Звіт

До практичного заняття №3-4

З теми: «Хеш-функції та перевірка цілісності інформації»

Підготував:

Студент групи МІТ-21

Чорноконь Денис

1. Написати програму, яка обчислює хеш-коди за всіма відомими алгоритмами для заданих даних. Порівняти розміри хеш-кодів та значення для однакових та різних даних. Зробити висновки.

2. Відомо, що користувач використав для пароля довжиною 8 символів лише цифри. Шляхом пасивного прослуховування мережі отримано MD5 хеш-код цього пароля: {564c8da6-0440-88ec-d453-0bbad57c6036} та po1MVkAE7IjUUwu61XxgNg== Відновити пароль користувача та зробити висновки про надійність такого пароля.

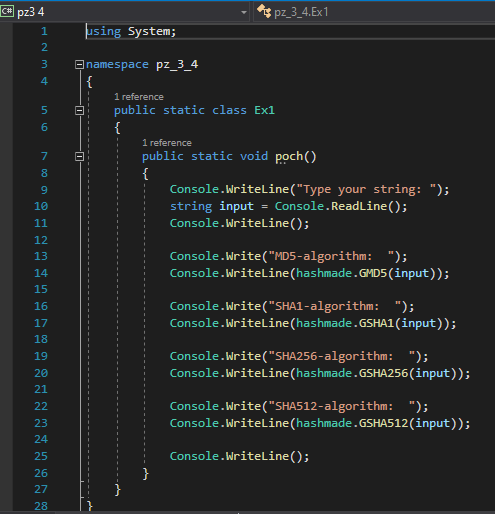
3. Написати програму для обчислення хеш-коду автентифікації повідомлення а також реалізувати можливість перевірки автентичності повідомлення.

4. Написати програму для реєстрації користувача за логіном/паролем та авторизації шляхом співставлення відповідних логінів і паролів. Зберігання пароля у відкритому вигляді неприпустиме.

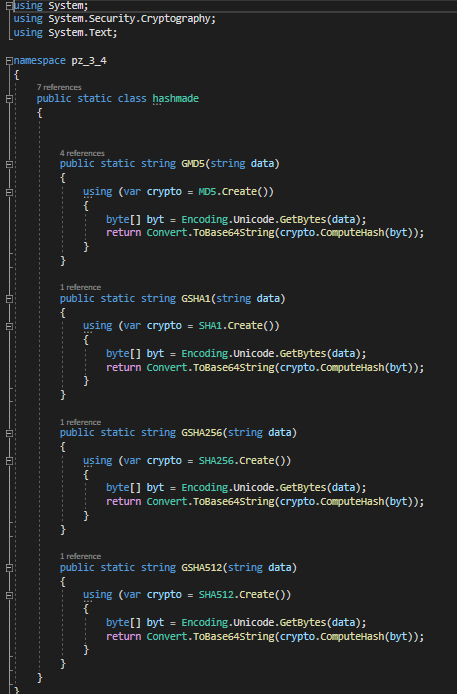
**Хід роботи**

Завдання 1.

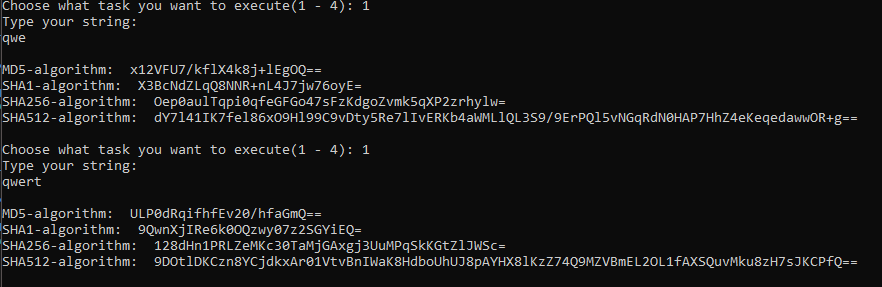
Організовано вивід:



Створено хешування:

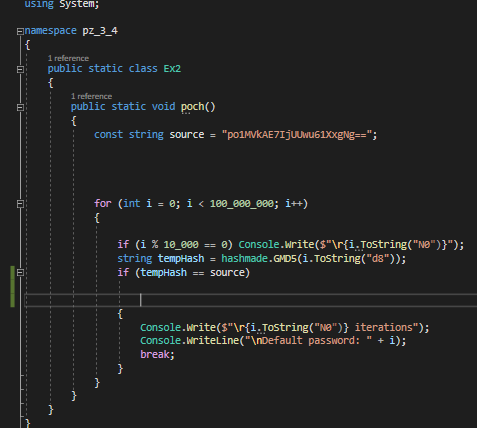


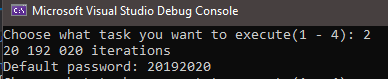
Порівняно розмір хешу при хешуванні:



Отже, розмір хешу залежить від алгоритму хешування, та не залежить від об’єму даних.

