Лабораторна робота. Порівняння даних за допомогою хешу

Цілі та задачі

Використати програму хешування для перевірки цілісності даних.

1. Довідкова інформація/Сценарій

Важливо виявляти, пошкодження або підмінену дані. Програма хешування може бути використана для перевірки, чи змінилися дані, чи вони залишилися незмінними. Програма хешування виконує хеш-функцію на даних або файлі, та повертає значення (як правило, набагато коротше) . Є багато різних хеш-функцій, деякі дуже прості, а деякі дуже складні. Коли однакова хеш-функція виконується з однаковими даними, то значення, що повертається, завжди однакове. Якщо з даними відбуваються будь-які зміни, то повернене значення хешу буде іншим.

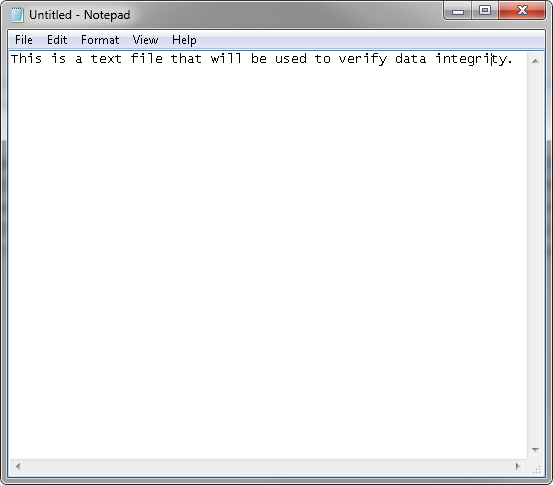
**Примітка**: Для встановлення Windows програм вам знадобляться відповідні привілеї та деякі знання.

1. Необхідні ресурси

* ПК з доступом до Інтернету

Крок 1: Створіть текстовий файл

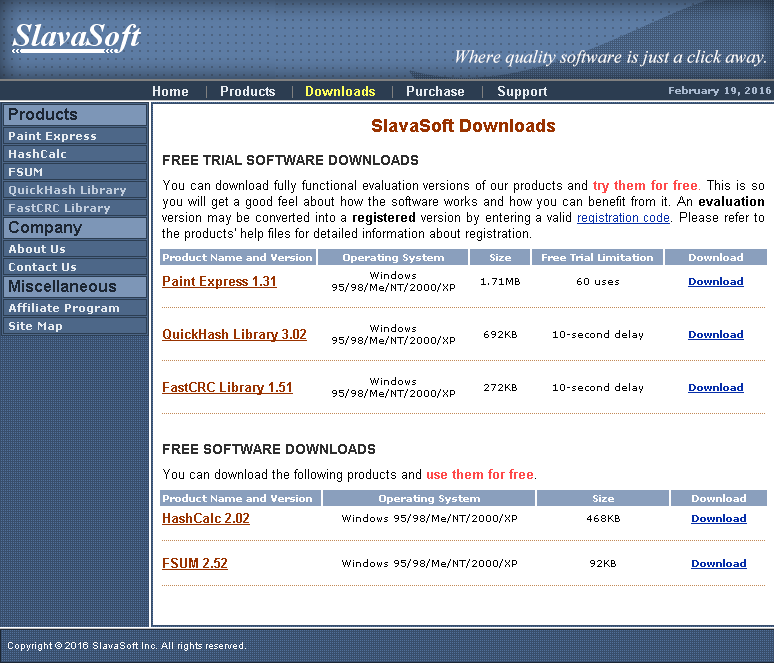
* + 1. Знайдіть на своєму комп'ютері програму Блокнот (Notepad) і відкрийте її.
    2. Введіть текст у програмі.



* + 1. Виберіть **Файл> Зберегти (File > Save)**.
    2. Перейдіть до **Робочого столу**
    3. Введіть**Hash** у поле **Ім'я файлу: (File name:)**і натисніть **Зберегти (Save)**.

