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

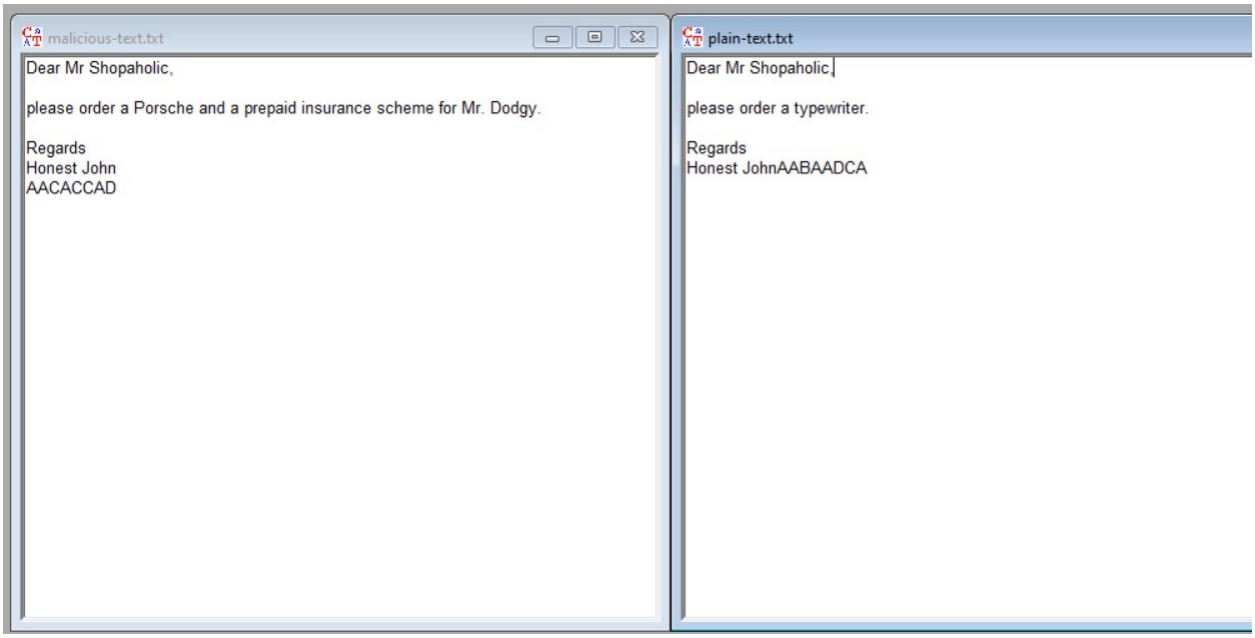
```
message: Muravlyov Andrey
Message hash after symmetric encryption: AB C6 C2 49 A9 F6 05 C2 4C 6E 41 CC 5C 40 79 D6 A0 F4 E8 70
Received message: Muravlyov Andrey
Received message hash: AB C6 C2 49 A9 F6 05 C2 4C 6E 41 CC 5C 40 79 D6 A0 F4 E8 70
```

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.

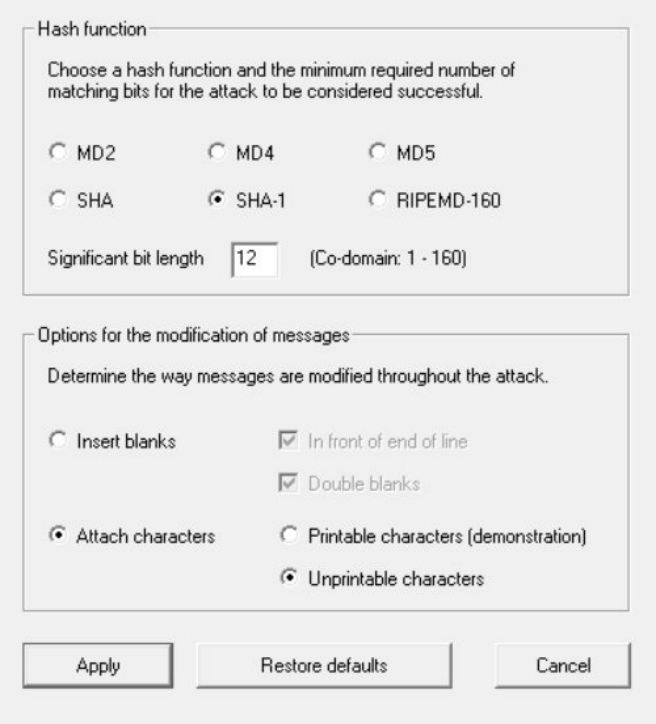
Кількість символів хешу що мають збігатися l = 10 + (18 + 82) % 7 = 12.

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

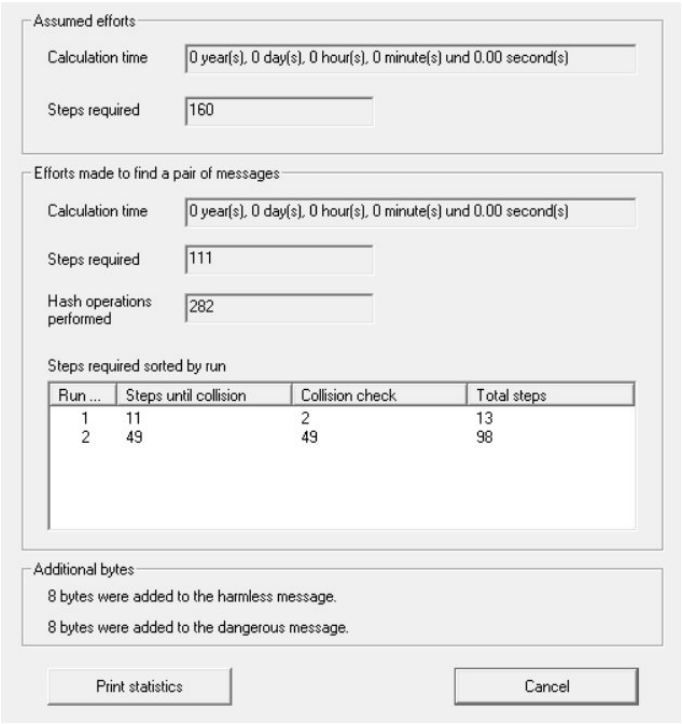


Вихідні тексти

Очевидно, що текст зліва є підробкою.



Налаштування злому



Статистика злому

Порівняння хешів двох файлів:

```
PS C:\Users\davyd.rudenko> cd D:\Labs\Andrey\Bis2\Bis4\Texts
PS D:\Labs\Andrey\Bis2\Bis4\Texts> openssl dgst -out plain-text.hex -binary -sha1 plain-text.txt
PS D:\Labs\Andrey\Bis2\Bis4\Texts> openssl dgst -out malicious-text.hex -binary -sha1 malicious-text.txt
PS D:\Labs\Andrey\Bis2\Bis4\Texts> fc.exe /b plain-text.hex malicious-text.hex
Comparing files plain-text.hex and MALICIOUS-TEXT.HEX
00000001: C9 CB
00000002: 70 EF
00000003: 6D D6
00000004: 43 6C
00000005: A7 A1
00000006: B5 8D
00000007: 76 9A
00000008: 67 06
00000009: 43 A5
0000000A: 09 C7
0000000B: F5 9D
0000000C: A7 83
0000000D: C3 91
0000000E: 30 28
0000000F: BD F3
00000010: C1 73
00000011: EB 09
00000012: 05 34
00000013: 9A 36
PS D:\Labs\Andrey\Bis2\Bis4\Texts>
```

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 2×10^{93} 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.