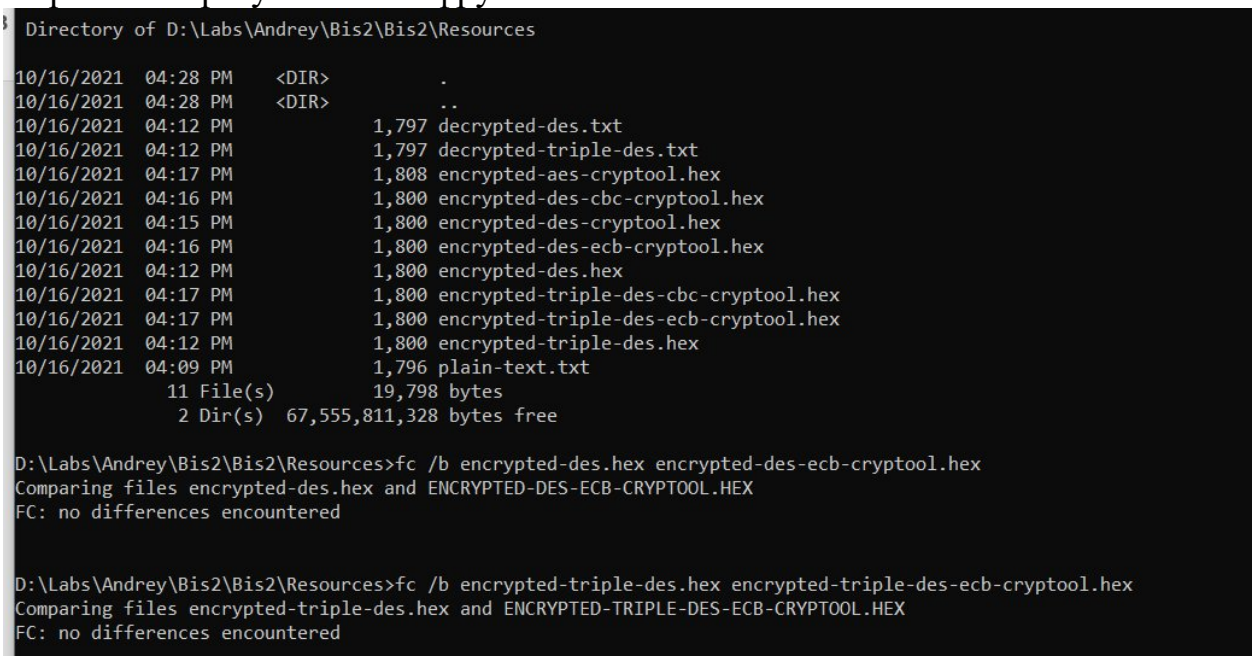
Програма для шифрування за допомогою шифрів DES (ECB)

Вихідний код для програми знаходиться за посиланням твоя линка на гх

Результати роботи програми та структура проекту



Порівняємо результати шифрування:



Порівняння результатів роботи програми та пакету CrypTool

Шляхом порівняння файлів за допомогою утиліти Windows fc у режимі порівняння бінарних файлів (ключ /b) бачимо, що результати отримані створеною програмою та результати, отримані за допомогою пакету CrypTool не відрізняються. Таким чином, можемо зробити висновок, що програма працює коректно. Також це підтверджується корректною дешифровкою програмою тексту, що був зашифрований за допомогою пакету CrypTool.

Висновки

В результаті роботи було досліджено відносно сучасні методи симетричного шифрування та проаналізовано їх криптостійкість. У результаті аналізу було зроблено висновок про неподаваність даних шифрів частотному аналізу на основі величини ентропії та характеру вихідного файлу. Було проаналізовано криптостійкість алгоритму DES у режимі Cypher Block Chaining, CBC при зломі методом грубої сили, результати аналізу зведено в таблицю та отримано залежність часу злому від кількості відомих байтів ключа. В результаті аналізу можна зробити висновок, що даний алгоритм досить довго зламується при повністю невідомому ключі(необхідний час – порядку 2,000 років на процессорі Intel(R) Core(TM) i7-10510U @ 1.80GHz), проте кожний відомий байт зменшує час на злом приблизно у сто разів. Також в ході роботи було отримано досвід інтеграції існуючих реалізацій даних алгоритмів на платформі .NET Core 3.1 з використанням простору імен *System.Security.Cryptography,* який широко використовується у промислових проектах на даній платформі.