**Звіт**

**до предмету «Основи інформаційної безпеки»**

Студента Київського Національного Університету ім. Тараса Шевченко

Пруніча Сергія Миколайовича

Факультет інформаційних технологій

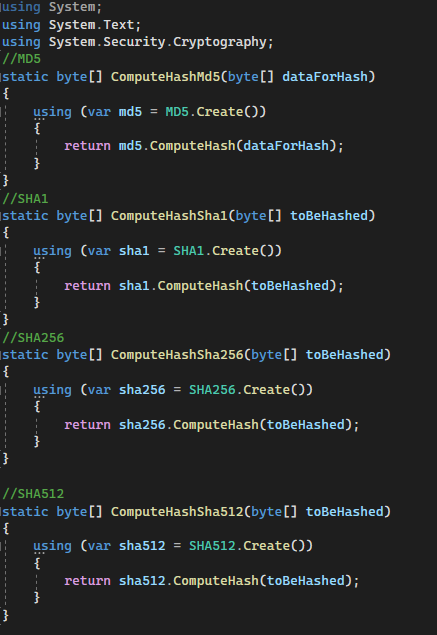
Група МІТ-21



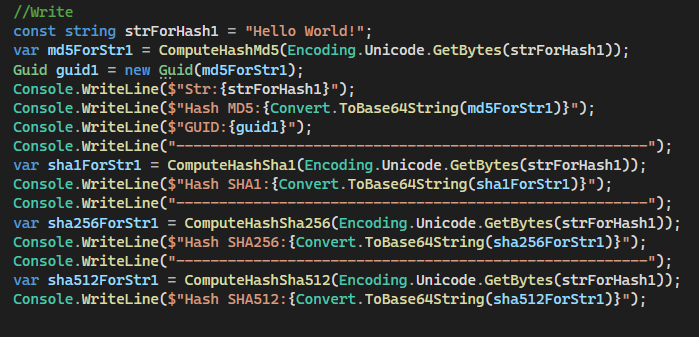
Лабораторна робота №3

Тема: «Хеш-функції та перевірка цілісності інформації»

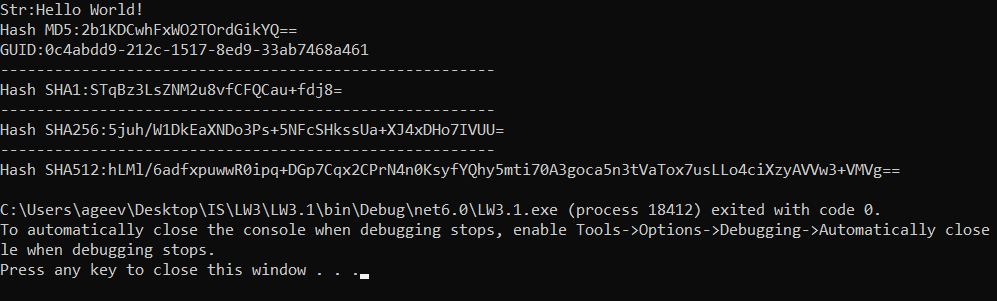
1. Написати програму, яка обчислює хеш-коди за всіма відомими алгоритмами для заданих даних. Порівняти розміри хеш-кодів та значення для однакових та різних даних. Зробити висновки.



Спочатку створюю функції для різних видів хешування. Між собою вони відрізняються тільки видами хешування, а також MD5 окрім хеш коду має додатково GUID код.



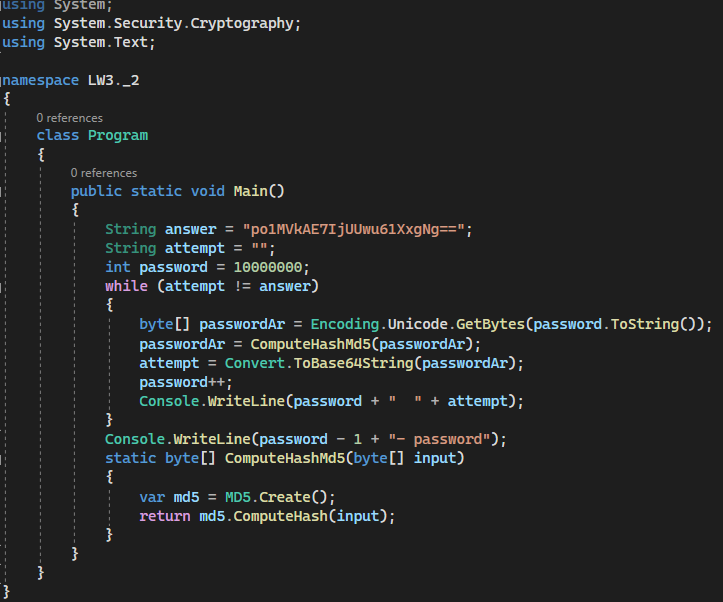
В основній частині програми маємо константне значення фрази яку будемо хешувати. Послідовно викликаємо функції та виводимо значення на екран



