МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

НАВЧАЛЬНО-НАУКОВИЙ КОМПЛЕКС

«ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ»

Лабораторна робота № 2

з курсу «Технології захисту інформації»

Тема: «Дослідження сучасних симетричних систем шифрування»

Виконав:

студент IV курсу

групи ДА-32

Колінько Анжела

Київ – 2017

Варіант 11

1. Ключі для кожного шифру:

a. DES (ECB), key={59,56,152,55,21,32,247,94} (hex: 3b 38 98 37 15 20 f7 5e)

b. DES (CBC), key={59,56,152,55,21,32,247,94}

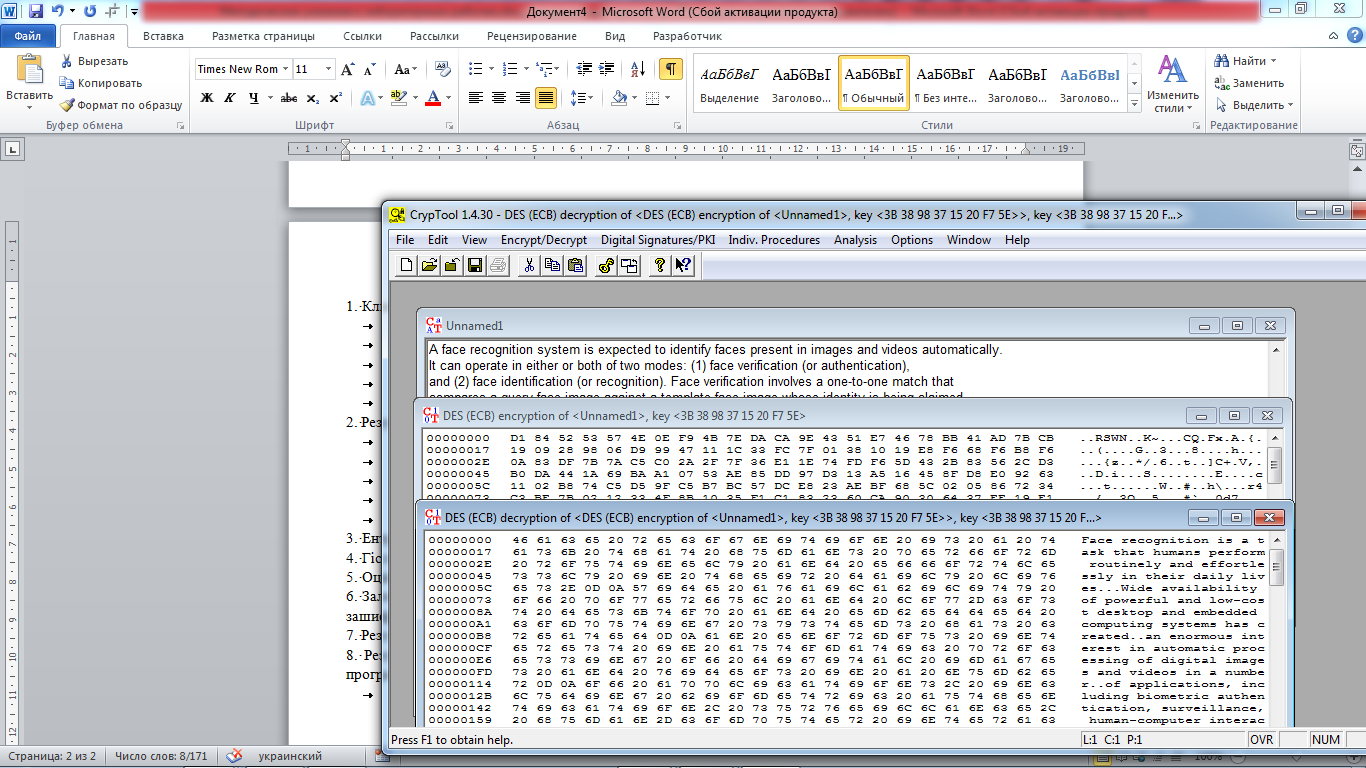
c. TripleDES (ECB), key[i]={59,56,152,55,21,32,247,94}

d. TripleDES (CBC), key[i]={59,56,152,55,21,32,247,94}

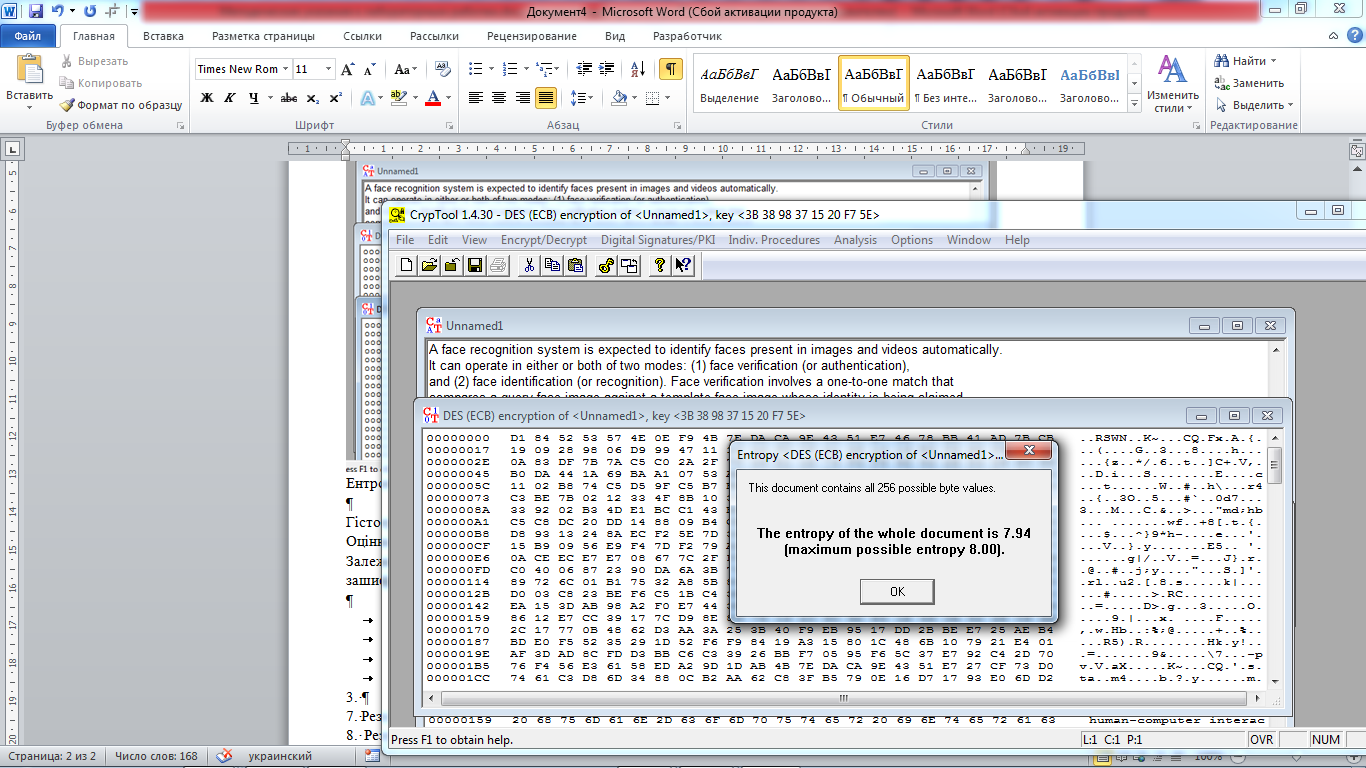
e. AES. key={59,56,152,55,21,32,247,94}

2. Результати шифрування и дешифрування текстового файлу в пакеті CrypTool з використаних алгоритмів

