Міністерство освіти і науки України

Національний технічний університет «ХПІ»

Навчально-науковий інститут комп’ютерних наук та інформаційних технологій

Кафедра комп’ютерної інженерії та програмування

**ЗВІТ**

з лабораторної роботи № 1

з дисципліни «Сучасні технології безпечного програмування»

**«Хешування»**

Виконав:

студент гр. КН-Н922б

Зозуля В.Д.

Перевірив:

доцент кафедри

Бульба С.С.

Харків – 2022

**Мета роботи**: Дослідити принципи роботи хешування.

Як працює алгоритм SHA256:

1. Pre-Processing
2. Initialize Hash Values (h)
3. Initialize Pound Constants (K)
4. Chunk Loop
5. Create Message Schedule (w)
6. Compression
7. Modify final values

**Хід роботи**

1. Pre-Processing. Конвертація рядка в байти.

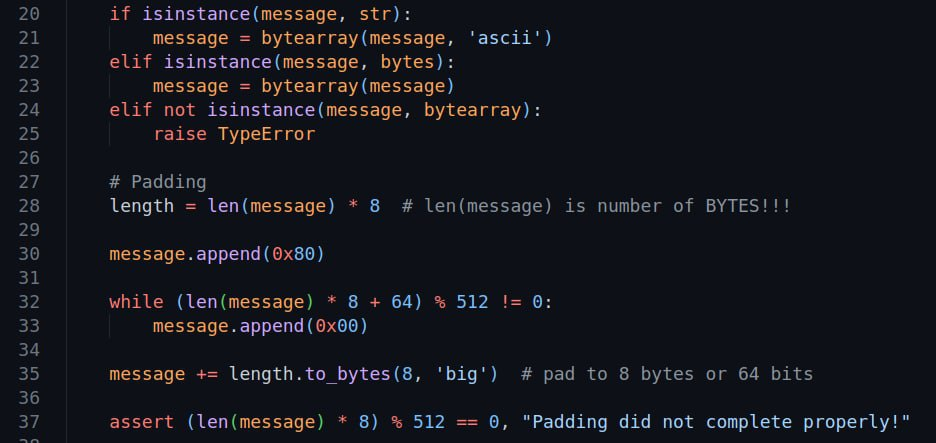


Рисунок 1. Препроцесінг

