**Національний технічний університет України  
«Київський політехнічний інститут»**

Інститут Прикладного системного аналізу  
Кафедра Системного проектування

Лабораторна робота № 4

з дисципліни «**ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ**»

# «Дослідження SHA-1. Цифровий підпис. Атака “Днів народження”»

Виконав:

студент групи ДА-82

факультету «ІПСА»

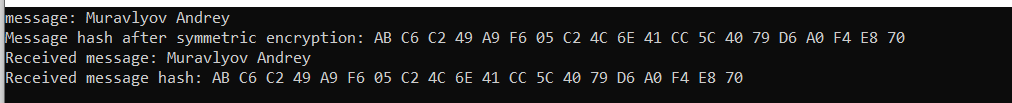
Муравльов А. Д.  
Варіант 17

Київ – 2021

**Хід роботи**

Вихідний код для програми з завдань 1 – 4 доступний за посиланням.

<https://github.com/lakub-muravlov/fourth-course-projects/tree/main/Information_System_Security/Lab4/Code>

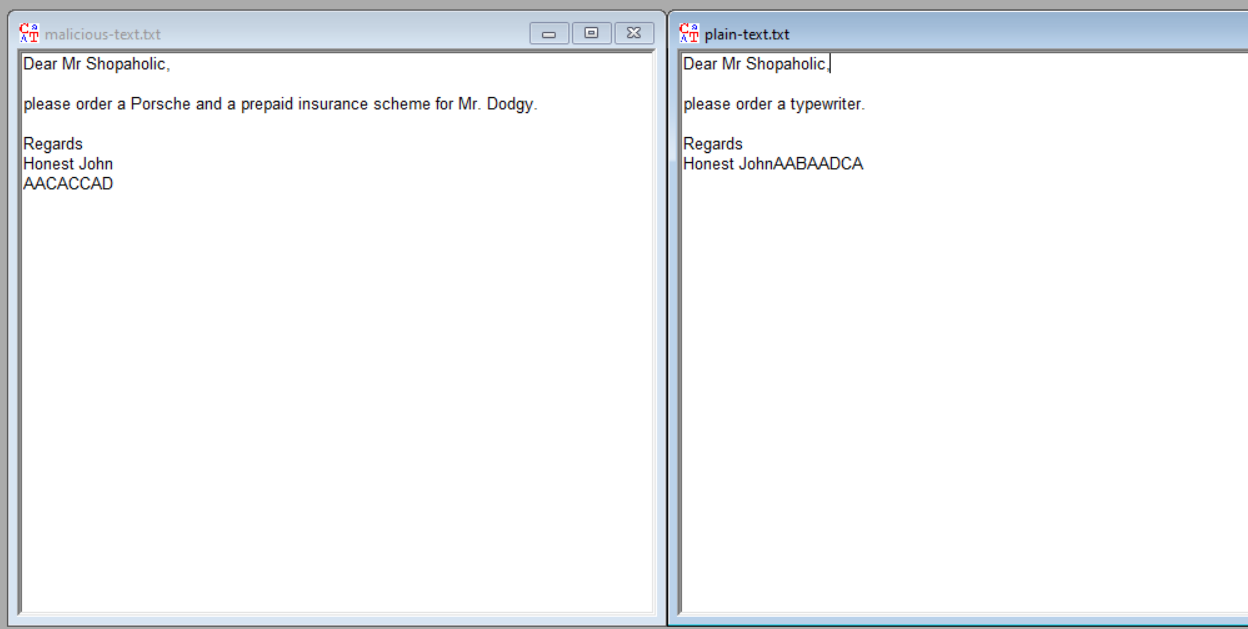


Результат роботи програми

**5. Використати програму CrypTool для реалізації атаки “Днів народження”, самостійно обравши вихідний текст та текст підміни. Кількість символів хешу SHA-1, що має збігтись в тексті обрати за формулою l = [10 + (v + g)%7], де v - номер студента в групі, g - номер групи. Перевірити SHA-1 скорегованих текстів.**

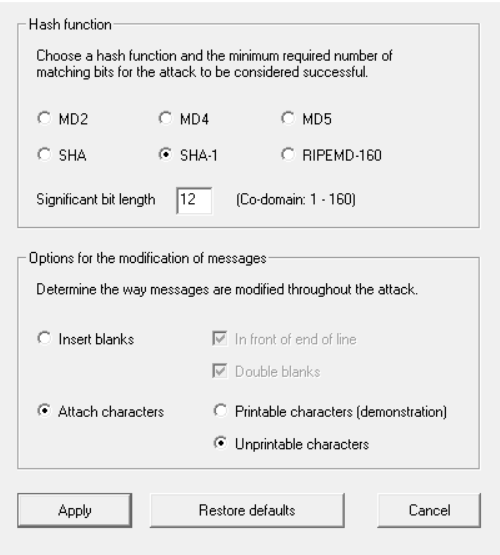
*Кількість символів хешу що мають збігатися l = 10 + (18 + 82) % 7 = 12.*