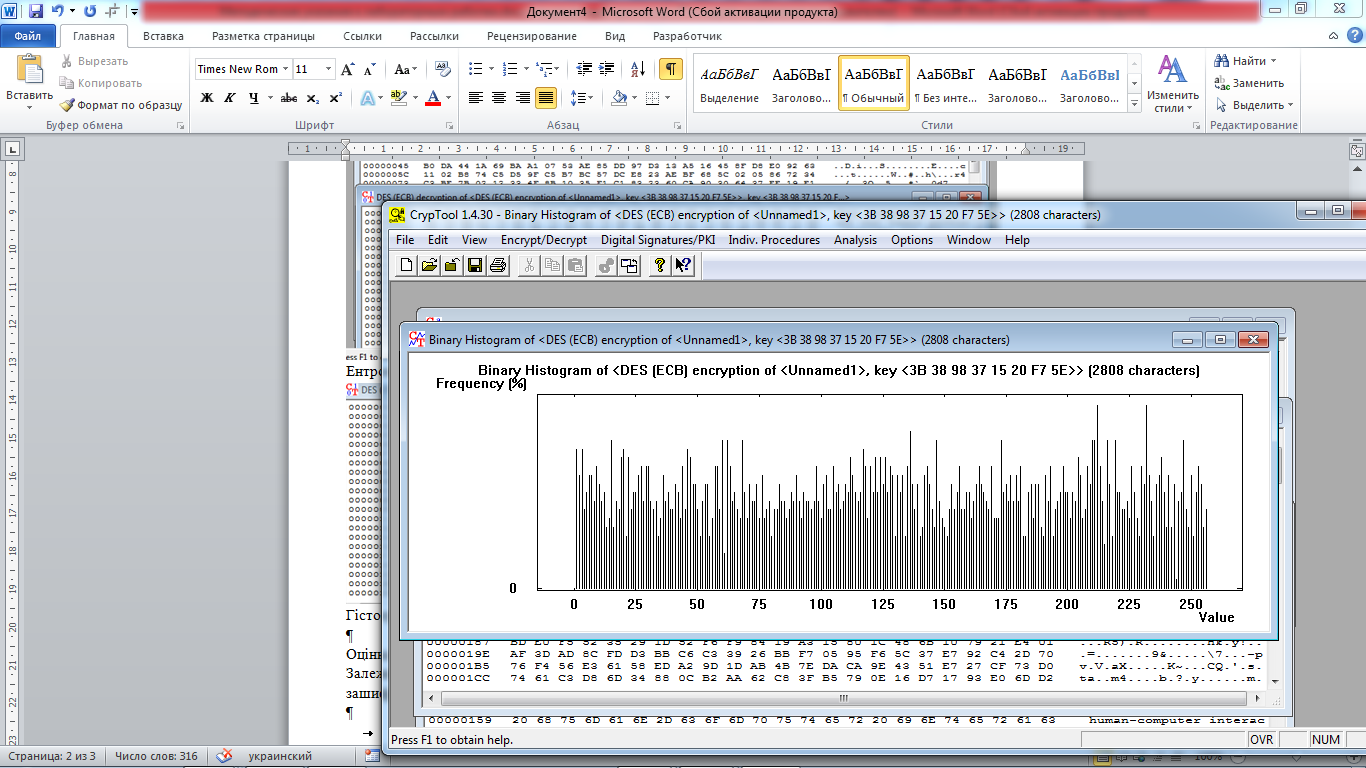
a. DES (ECB),



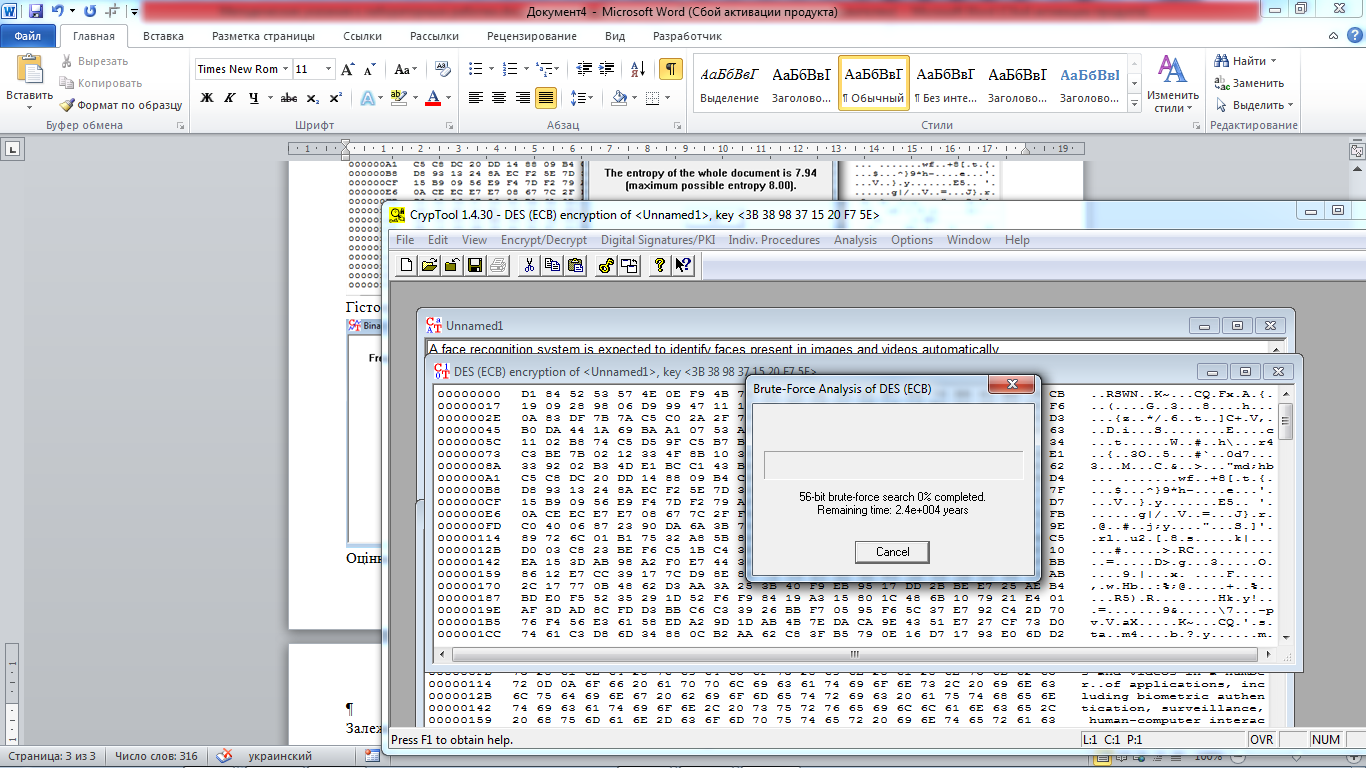
Ентропія, максимально можлива ентропія зашифрованих файлів:



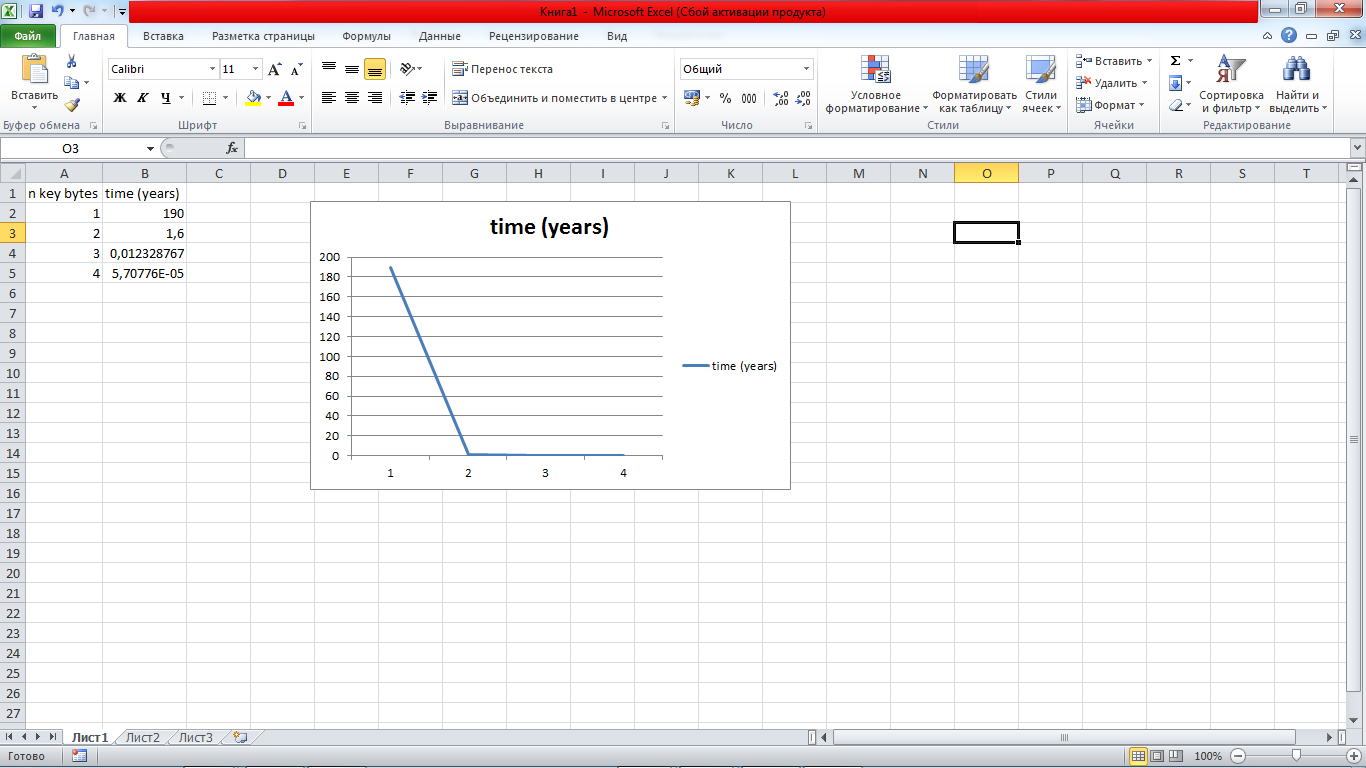
Гістограми розподілу частот символів зашифрованих файлів:



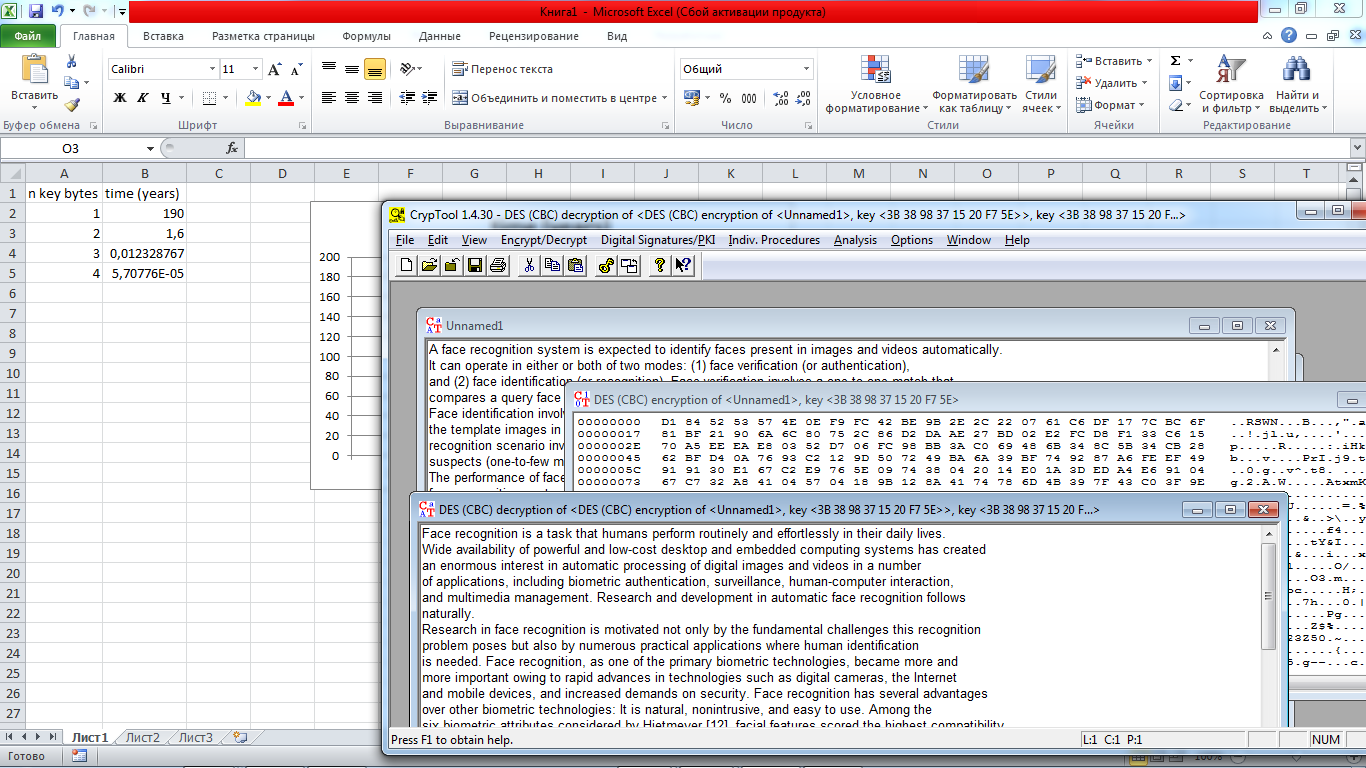
Оцінка часу для взлому зашифрованих фалів методом "грубої сили":