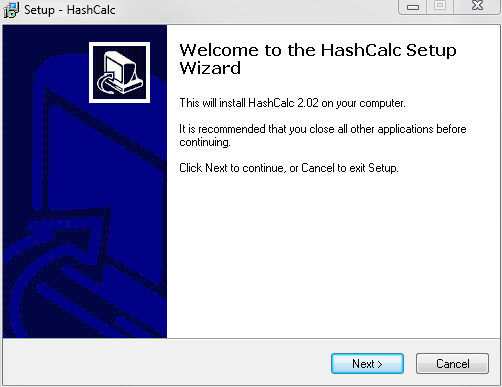
Крок 2: Встановіть HashCalc

a Відкрийте веб-браузер і перейдіть за посиланням <http://www.slavasoft.com/download.htm>.



b Натисніть **Завантажити (Download)** у рядку **HashCalc**.

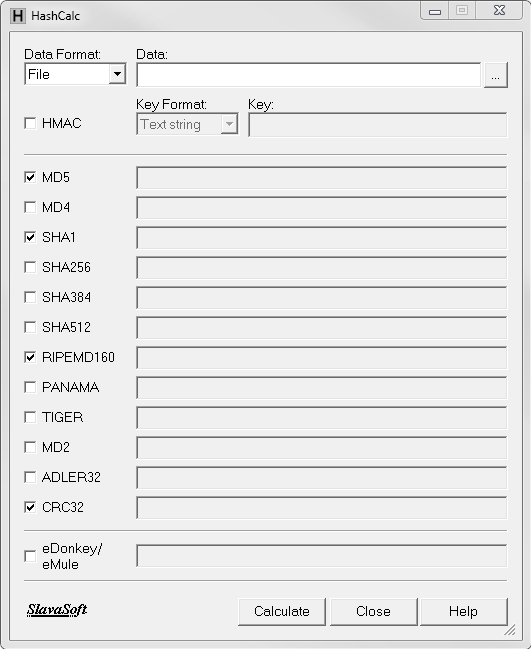
c Відкрийте **hashcalc.zip** файл та запустіть файл **setup.exe** всередині.



d Дотримуйтесь вказівок Майстра установки (Іnstallation wizard), щоб встановити HashCalc.

e Натисніть кнопку **Готово (Finish)** на останньому екрані та закрийте файл **README**, якщо він відкритий. Ви можете прочитати файл, якщо захочете.

g HashCalc тепер встановлено та запущено.



Крок 3: Обчисліть хеш файлу Hash.txt

* + 1. Вкажіть наступні елементи у HashCalc:
       1. Формат даних (Data Format): **Файл (File)**.
       2. Дані: натисніть **...**Поруч із полем Дані (Data), перейдіть на **Робочий стіл (Desktop)**і виберіть файл**Hash.txt**.
       3. Зніміть прапорець **HMAC**
       4. Зніміть усі типи хешів, крім **MD5**
    2. Натисніть кнопку **Обчислити (Calculate)**.

Яке значення поряд із **MD5**?.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Крок 4: Внесіть зміни у файлі Hash.txt

* + 1. Перейдіть на **Робочий стіл** і відкрийте файл **Hash.txt**.
    2. Зробіть невелику зміну тексту, наприклад, видалення літери або додавання пробілу.
    3. Натисніть **Файл> Зберегти (File > Save)** та закрийте **Блокнот**.

Крок 5: Обчисліть новий хеш файлу Hash.txt

* + 1. Знову натисніть кнопку **Обчислити (Calculate)** в HashCalc.

Яке значення поряд із **MD5**?.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Чи значення відрізняється від значення, що одержано на кроці 3?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Поставте прапорець біля усіх типів хеш-функцій.
    2. Натисніть **Обчислити (Calculate)**
    3. Зверніть увагу, що багато типів хеш-функцій створюють хеш різної довжини. Чому?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_