Для цього завдання можемо скористатись текстами, які пропонуються в пакеті CrypTool за замовчуванням:

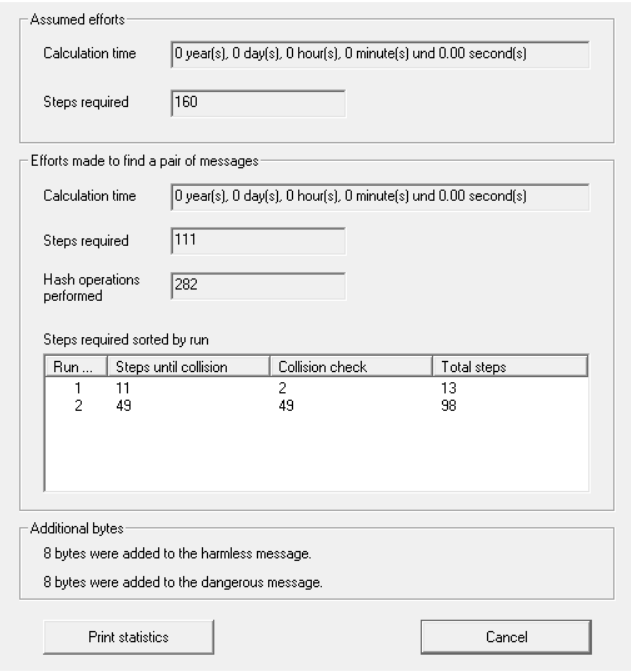


Вихідні тексти

Очевидно, що текст зліва є підробкою.



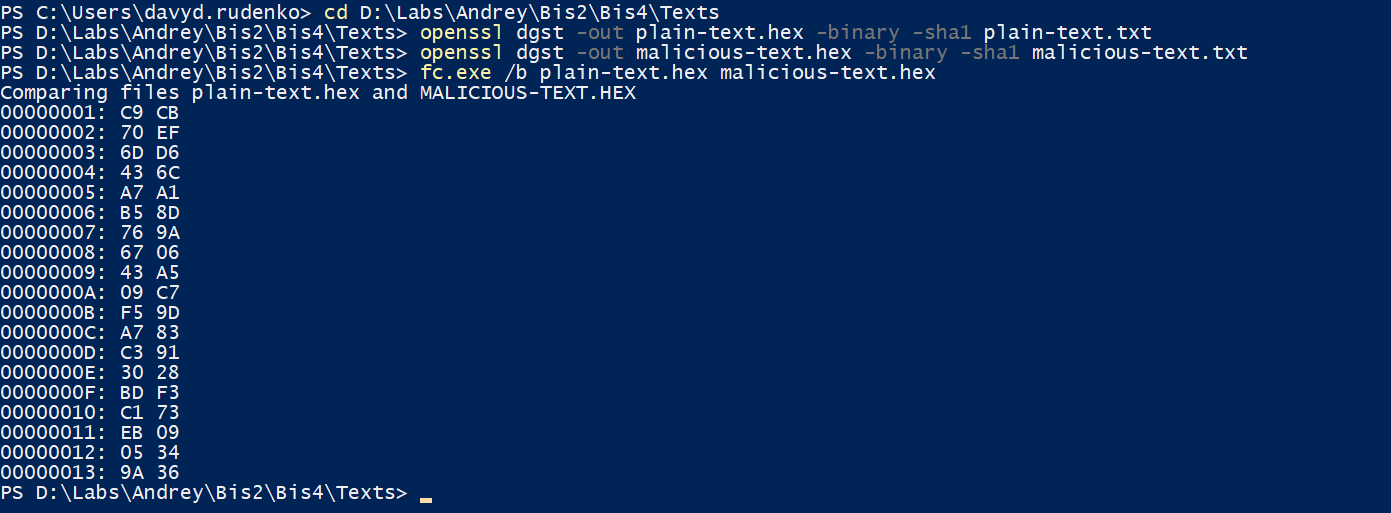
Налаштування злому



Статистика злому

Порівняння хешів двох файлів:

Бачимо, що перші 12 бітів хешів співпадають, як і потрібно було за завданням. Також варто зазначити, що дана атака є вкрай складною обчислювальною задачею – так, якщо нам буде потрібно, щоб хеші співпадали повністю для цього знадобиться 2 x 1093 років обчислень на сучасному персональному комп’ютері.



**Висновки**

В ході роботи я реалізував симуляцію системи, в якій дані передаються з використанням алгоритму комбінованого шифрування на алгоритмах RSA(асиметричне шифрування) та простої підстановки(симетричне шифрування). Також було досліджено механізми хешування, зокрема SHA1 та проведено так звану «атаку днів народження», для якої також було проведено аналіз часу для злому.