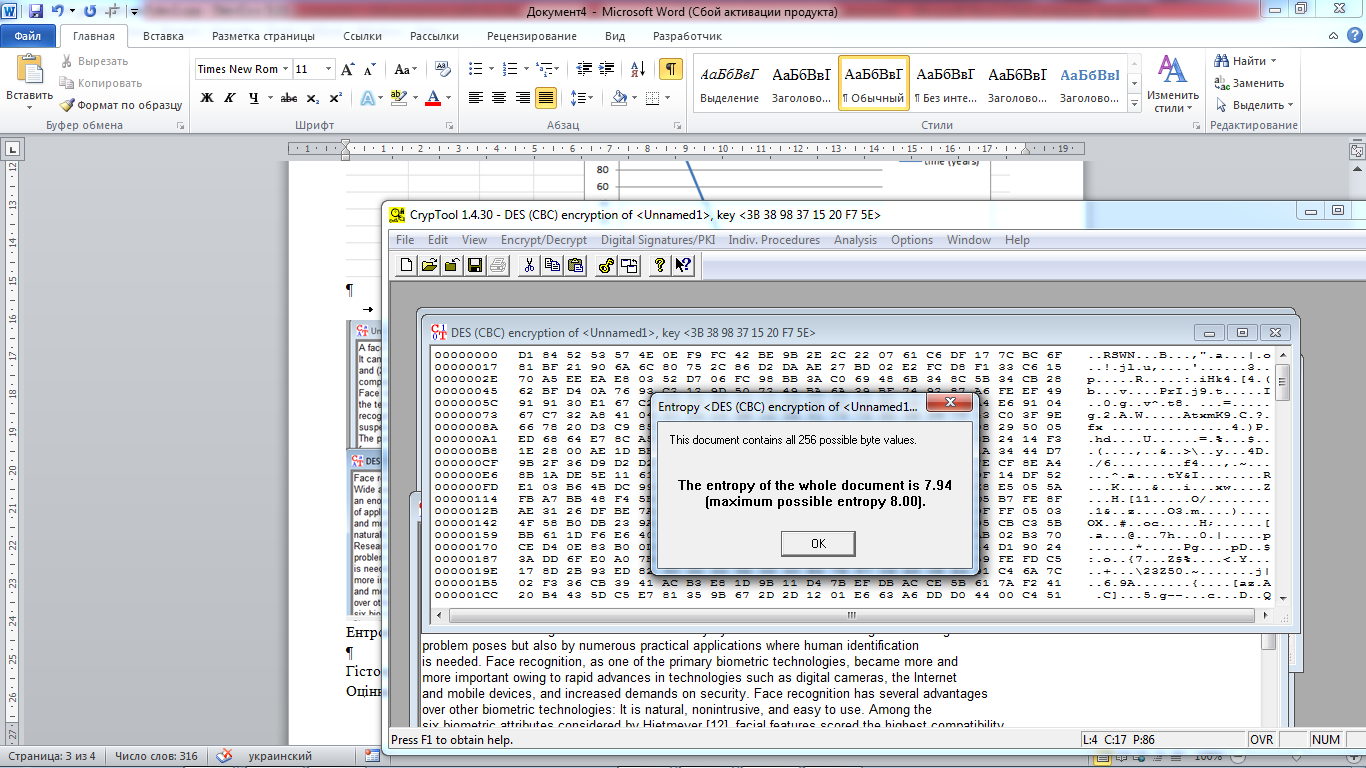
Залежність тривалості взлому досліджуваних шифрів від довжини ключа (результати криптоаналізу зашифрованих файлів при зменшеній довжині ключа):



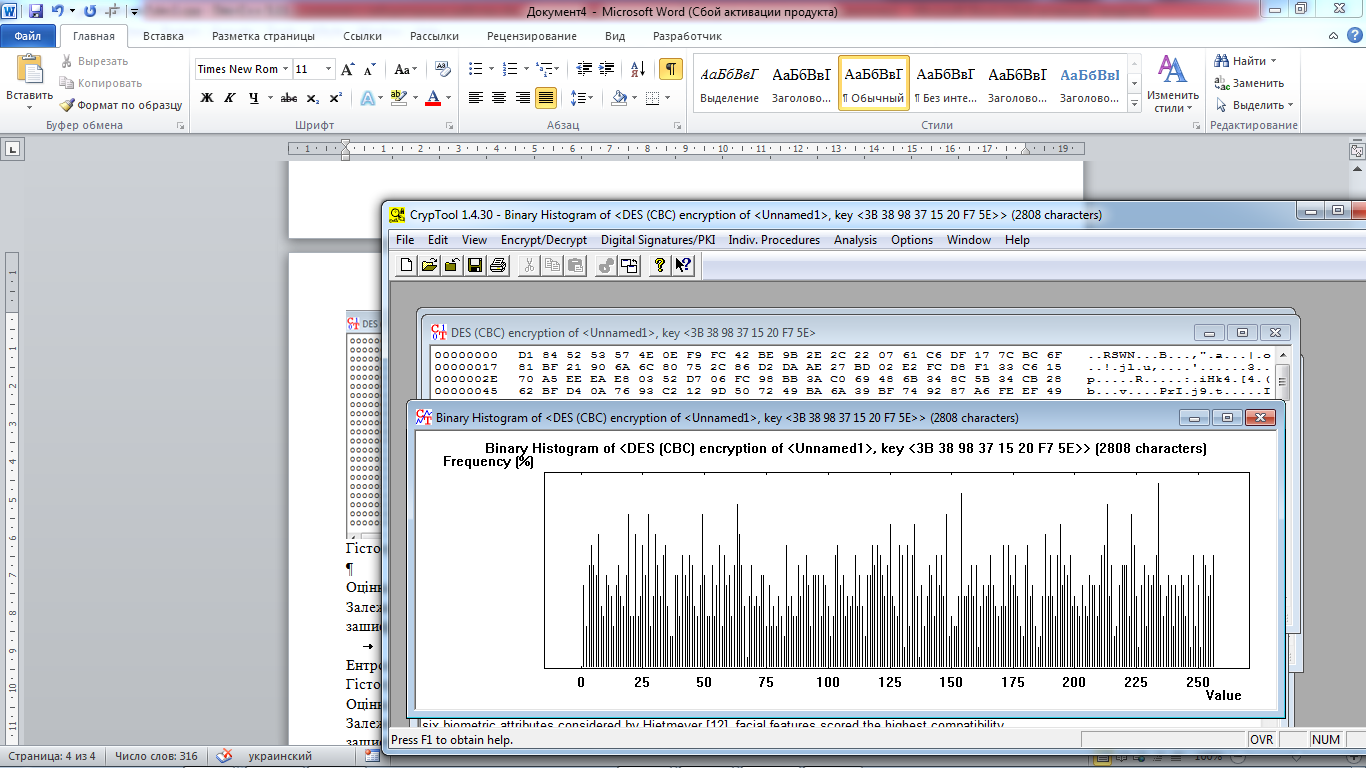
b. DES (CBC),



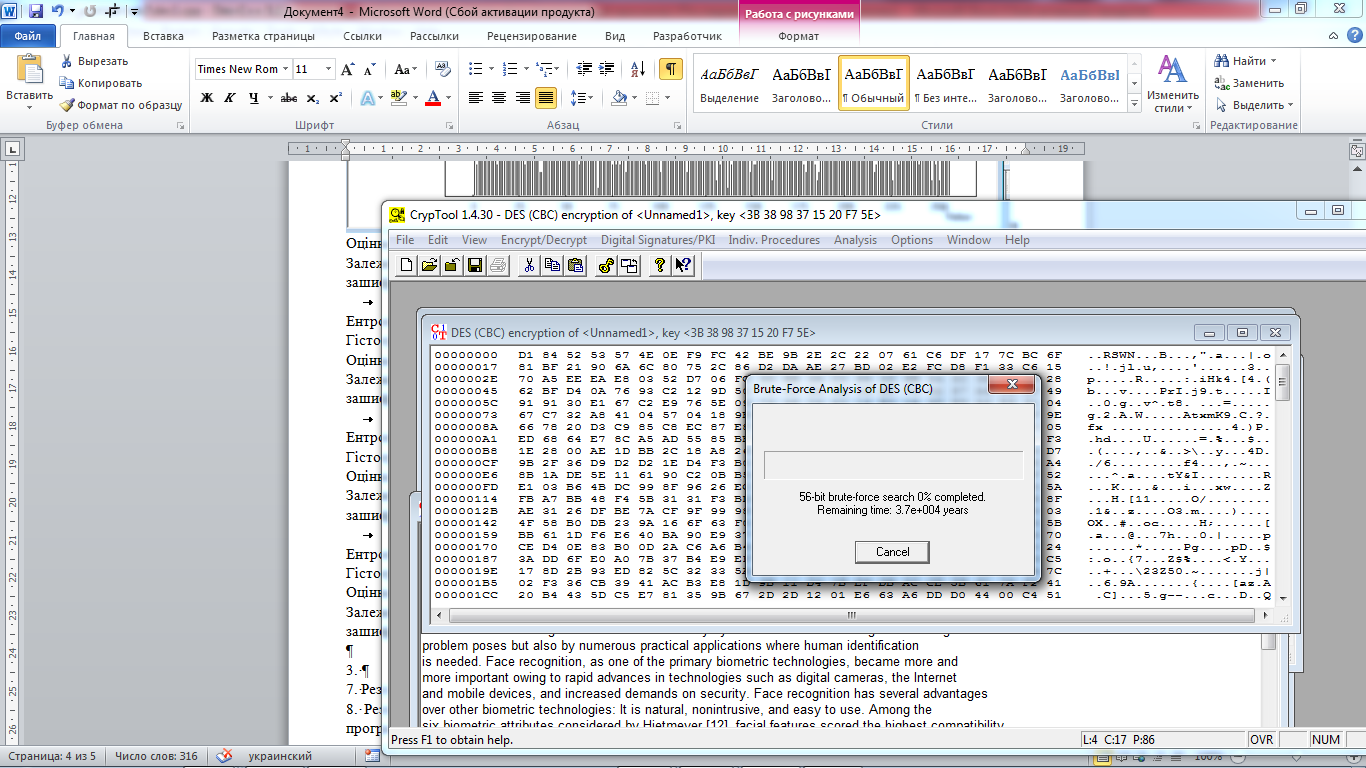
Ентропія, максимально можлива ентропія зашифрованих файлів:



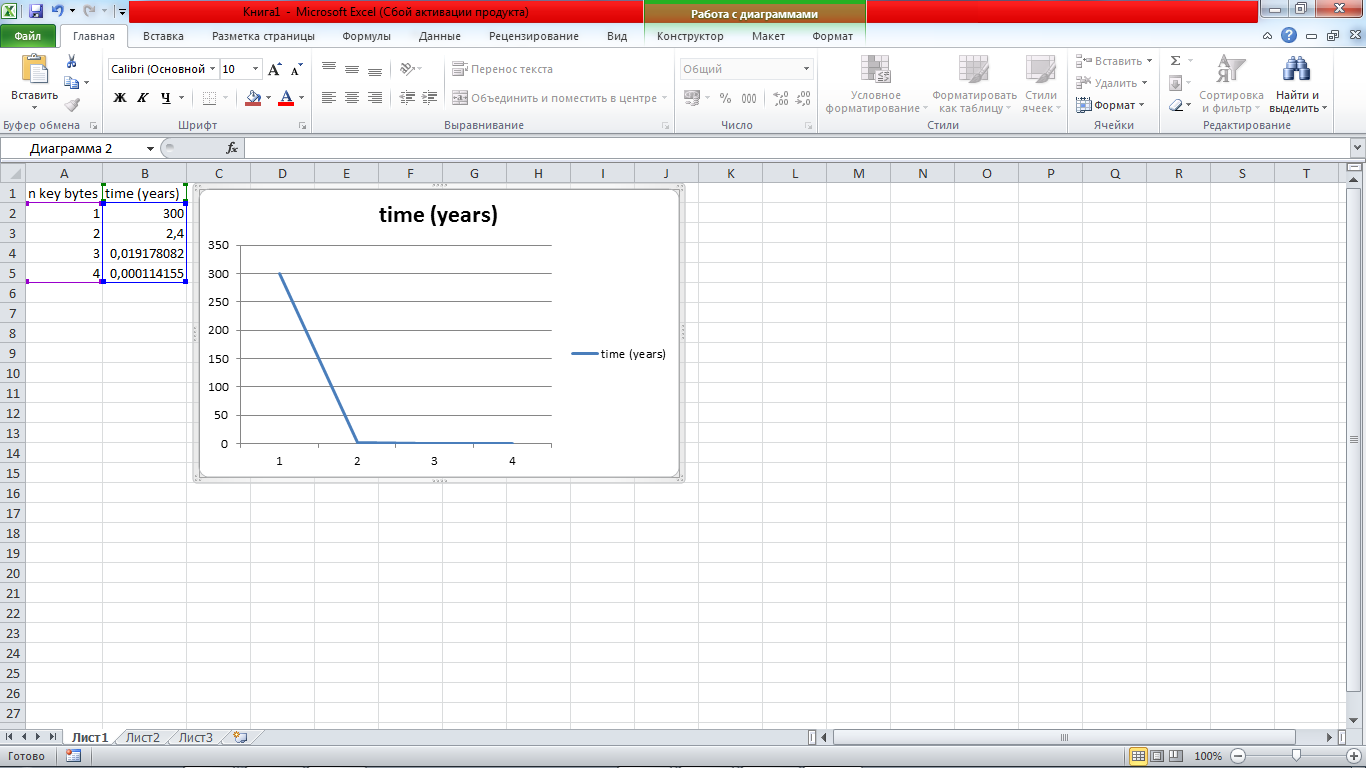
Гістограми розподілу частот символів зашифрованих файлів:



