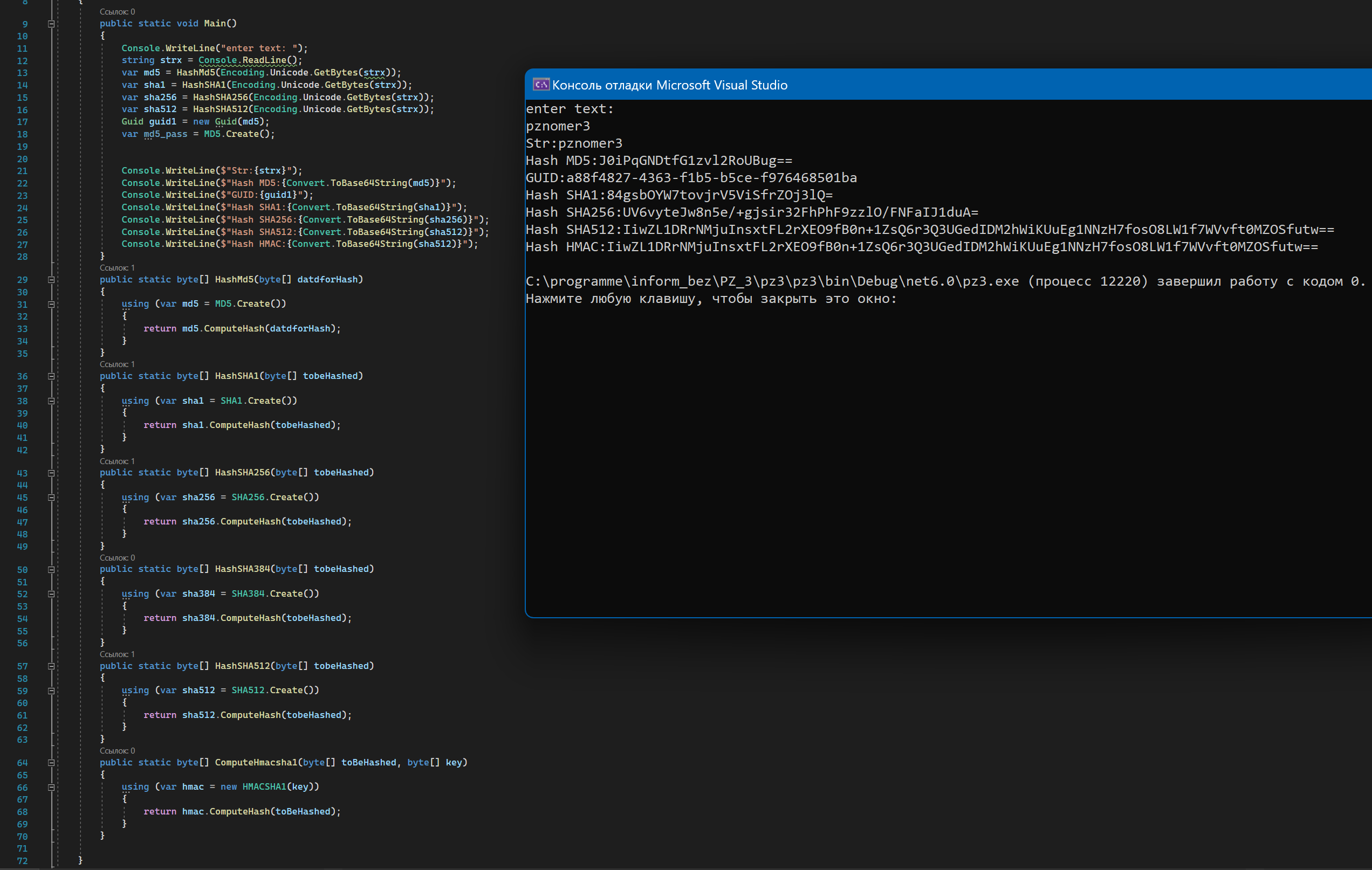
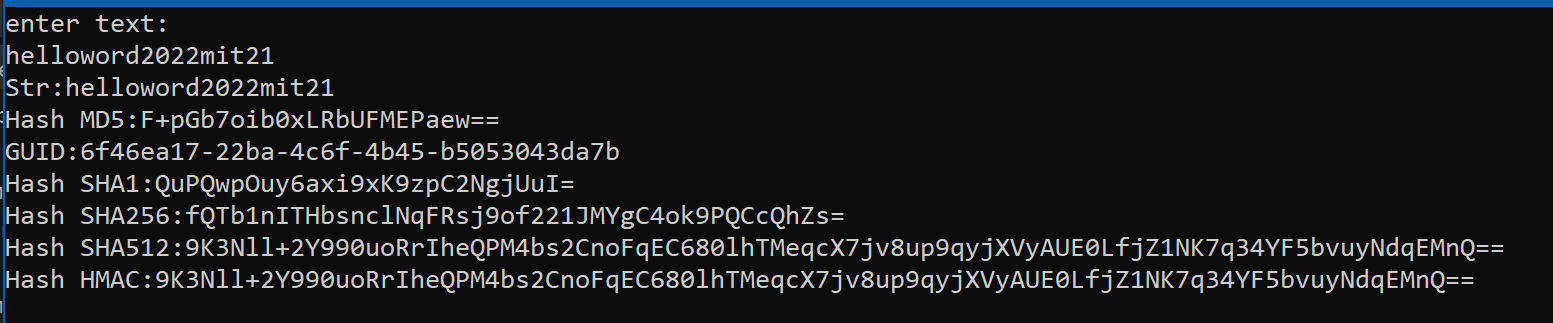