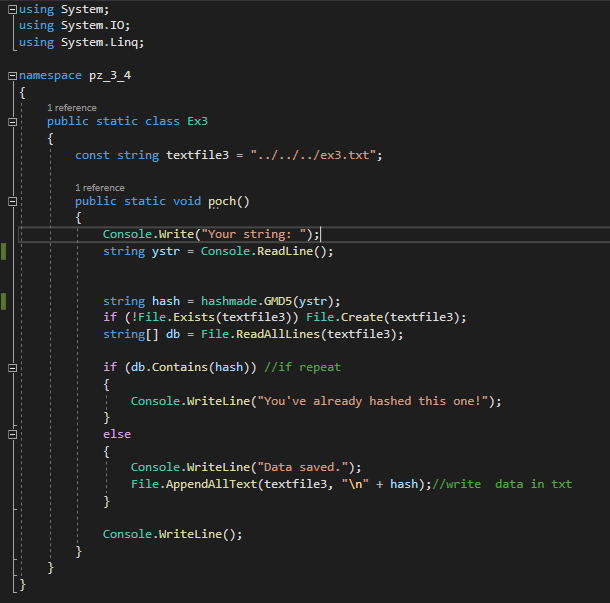
**Завдання 2**. Програма по відновленню пароля та підрахунку кількості ітерацій, для подальшого визначення його надійності.



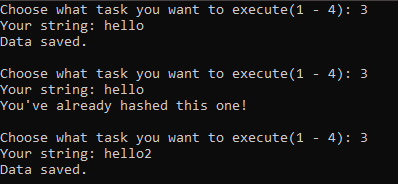


Отже, можна зробити висновок, що пароль, складений тільки з цифр не є надійним, і його відновлення було легше та швидше ніж пароля з літерами.

Завдання 3. Створено текстовий файл для хешу.  
Введені дані хешуються, перевіряються на ідентичність, та заносяться в попередньо створений файл.



Ось, що виводиться на консоль:

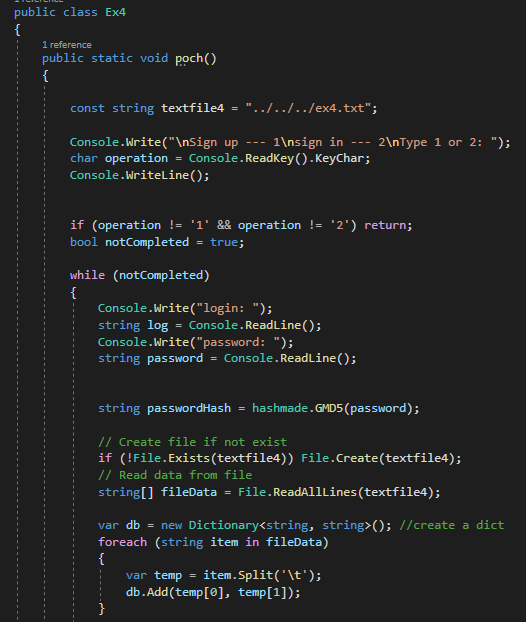


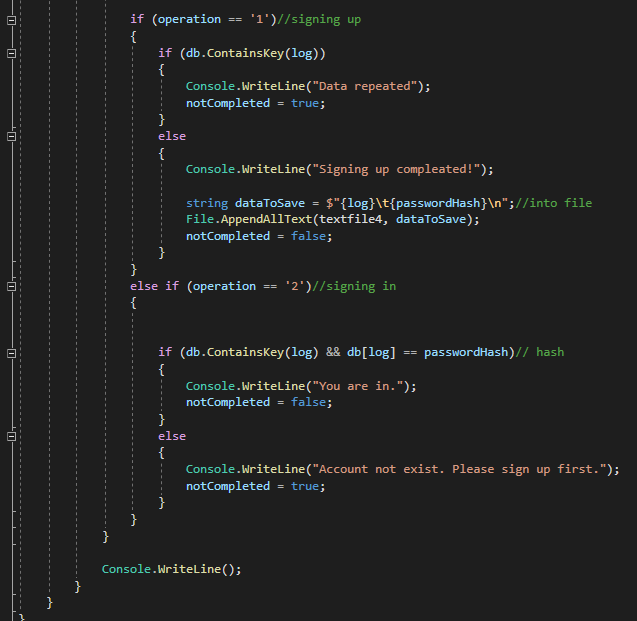
Завдання 4. Створено текстовий файл для для логіну та хешу.

Під час реєстрації логін та хешований пароль заноситься у текстовий файл.

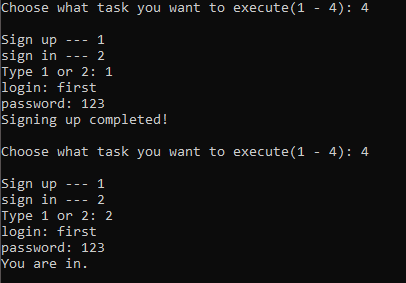
Вхід відбувається за допомогою словника.

Реєстрація по логіну, який уже існує в системі не можлива.

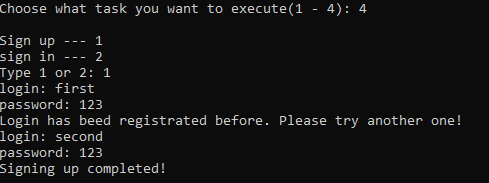




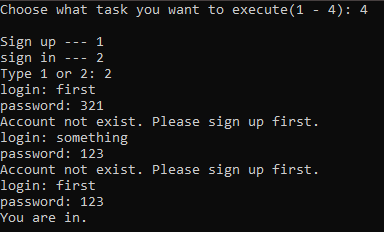
Реєстрація та вхід:



Повтор логіну під час реєстрації:



Невірний логін або пароль:



Програма готова.