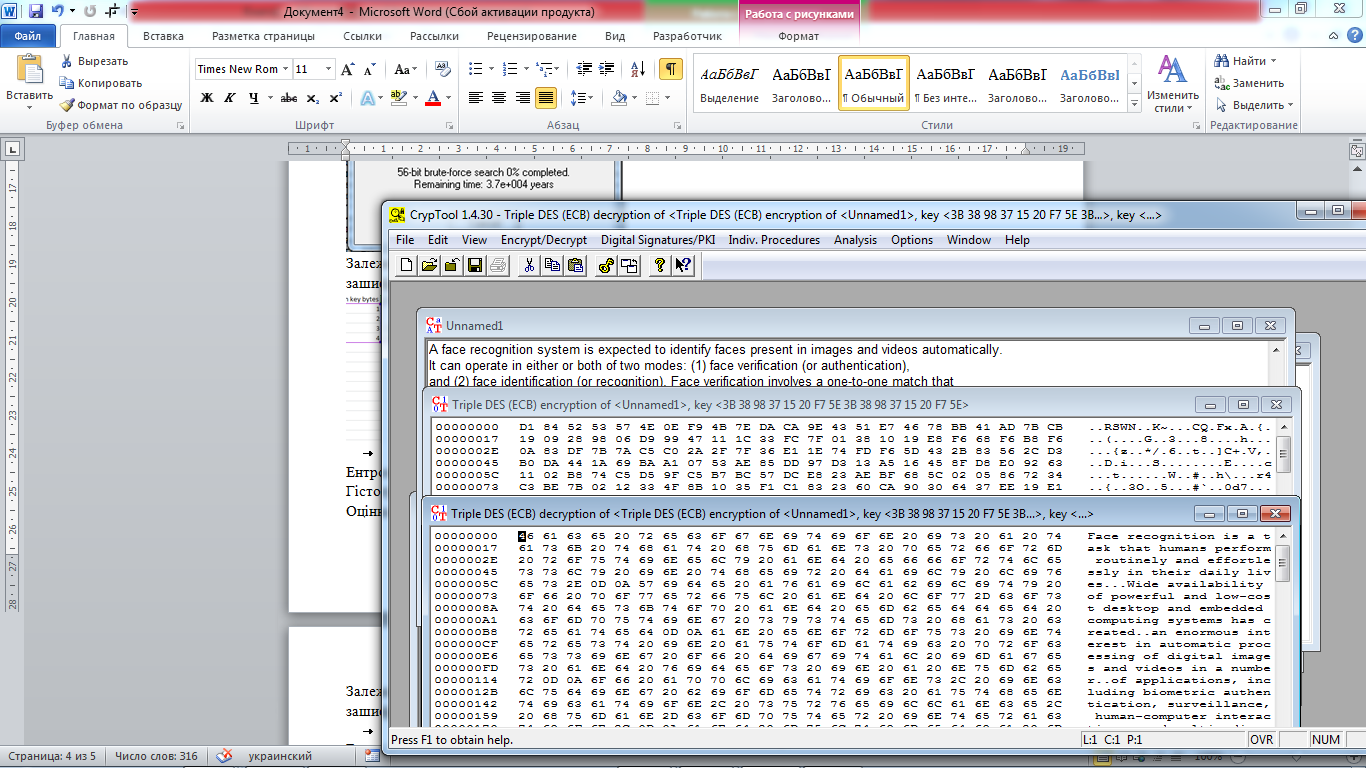
Оцінка часу для взлому зашифрованих фалів методом "грубої сили":



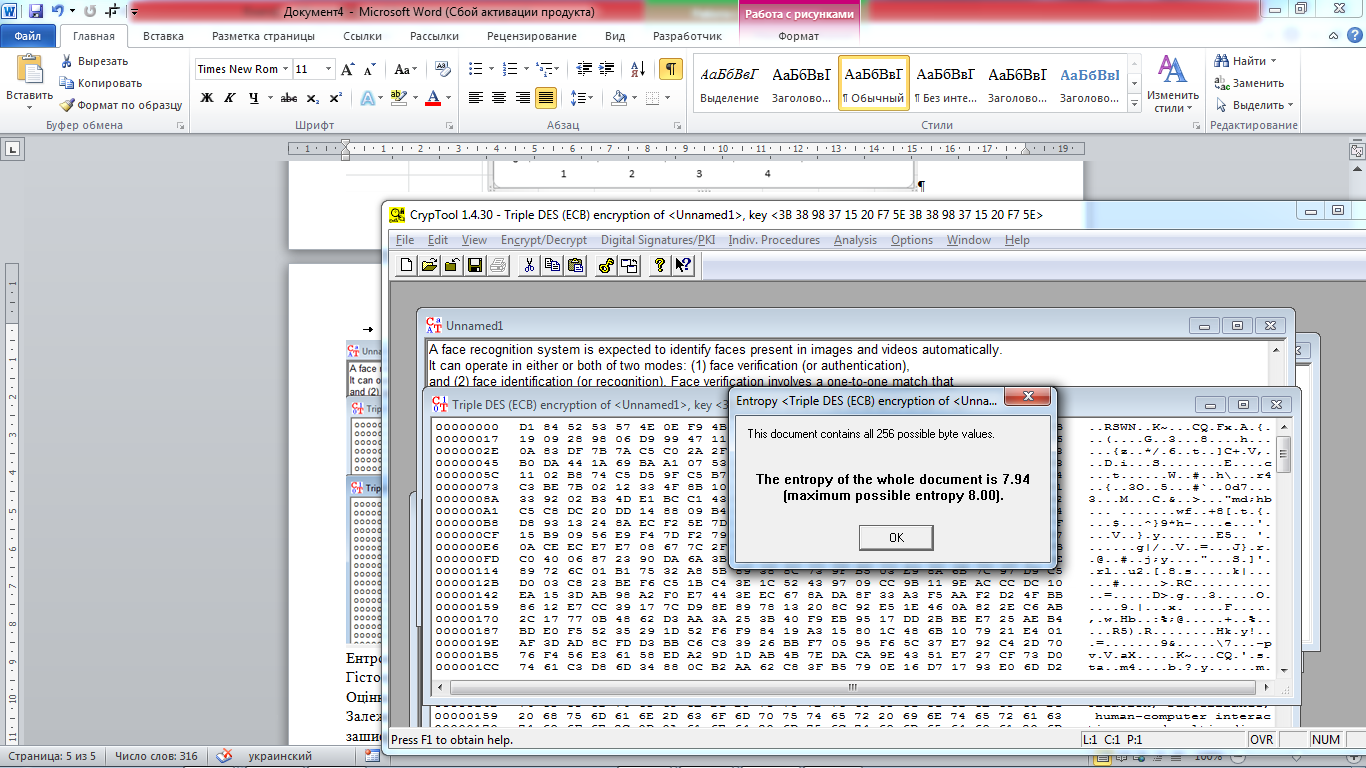
Залежність тривалості взлому досліджуваних шифрів від довжини ключа (результати криптоаналізу зашифрованих файлів при зменшеній довжині ключа):



c. TripleDES (ECB),



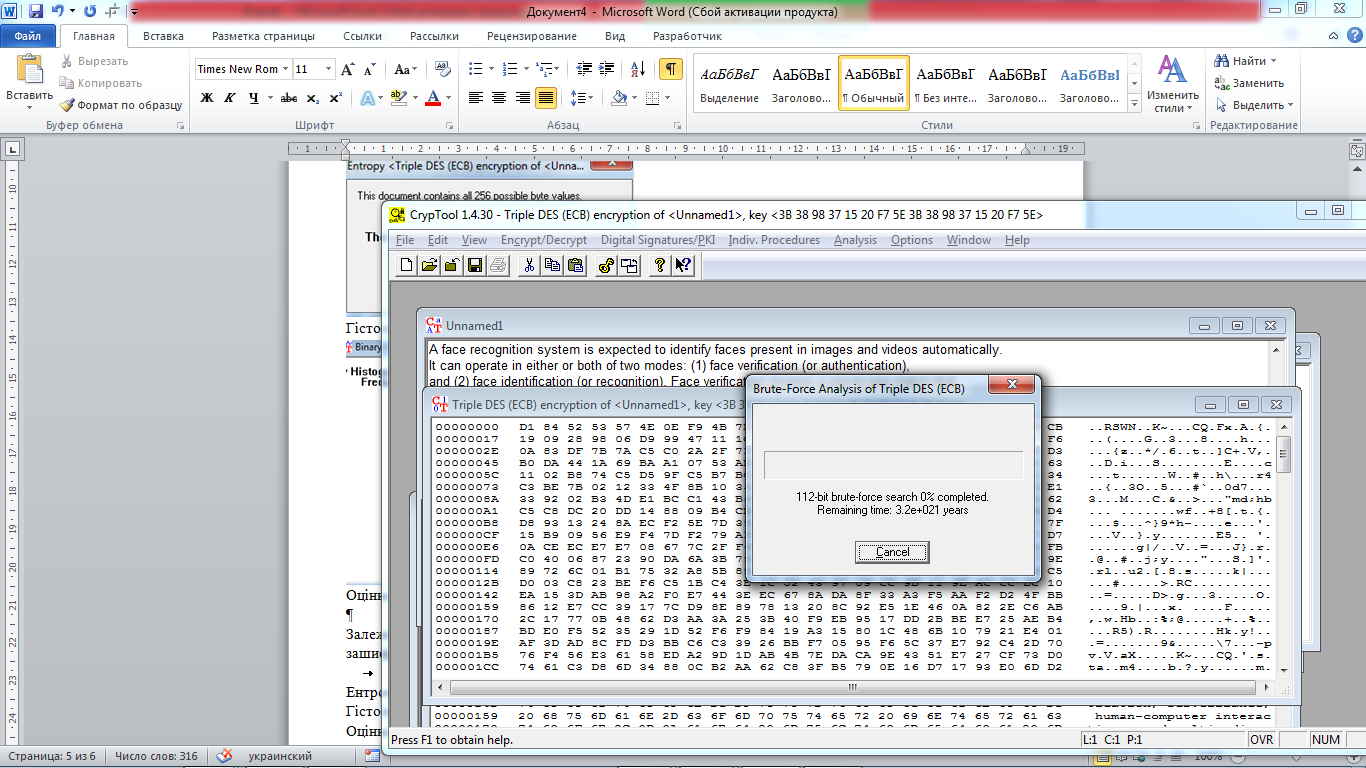
Ентропія, максимально можлива ентропія зашифрованих файлів:



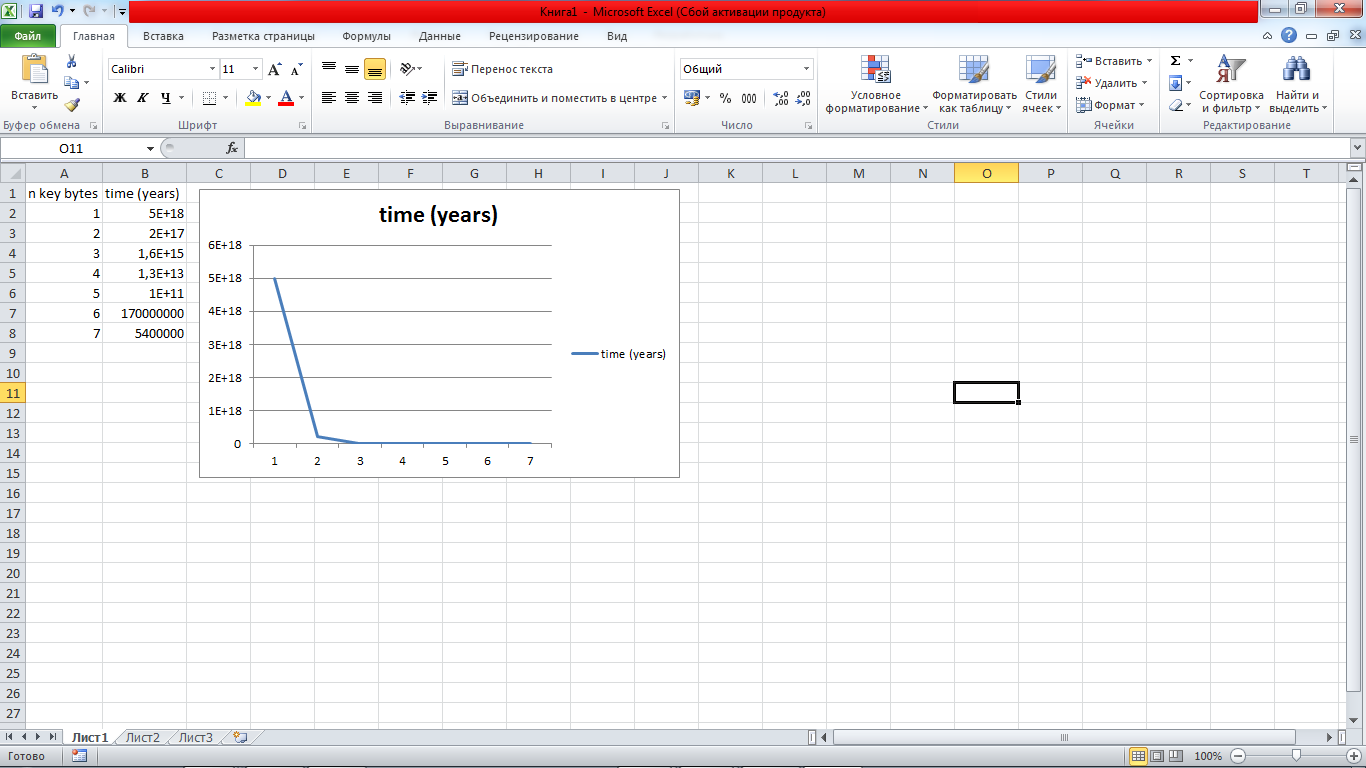
Гістограми розподілу частот символів зашифрованих файлів:



Оцінка часу для взлому зашифрованих фалів методом "грубої сили":



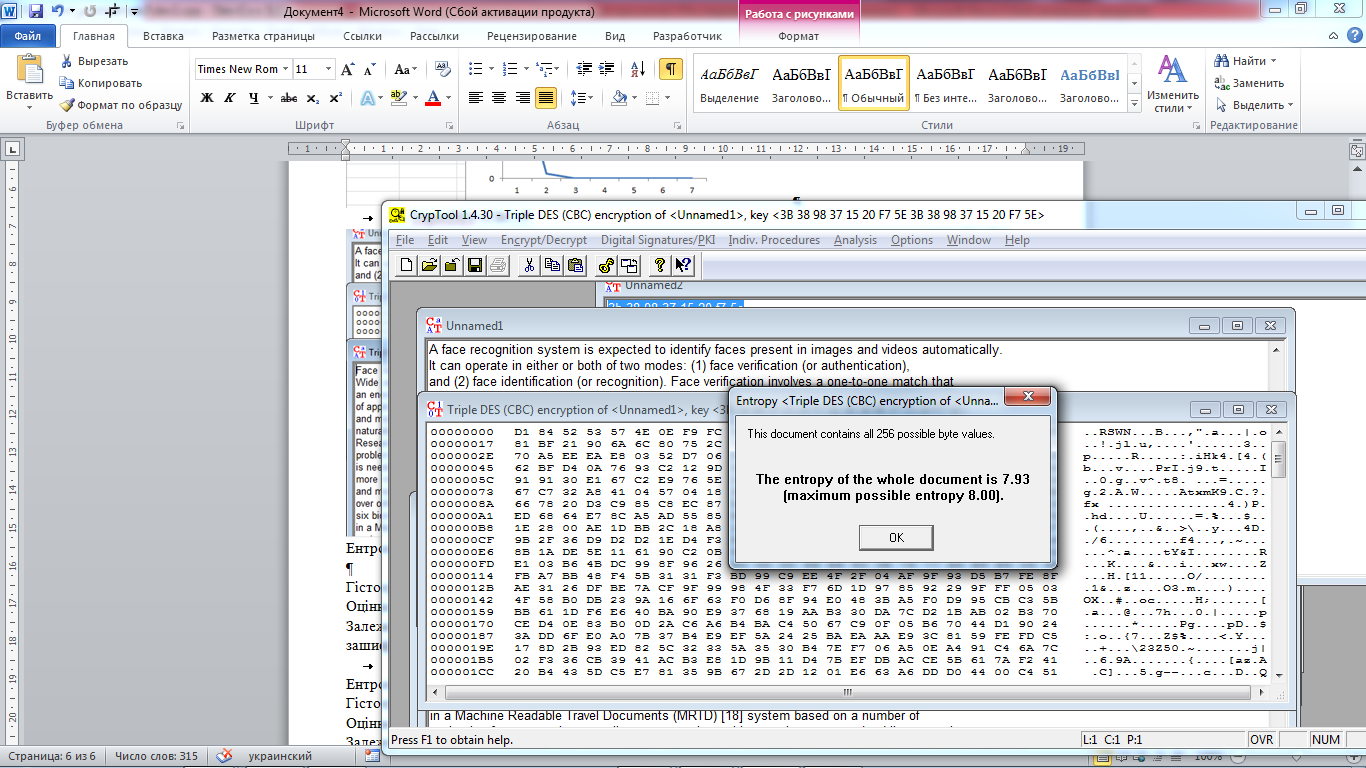
Залежність тривалості взлому досліджуваних шифрів від довжини ключа (результати криптоаналізу зашифрованих файлів при зменшеній довжині ключа):



d. TripleDES (CBC),



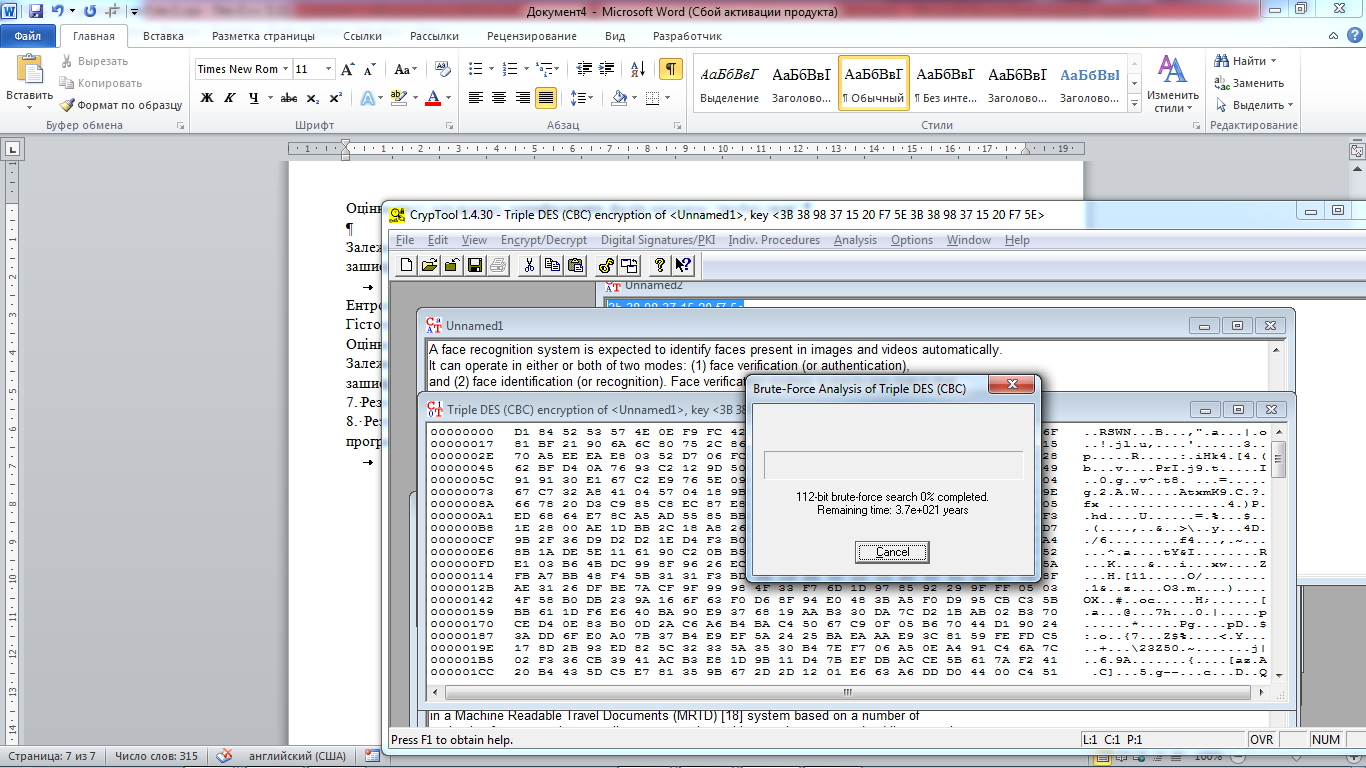
Ентропія, максимально можлива ентропія зашифрованих файлів:



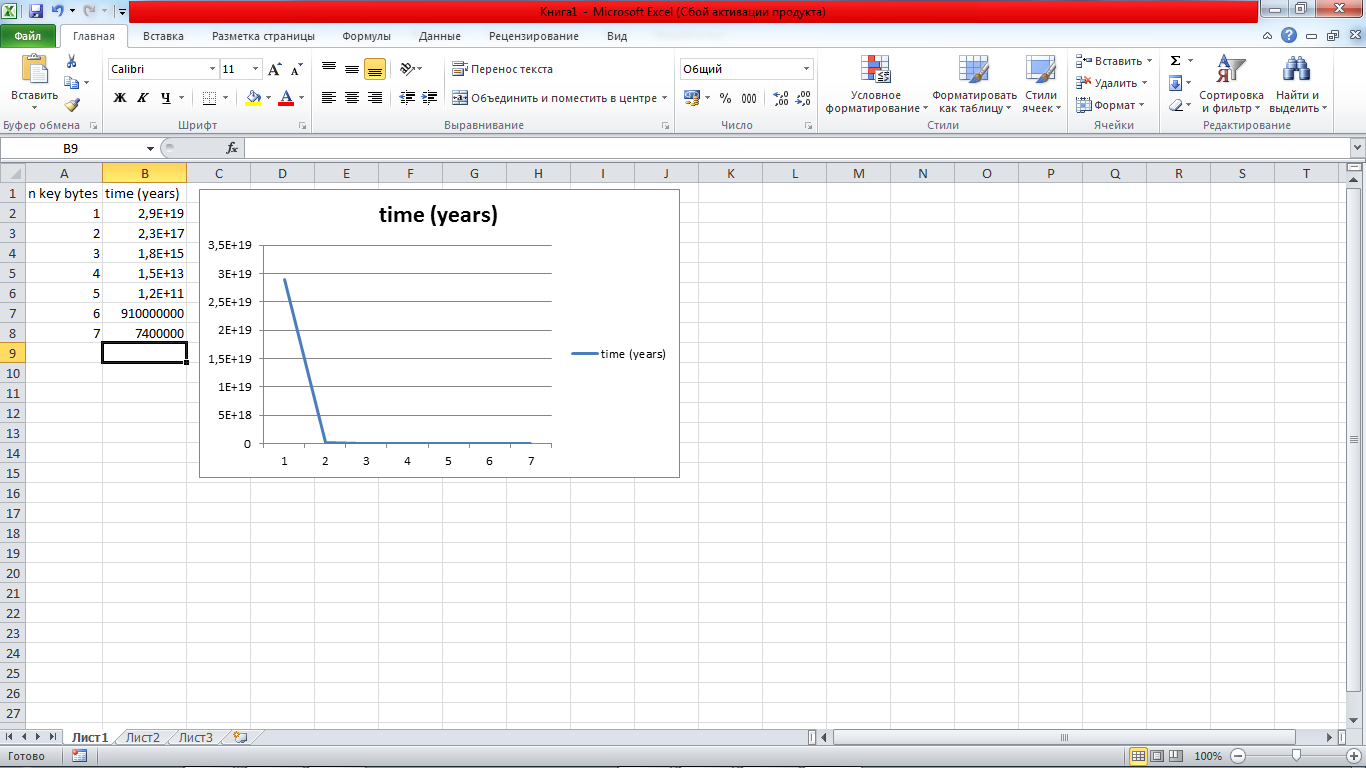
Гістограми розподілу частот символів зашифрованих файлів:



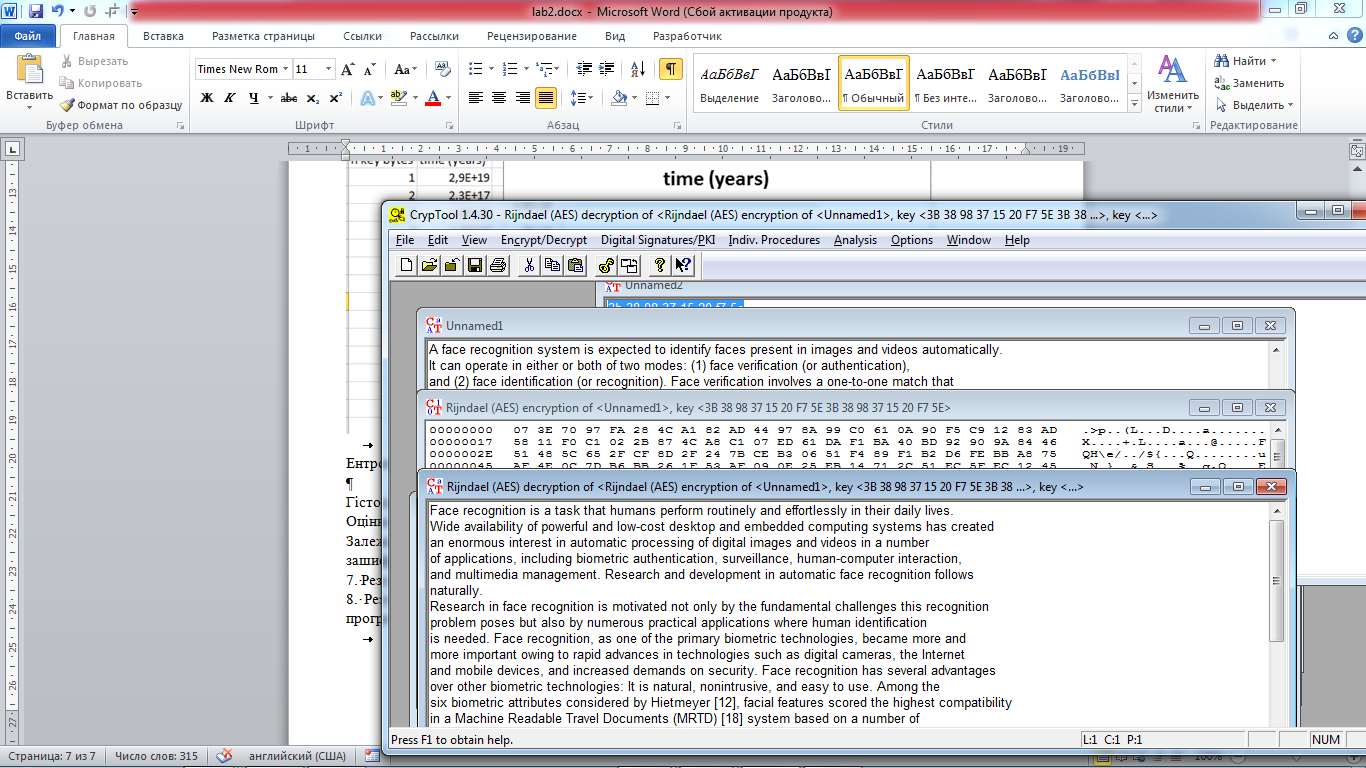
Оцінка часу для взлому зашифрованих фалів методом "грубої сили":



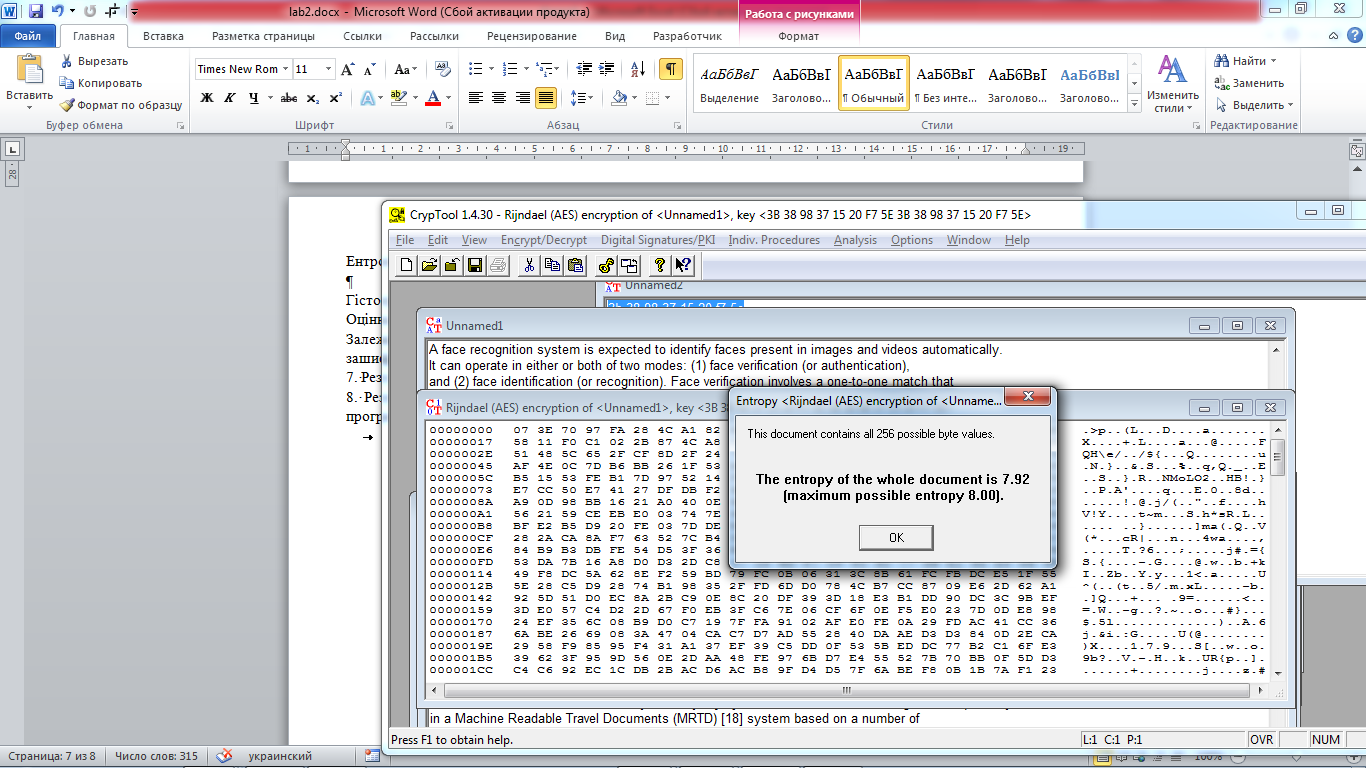
Залежність тривалості взлому досліджуваних шифрів від довжини ключа (результати криптоаналізу зашифрованих файлів при зменшеній довжині ключа):