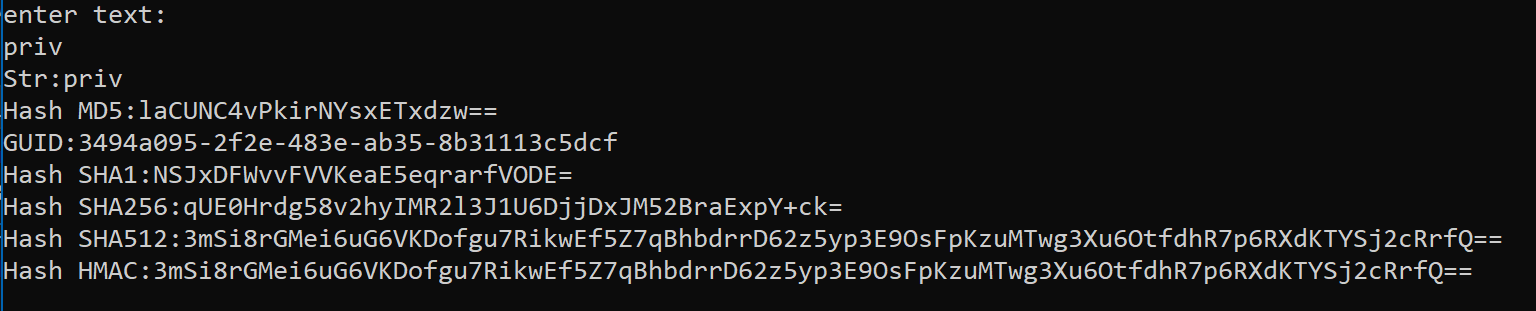
Звіт з інформаційної безпеки №3