1. Initialize Hash Values.

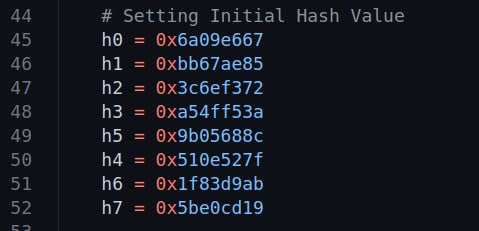


Рисунок 2. Хеш значення

1. Initialize Pound Constants (K).

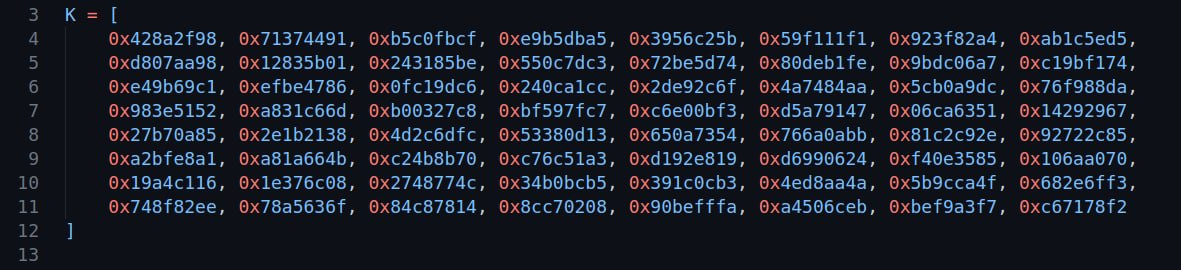


Рисунок 3. Константи

1. Chunk Loop.

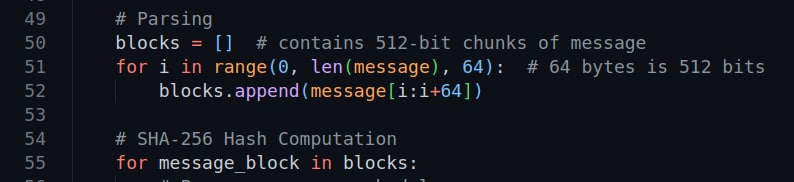


Рисунок 4. Chunk Loop

1. Create Message Schedule (w)

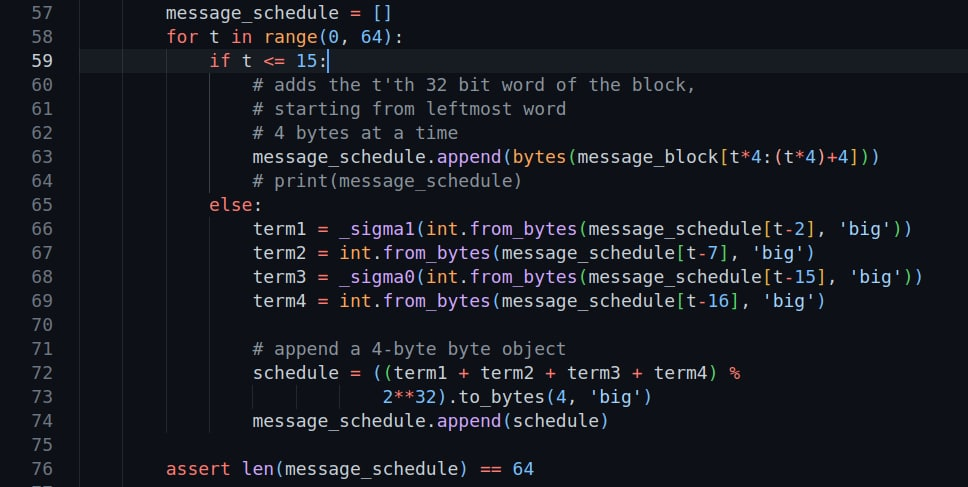


Рисунок 5. Create Message Schedule (w)

1. Compression.

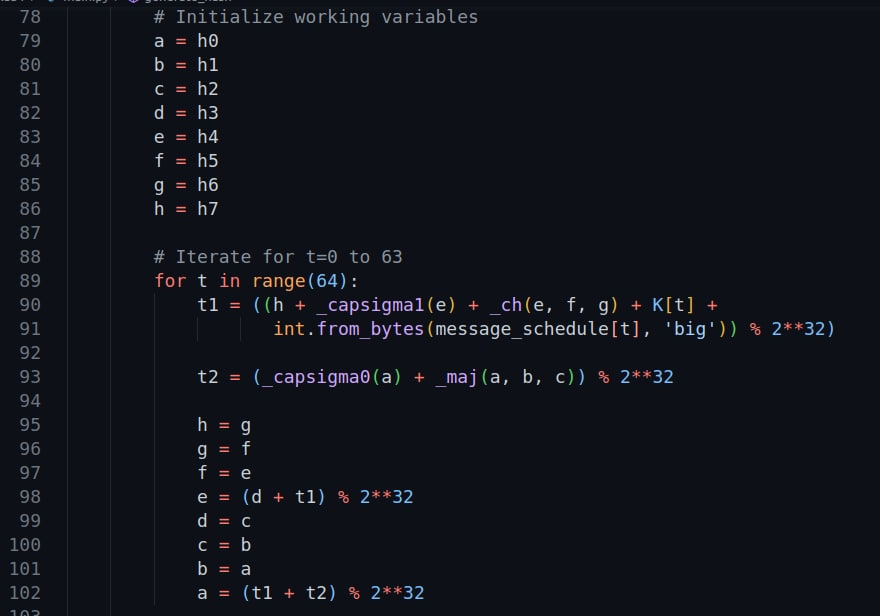


Рисунок 6. Compression

1. Modify final values

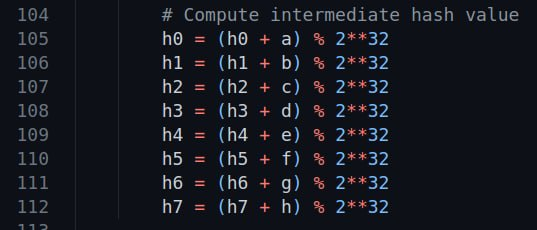


Рисунок 7. Modify final values

**Результат роботи**

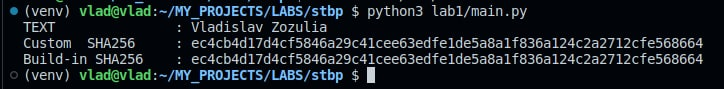


Рисунок 8. Результат роботи програми

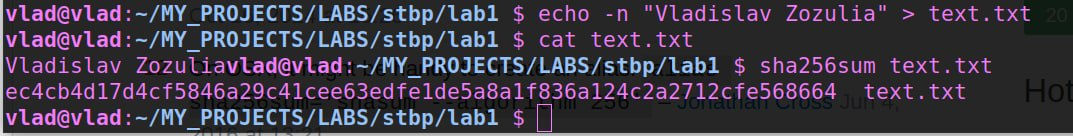


Рисунок 9. Порівняння із командою sha256sum у Linux

**Висновок**

Дослідив принципи роботи хешування.