У ході виконання програми на екран виводиться оригінальна фраза, а далі хеш коди різних видів.

Хешування типу SHA1-512 відрізняється розміром та складністю.

1. 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.

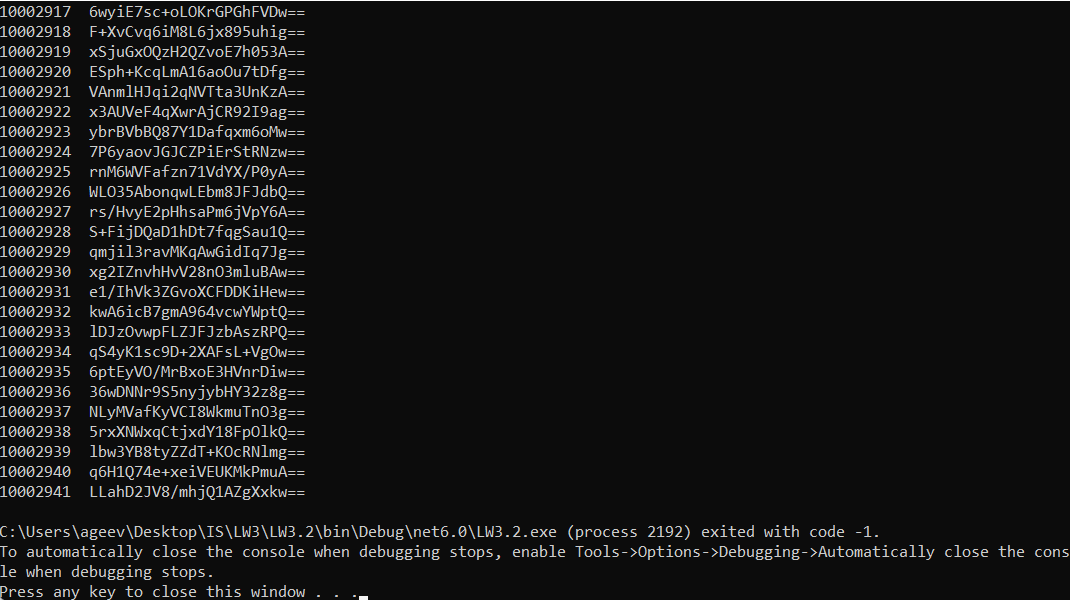


За допомогою метода перебору дізнаємось пароль

У зміну answer записуємо правильну відповідь у вигляді MD5 хеш коду

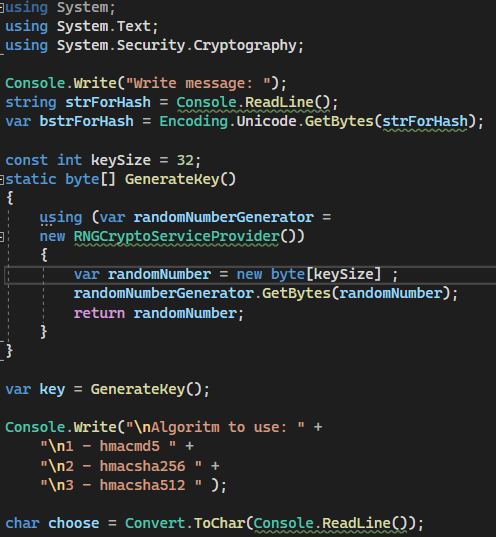
Також маємо змінну password яка буде мати в собі правильний пароль у звичній нам формі.

За допомогою циклу кожен раз отримуємо масив з поточним паролем, який перетворюємо у хеш код, та порівнюємо з наявним. Повторюємо доки не отриманий хеш код не буде таким самим, як наявний.



