6. Ростока М. Л. Виставкова діяльність у контексті інформаційно-аналітичного супроводу модернізації національної освіти / М. Л. Ростока, В. В. Кушнір // Науковий вісник Ужгородського університету. Серія: Педагогіка. Соціальна робота. 2022. Вип. 2. С. 122-126. Режим доступу: http://nbuv.gov.ua/UJRN/Nvuuped_2022_2_27.
7. Туровська Л. Електронна виставка як комунікаційна модель діяльності наукової бібліотеки / Л. Туровська, І. Смоляр // Вісник Книжкової палати. 2015. № 3. С. 29-31. Режим доступу: http://nbuv.gov.ua/UJRN/vkp_2015_3_9.

МАРЧИШИН І. А.,
ТКАЧЕНКО О.М.,
ВНТУ,

АНАЛІЗ РОБОТИ АЛГОРИТМІВ ХЕШУВАННЯ SHA-384 ТА SHA-512

Анотація. У роботі проаналізовано ефективність роботи алгоритмів хешування.
Ключові слова: алгоритми, хешування, ефективність, SHA-384, SHA-512.
Abstract. This research thesis analyzes the effectiveness of hashing algorithms.
Keywords: algorithms, hashing, efficiency, SHA-384, SHA-512.

Вступ. У сучасному світі криптографії 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-384 [1] та SHA-512 [1].

Аналіз роботи алгоритмів

Щоб проаналізувати ефективність та стійкість алгоритмів SHA-384 та SHA-512, 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 у порівняльній таблиці та відображені на графіку.

Таблиця 1. Порівняльна таблиця експериментальних даних та результатів експериметну

Розмір таблиці	Коефіцієнт заповнення (%)	Колізії SHA-384	Колізії SHA-512
500.000	50	0	0
500.000	90	1	0
650.000	90	1	0
750.000	90	3	2
1.000.000	100	1	1
1.500.000	100	7	6
2.000.000	100	14	10

Варто зауважити, що наведені результати є лише експериментальними і слугують для загального порівняння алгоритмів. Вони можуть змінюватись 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-384 та SHA-512 при різних розмірах хеш-таблиці та коефіцієнтах заповнення.

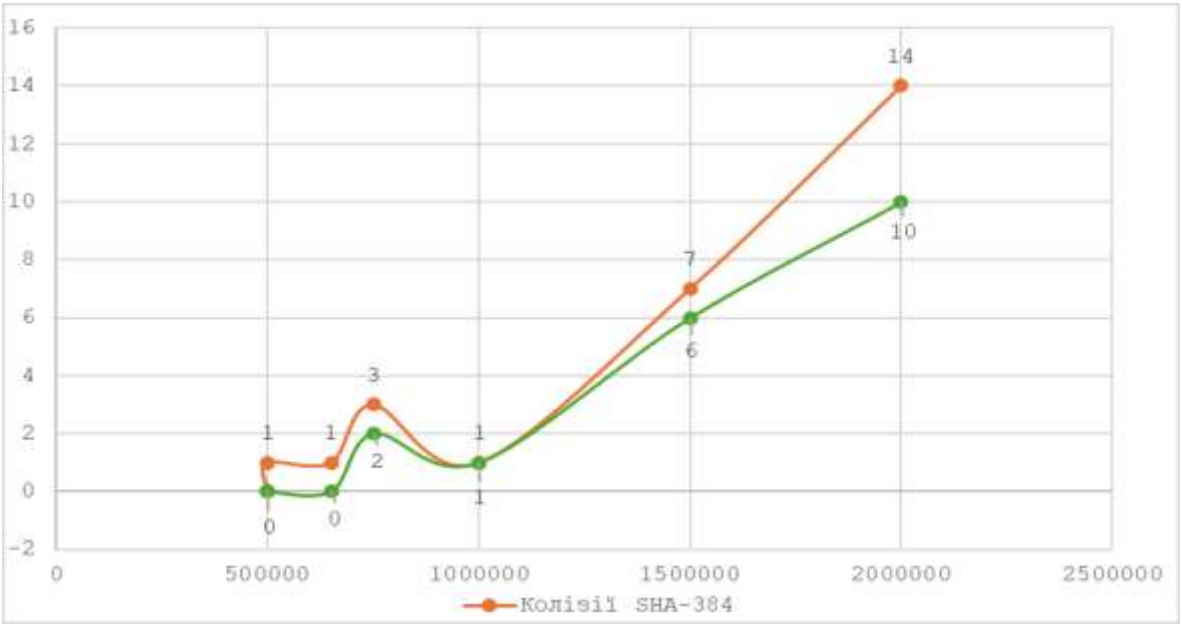

Рис. 1. Графічне відображення виникнення колізій у алгоритмах хешування SHA-384 та SHA-512

На вище зображеному 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 750.000 записів при повному заповненні алгоритм SHA-384 генерує 3 колізії, тоді як SHA-512 лише 2. При розмірах таблиць 1.500.000 і більше, видно, що обидва алгоритми починають працювати приблизно однаково, але SHA-512 залишається більш ефективним.

Висновки

Отже, порівнюючи алгоритми хешування SHA-384 та SHA-512 продемонстровано, що SHA-512 є більш надійним, демонструючи меншу кількість колізій при різних розмірах хеш-таблиць та рівнях заповнення. Це робить SHA-512 кращим вибором для використання в тих випадках, де потрібна висока криптографічна стійкість та мінімізація колізій, але потрібно враховувати, що все залежить від конкретних потреб застосування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

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

МЕЛЕНЧУК Л.І.,
ГАВРИШКІВ Н.Г.,
СЛЄПЦОВА О.Я.
Галицький фаховий коледж ім.В.Чорновола

ВИКОРИСТАННЯ РІЗНОРІВНЕВИХ ЗАВДАНЬ ПРИ ДИСТАНЦІЙНОМУ НАВЧАННІ, ЯК КЛЮЧ ДО ІНДИВІДУАЛІЗАЦІЇ

Анотація: стаття розглядає використання різнорівневих завдань як ефективний спосіб індивідуалізації навчання в умовах дистанційної освіти. Обґрунтовується важливість такого підходу для підвищення мотивації здобувачів освіти, розвитку їхніх пізнавальних здібностей та запобігання академічним невдачам. Пропонуються практичні рекомендації щодо створення та застосування різнорівневих завдань, а також описуються використання сучасних технологій для організації індивідуалізованого навчання.

Ключові слова: дистанційне навчання, різнорівневі завдання, індивідуалізація, індивідуалізоване навчання, критичне мислення.

Зростання темпу життя та великий потік інформації змушують людину оперативно знаходити рішення, використовуючи пошукові навички та працюючи з різноманітними джерелами. У цьому