

РЕАЛІЗАЦІЯ КРИПТОАЛГОРИТМУ ХЕШУВАННЯ SHA256

IMPLEMENTATION OF THE SHA256 HASHING CRYPTO ALGORITHM

Реалізація мовою Python містить чотири модулі: «binary_operations», «encoding», «SHA256», «main». Їх призначення такі:

– в першому модулі реалізовані операції над двійковими рядками (векторами) - операція побітового виключного або, циклічного зсуву вправо, логічного зсуву вправо, двійкового додавання двох векторів за модулем 2^{32} , операція побітового «І», операція побітового заперечення;

– у другому модулі були реалізовані методи кодування - перетворення текстового рядка в бінарний рядок кодування UTF8, переведення цілого десяткового числа в двійкове подання у вигляді рядка, переведення рядка двійкового подання у рядок шістнадцяткового подання;

– у третьому модулі було реалізовано клас, що містить функціонал хеш-функції. При створенні екземпляра класу відбувалася ініціалізація констант. Було реалізовано метод «hash_data», який приймає вхідний текстовий рядок. У ньому відбувалося початкове скидання констант (щоб забезпечити правильне хешування за нового виклику даного методу), після чого проводився алгоритм хешування, описаний у попередньому розділі. Наприкінці отриманий результат переводився в шістнадцяткову форму і повертався;

– в останньому модулі знаходиться точка входу в програму, в якій створювався рядок і подавався на вхід функції хешування.

Для перевірки коректності алгоритму було здійснено порівняння для пробного тексту, що містить 7965 символів. Як «еталонна» реалізація використовувалася реалізація SHA256 у бібліотеці «hashlib» [1]. Результати наведено на рис. 1. На ньому зображені підсумкові значення змінних у шістнадцятковій і двійковій формі. Далі вказана їхня конкатенація – результат алгоритму SHA256. В останньому рядку вказано результат хешування ««hashlib.sha256»».

```
h0 = 082012D9 = 00001000001000000001001011011001
h1 = 52CBDD03 = 01010010110010111101110111010011
h2 = 03728F4B = 00000011011100101000111101001011
h3 = 7AAF36FF = 01111010101011110011011011111111
h4 = 698496A9 = 01101001100001001001011010101001
h5 = 20B4E904 = 00100000101101001110100100000100
h6 = 599F1BA5 = 01011001100111110001101110100101
h7 = 8F28EE76 = 10001111001010001110111001110110
082012D952CBDD0303728F4B7AAF36FF698496A920B4E904599F1BA58F28EE76
082012D952CBDD0303728F4B7AAF36FF698496A920B4E904599F1BA58F28EE76
```

Рисунок 1. Результати роботи власної реалізації SHA256 та бібліотеки «hashlib»

Література

1. Hashlib — Secure hashes and message digests. [Електронний ресурс] – Режим доступу: <https://docs.python.org/3/library/hashlib.html> (дата звертання: 08.11.24).