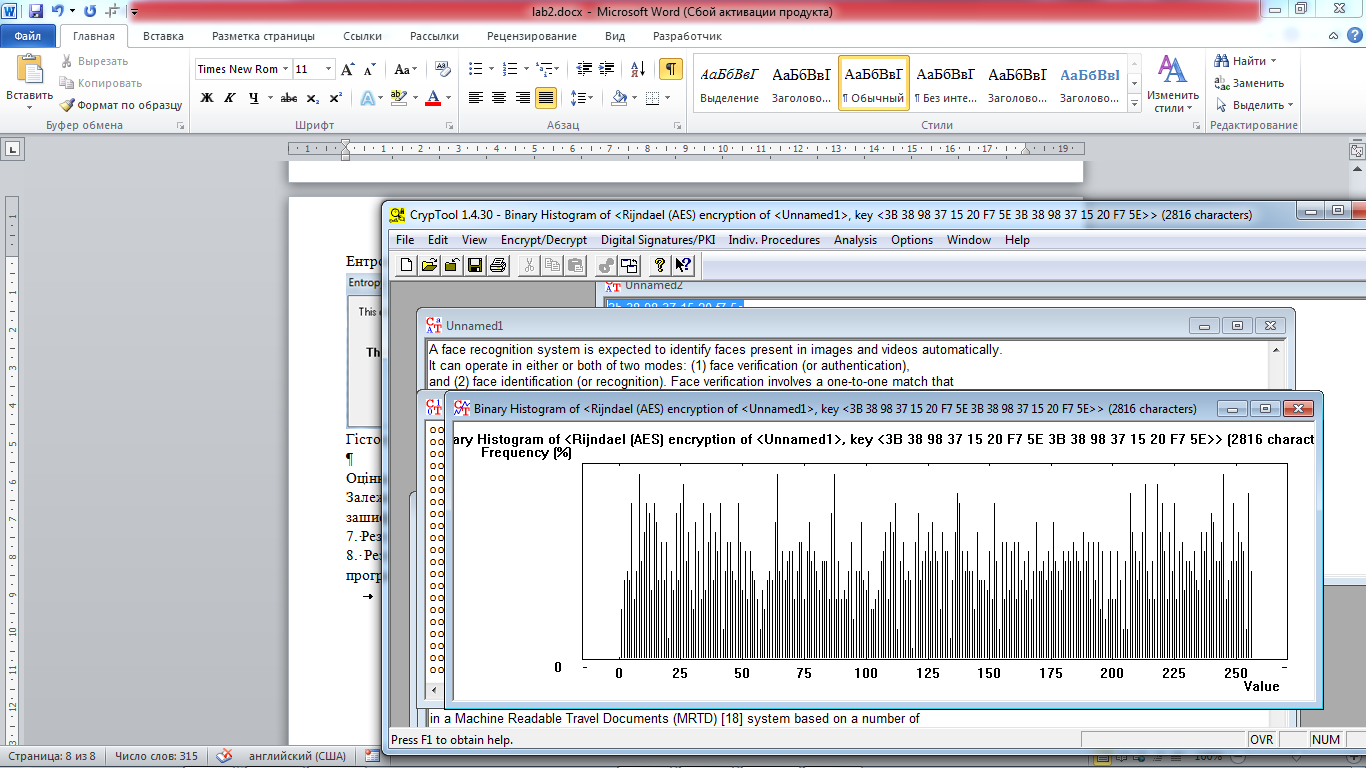
e. AES



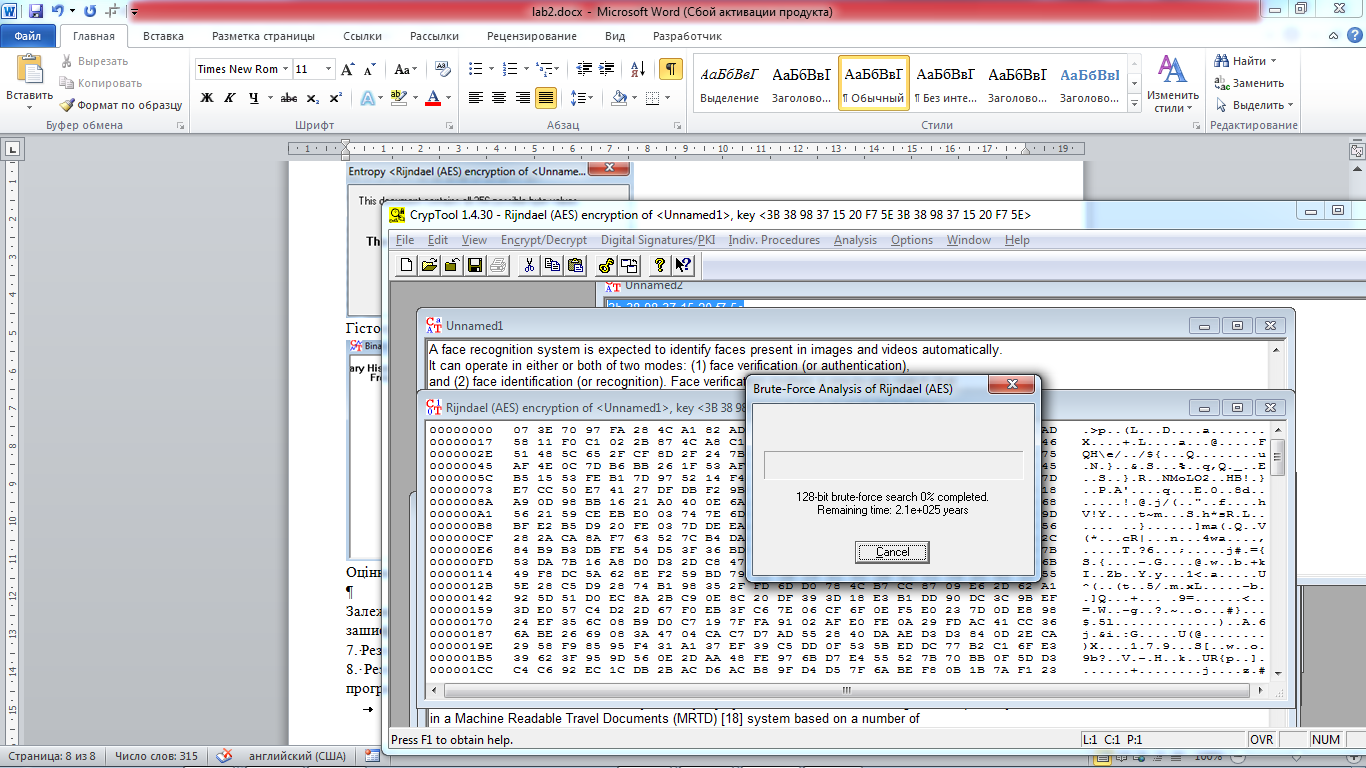
Ентропія, максимально можлива ентропія зашифрованих файлів:



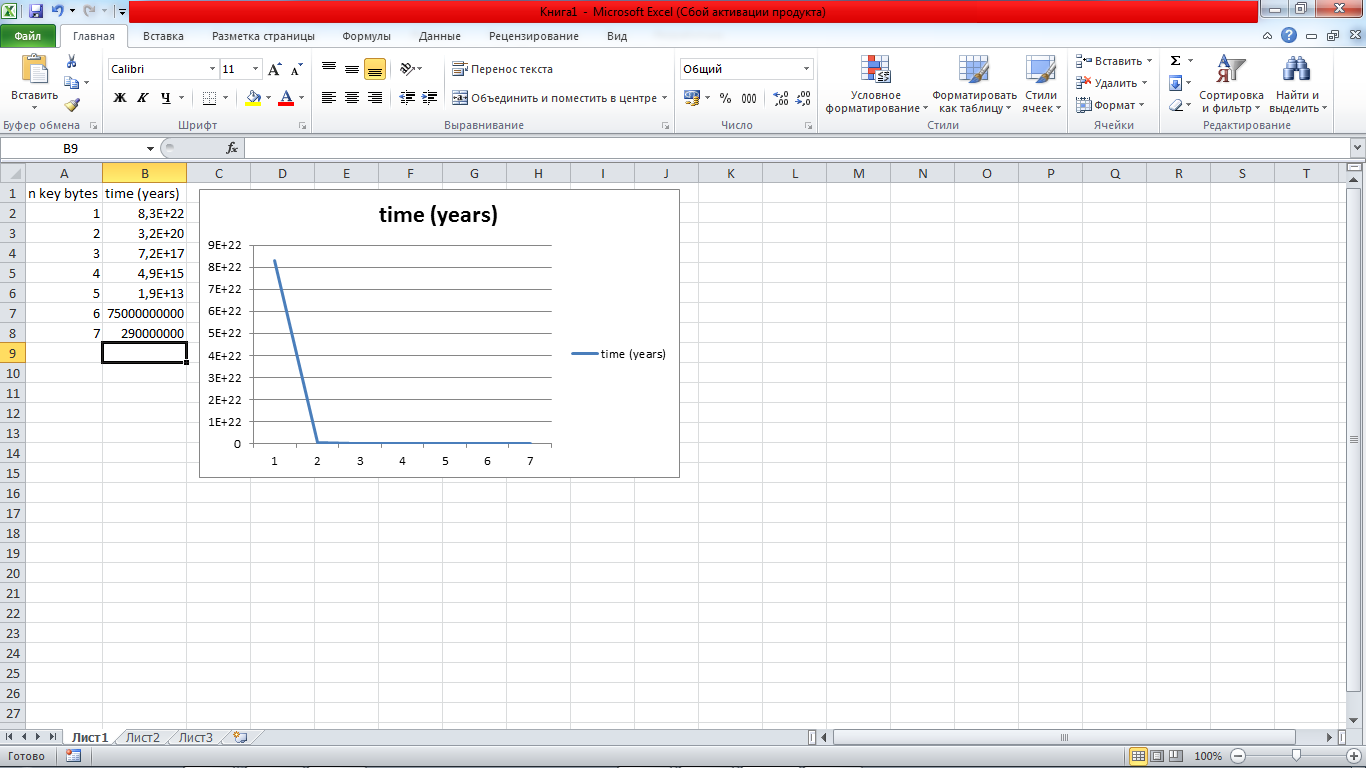
Гістограми розподілу частот символів зашифрованих файлів:



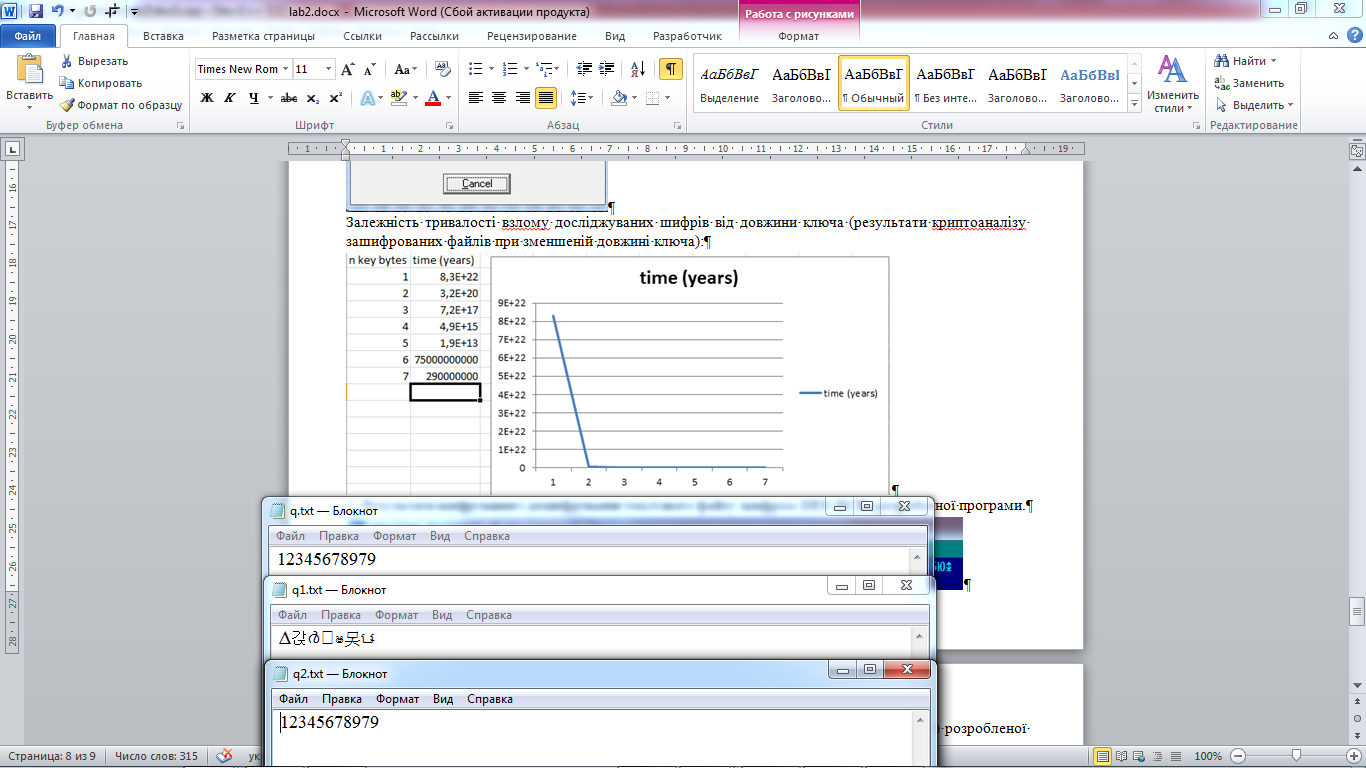
Оцінка часу для взлому зашифрованих фалів методом "грубої сили":

