УДК 004.02

МАРЧИШИН І. А.

ПОРІВНЯННЯ ЕФЕКТИВНОСТІ АЛГОРИТМІВ ХЕШУВАННЯ

Вінницький національний технічний університет

Анотація
У роботі проаналізовано ефективність алгоритмів хешування.
Ключові слова: алгоритми, хешування, ефективність, SHA-1, SHA-256.

Abstract
This research thesis analyzes the effectiveness of hashing algorithms.
Keywords: algorithms, hashing, efficiency, SHA-1, SHA-256.

Вступ

Наразі, в сучасному світі криптографії та кібербезпеки, є доволі багато різних алгоритмів хешування, кожен з яких відрізняється своєю ефективністю, стійкістю до колізій та об'ємами даних, з якими вони можуть працювати. Ці алгоритми використовуються для різних потреб: від побудови унікальних ідентифікаторів [1] для наборів даних до зберігання паролів у системах захисту [1]. У цій роботі, на практиці, проаналізовано ефективність двох алгоритмів хешування, а саме: SHA-1 [1] та SHA-256 [2].

Аналіз роботи алгоритмів

За для перевірки ефективності та стійкості алгоритмів SHA-1 та SHA-256, було проведено експерименти, реалізовані за допомогою мови програмування Python. Було використано кілька різних розмірів хеш-таблиць та рівнів заповнення, щоб оцінити результати роботи кожного алгоритму та виявити можливі колізії. Отримані результати представлені в порівняльній таблиці та відображені на графіку.

Таблиця 1. Порівняльна таблиця експериментальних даних та результатів експериметну

Розмір таблиці	Коефіцієнт заповнення (%)	Колізії SHA-1	Колізії SHA-256
100.000	50	0	0
300.000	90	1	1
550.000	90	1	0
650.000	100	3	0
1.000.000	100	4	2
1.500.000	100	9	4
1.800.000	100	10	5

Варто зазначити, що наведені результати є лише експериментальними і слугують для загального порівняння алгоритмів. Вони можуть варіюватися при кожному виконанні тесту. Різні генерації випадкових даних можуть призводити до різних результатів, тому не можна гарантувати однакові показники колізій для кожного запуску програми.

На наведеному нижче графіку (рис. 1) відображено результати тестування виникнення колізій для алгоритмів хешування SHA-1 та SHA-256 при різних розмірах хеш-таблиці та коефіцієнтах заповнення.

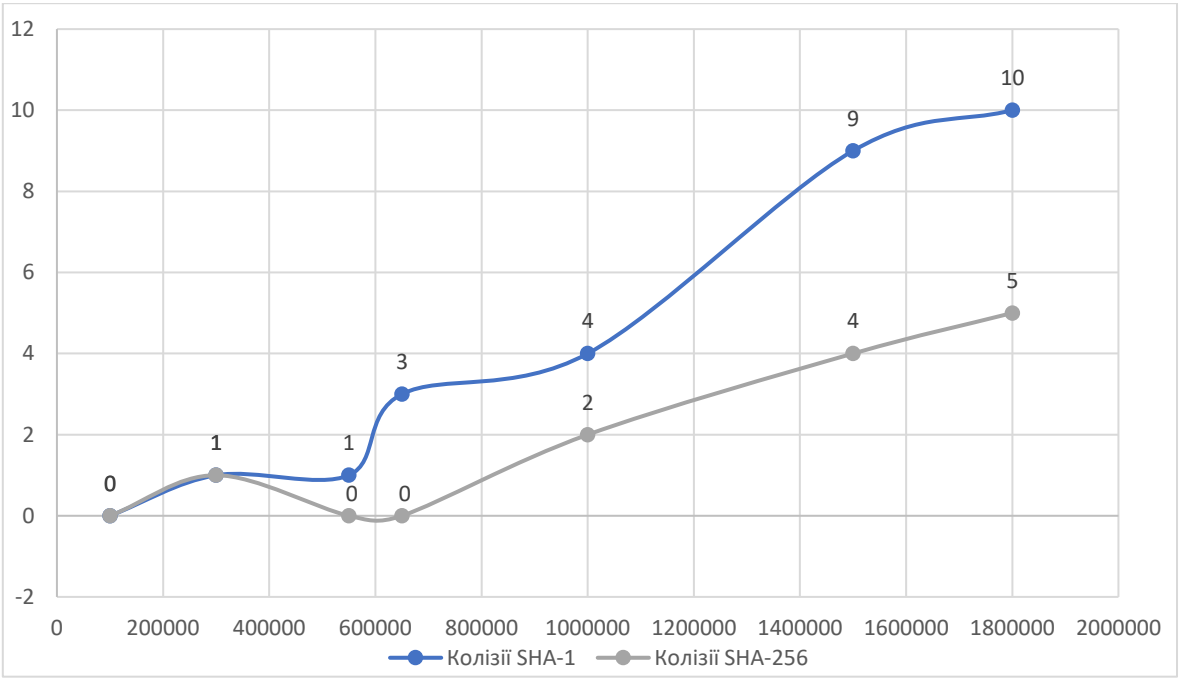

Рис. 1. Графічне відображення виникнення колізій у алгоритмах хешування SHA-1 та SHA-256

На графіку можна побачити, що при заповненні таблиць на 50% колізії відсутні для обох алгоритмів. Однак, при збільшенні заповнення до 90% та 100%, кількість колізій починає зростати. Наприклад, для таблиці розміром у 650.000 записів при повному заповненні алгоритм SHA-1 генерує 3 колізії, тоді як SHA-256 не створює жодної. При розмірах таблиць 1.000.000 і більше, видно, що обидва алгоритми починають генерувати колізії, але SHA-256 залишається більш ефективним.

Висновки

У результаті порівняння алгоритмів хешування SHA-1 та SHA-256 продемонстровано, що SHA-256 є більш надійним, демонструючи меншу кількість колізій при різних розмірах хеш-таблиць та рівнях заповнення. Це робить SHA-256 кращим вибором для застосувань, де потрібна висока криптографічна стійкість та мінімізація колізій, але потрібно враховувати, що все залежить від конкретних потреб та ситуацій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Wikipedia. “SHA-1” [https://uk.wikipedia.org/wiki/SHA-1]
2. Wikipedia. “SHA-2” [https://uk.wikipedia.org/wiki/SHA-2]

Марчишин Іван Андрійович — студент групи 5ПІ-23б, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: onemarc0101@gmail.com

Marchyshyn Ivan A. — Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: onemarc0101@gmail.com

Ткаченко Олександр Миколайович — к.т.н., доцент кафедри програмного забезпечення, Вінницький національний технічний університет.

Oleksandr Tkachenko — Cand. Sc. (Eng.), assistant professor of the Software Chair, Vinnytsia National Technical University, Vinnytsia, alextk1960@gmail.com.