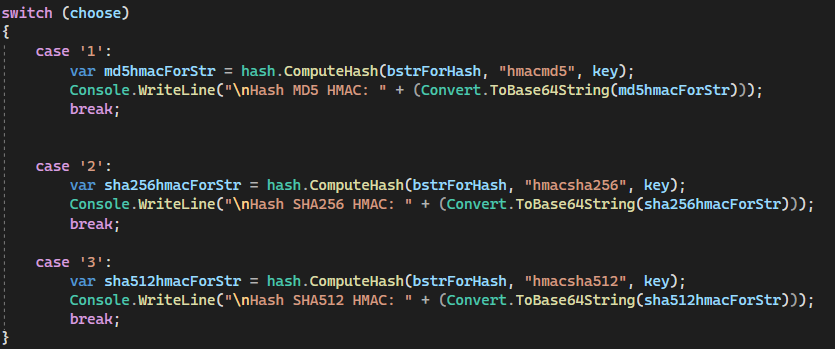
Через деякий час пароль буде підібрано, треба його зменшити на одиницю(тому що зайвий раз виконується цикл) і отримаємо правильний пароль **20192020**

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



Спочатку запрошуємо у користувача повідомлення, а також просимо обрати метод хешування.

Функція GenerateKey потрібна для генерування випадкового числа для використання в якості ключа.



Випливаючи з обраного методу хешуємо повідомлення за допомогою функції описаної нижче(у цю функцію передаємо три параметри: повідомлення, яким методомо хешувати повідомлення і також ключ)



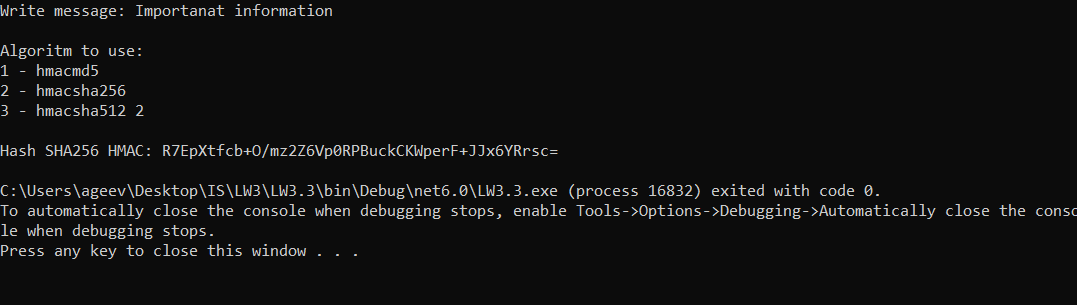
Далі описуємо функцію хешування:

За допомогою switch обираємо метод хешування

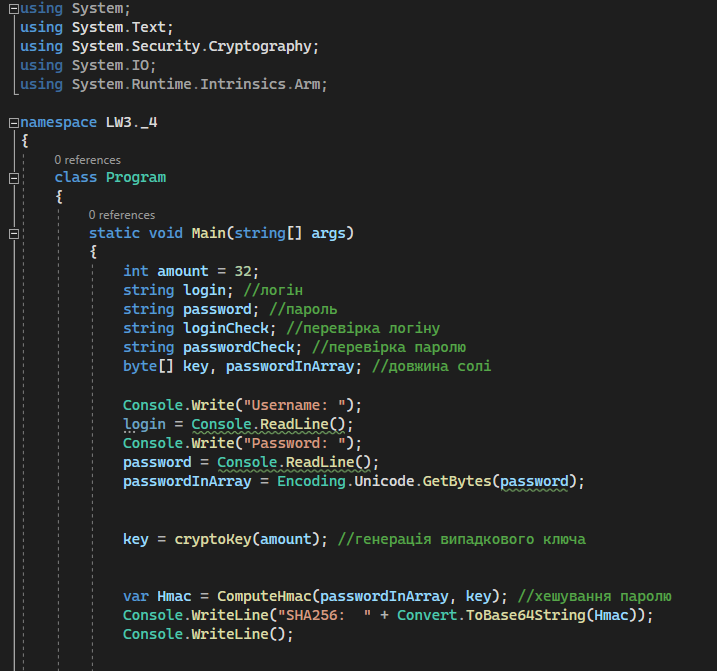
Хешуємо повідомлення з використанням завчасно згенерованого ключа

У кінці повертаємо значення змінної toBeHashed, яка містить в собі оброблене повідомлення.