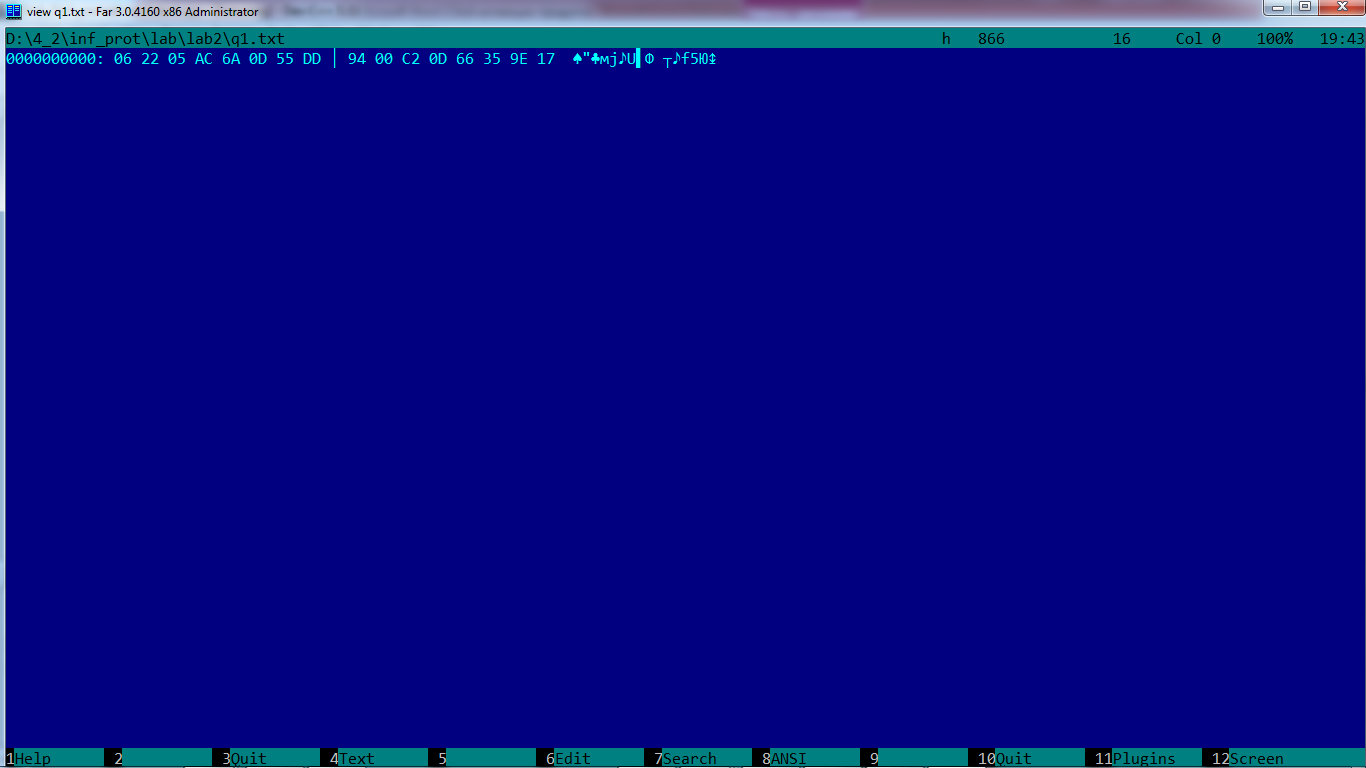


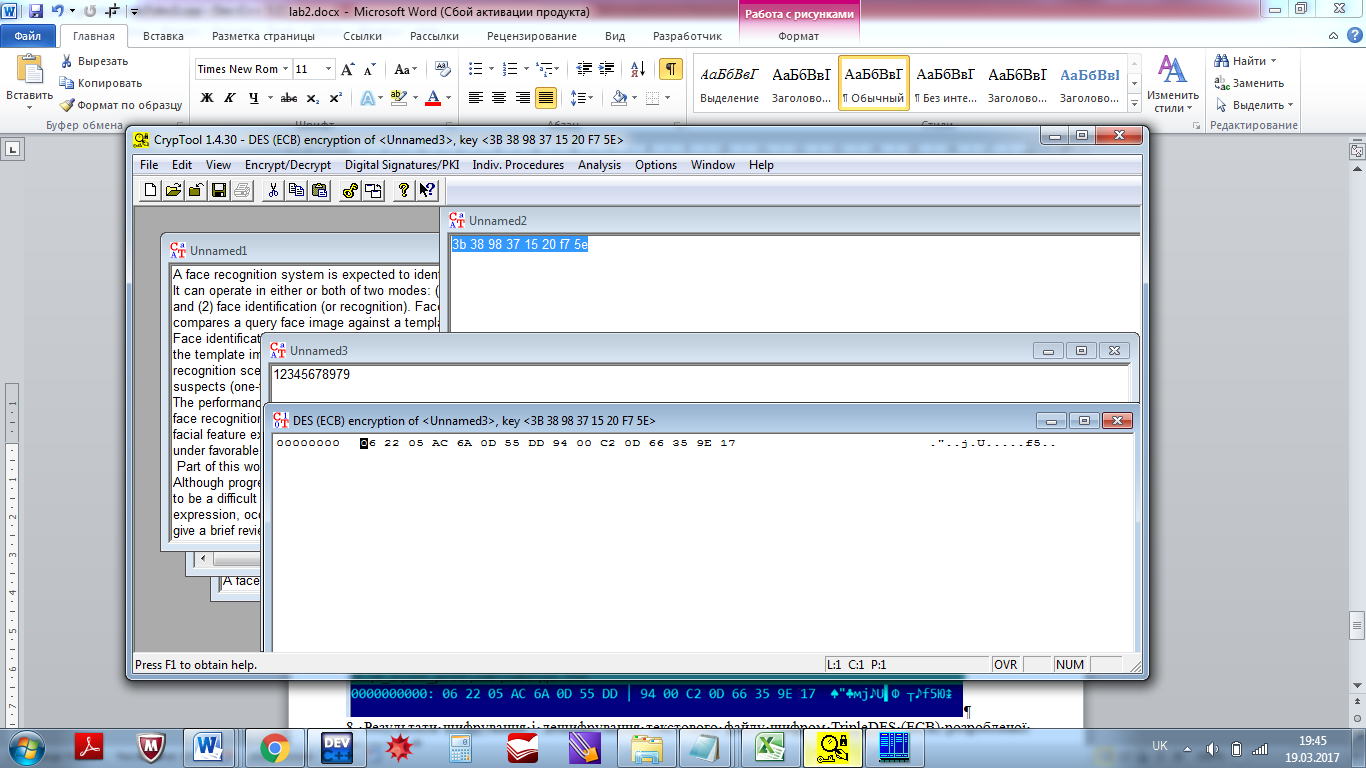
Залежність тривалості взлому досліджуваних шифрів від довжини ключа (результати криптоаналізу зашифрованих файлів при зменшеній довжині ключа):



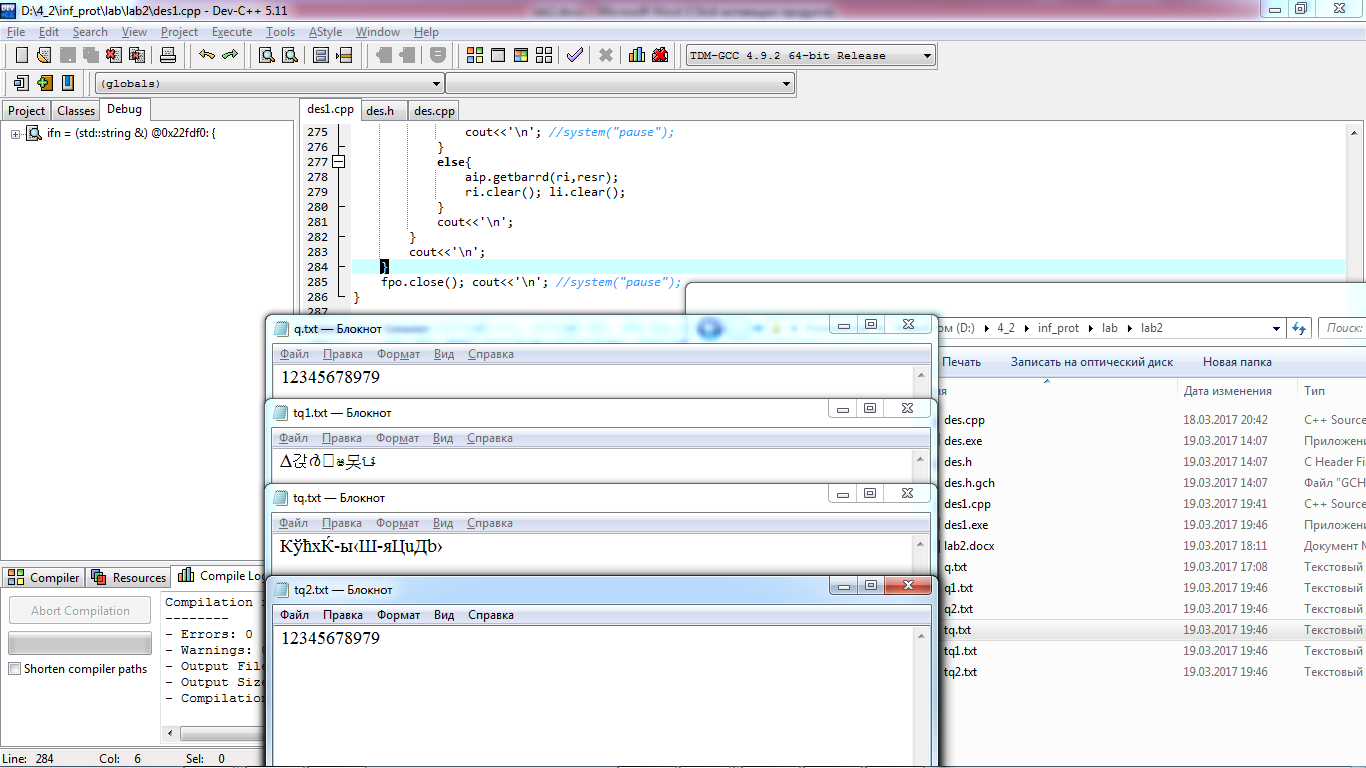
7. Результати шифрування і дешифрування текстового файлу шифром DES (ECB) розробленої програми.







8. Результати шифрування і дешифрування текстового файлу шифром TripleDES (ECB) розробленої програми.



Висновки: на лабораторній роботі розглядалися алгоритми 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.