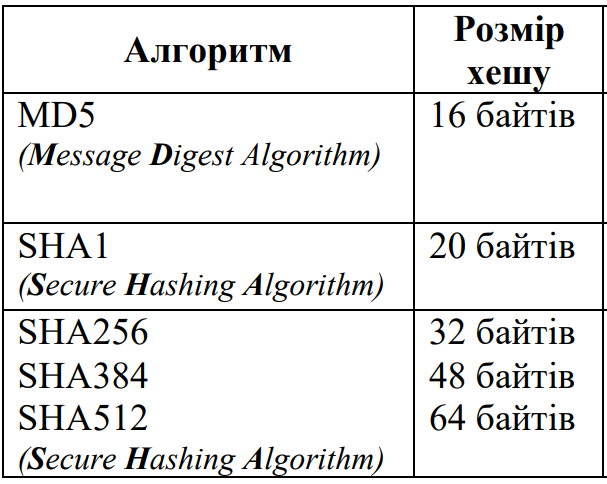
Квартюка Олексія

**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**

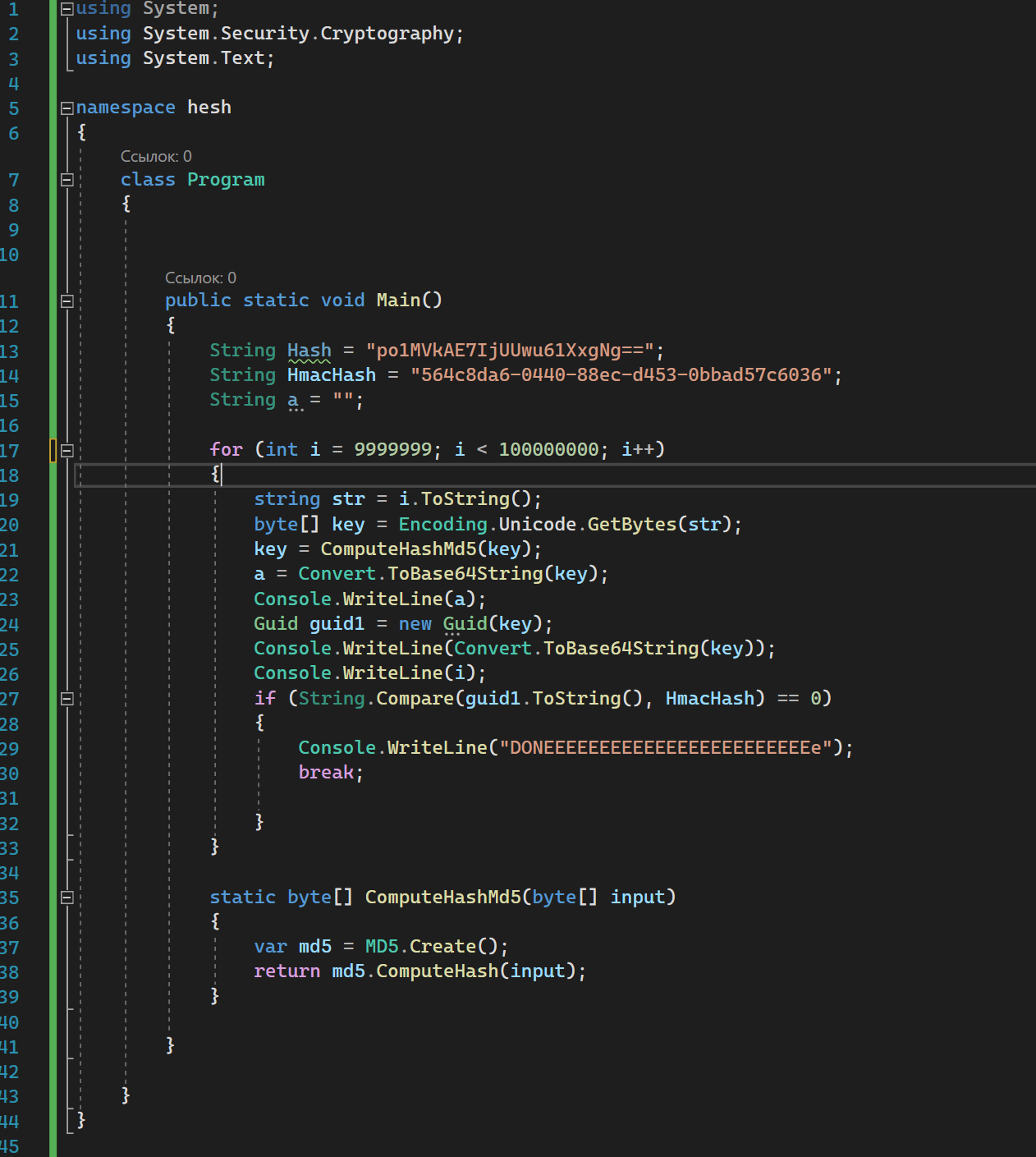


Порівнявши всі хеш-коди, можемо зробити висновок, що розмір не залежить від введеного тексту. Важливо лише кількість байтів.

