Науменко Д.

КН 922.а

Лабораторна робота №1

Гешування

Мета : Дослідити принципи роботи гешування

Завдання : Дослідити існуючі механізми гешування. Реалізувати алгоритм гешування SHA (будь-якої версії). Довести коректність роботи реалізованого алгоритму шляхом порівняння результатів з існуючими реалізаціями.

Хід роботи

Найпопулярніші геш-функції на пайтоні є MD5 та SHA.

MD5: Алгоритм виробляє хеш зі значенням 128 бітів. Широко використовується для перевірки цілісності даних. Не підходить для використання в інших областях через вразливість безпеки MD5.

SHA: Група алгоритмів, розроблених NSA Сполучених Штатів. Вони є частиною Федерального стандарту обробки інформації США. Ці алгоритми широко використовуються у кількох криптографічних додатках. Довжина повідомлення варіюється від 160 до 512 біт.

Модуль hashlib, застосований у стандартну бібліотеку Python, є модуль, що містить інтерфейс для найпопулярніших алгоритмів хешування. Hashlib реалізує деякі алгоритми, однак, якщо у вас встановлено OpenSSL, hashlib також може використовувати ці алгоритми.

```
import hashlib

hash_obj = hashlib.sha1(b'Dmitriy')
hex_dig = hash_obj.hexdigest()

print(hex_dig)
```

Початковий код написан на пайтоні за допомогою інтегрованої бібліотеки hashlib, яка має можливість гешування різних типів.

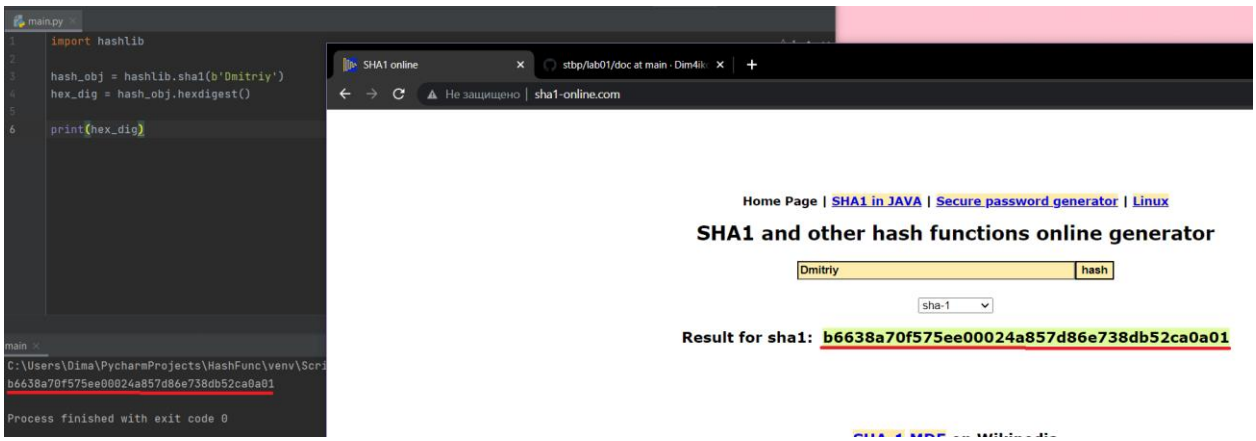

Рис. 1 – Результат.

Як бачимо, гешування виконано правильно. Остаточний результат співпадає с перевірочним сервісом.

Висновок : під час виконання лабораторної роботи я дослідив існуючі механізми гешування. Реалізував алгоритм гешування SHA (будь-якої версії). Довів коректність роботи реалізованого алгоритму шляхом порівняння результатів з існуючими реалізаціями.