Після цього, на екран виводиться хешоване потрібним методом повідомлення.



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



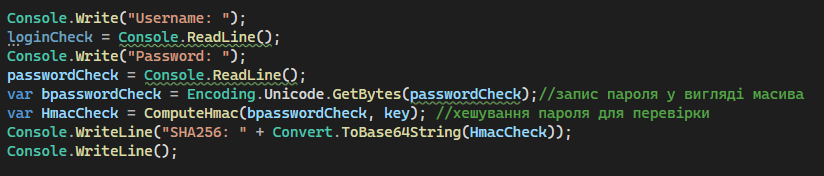
Спочатку проводиться ініціалізація таких змінних як довжина ключа, логін, пароль, змінні для перевірки та масиви з ключем та паролем користувача.

Потім просимо користувача ввести свій логін та пароль (зареєструватись)

Одразу записуємо введений користувачем пароль у вигляді масиву

Генеруємо ключ за допомогою функції cryptoKey (ця функція генерує випадкове число яке використовується в якості ключа)

Хешуємо пароль, та виводимо результат на екран



Знову просимо користувача ввести логін та пароль, але на цей раз для авторизації (робимо перевірку)

Введений другий раз пароль записуємо в окрему змінну, і також зберігаємо у вигляді масиву

Хешуємо пароль та розпочинаємо перевірку

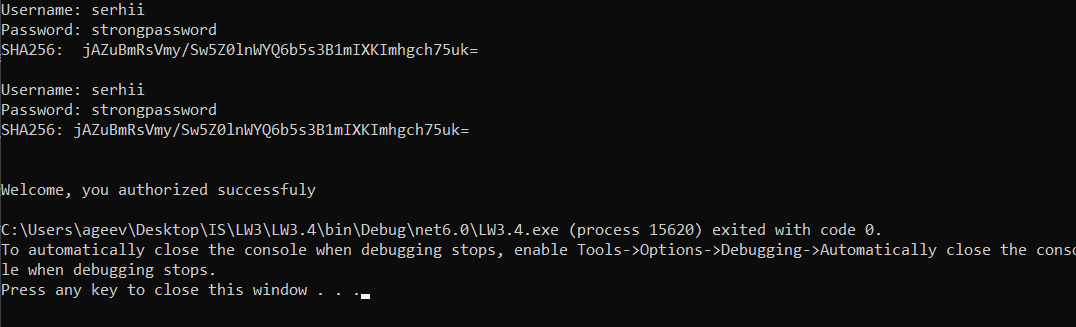


Передаємо у функцію CheckPass два хешованих пароля

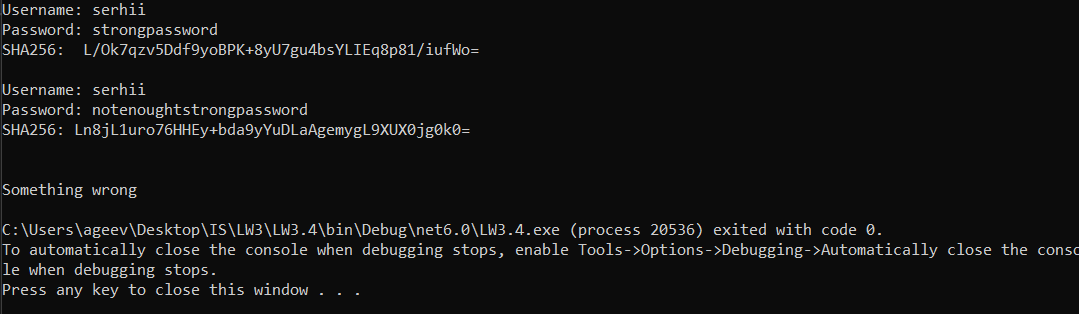
У самій функції паролі перетворюємо на рядок, та порівнюємо між собою

Якщо паролі збіглись, виводимо на екран повідомлення про успіх, якщо ні, виводимо повідомлення про невдачу

Нижче описані функцію генерування випадкового числа, а також функція хешування методом SHA256



Якщо пароль введений правильно, на екрані з’явиться повідомлення про успішну авторизацію



Якщо паролі не співпадають, виводиться повідомлення про невдачу.

**Висновок:** в ході цієї практичної роботи ми навчились обчислювати хеш-коди за всіма алгоритмами та обчислення хеш-коду автентифікації повідомлення.