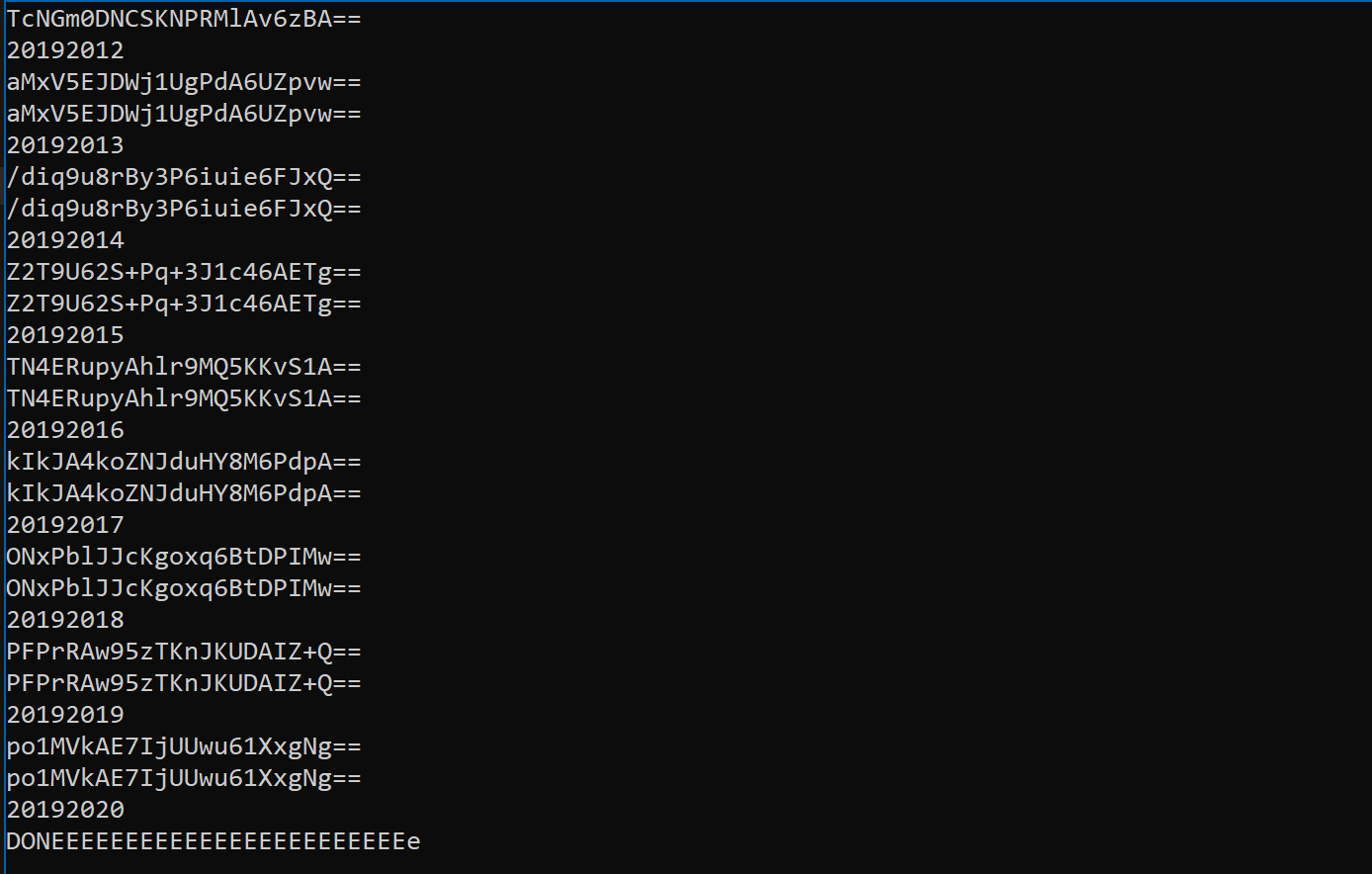




**2) Відомо, що користувач використав для пароля довжиною 8 символів лише цифри. Шляхом пасивного прослуховування мережі отримано MD5 хеш-код цього пароля: {564c8da6-0440-88ec-d453-0bbad57c6036} та po1MVkAE7IjUUwu61XxgNg== Відновити пароль користувача та зробити висновки про надійність такого пароля**

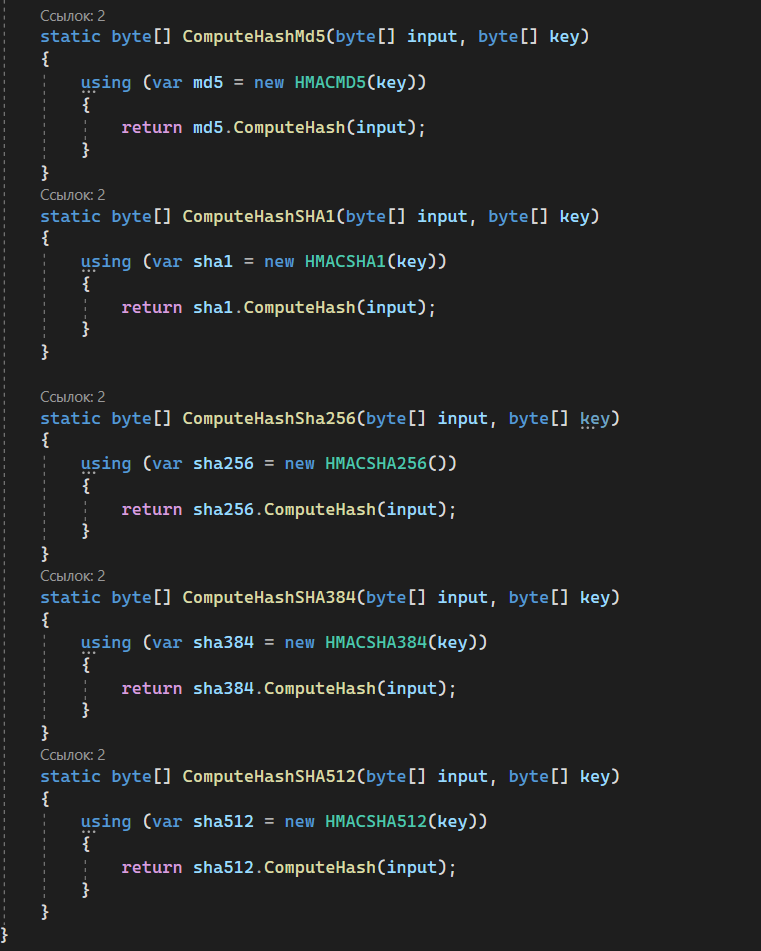
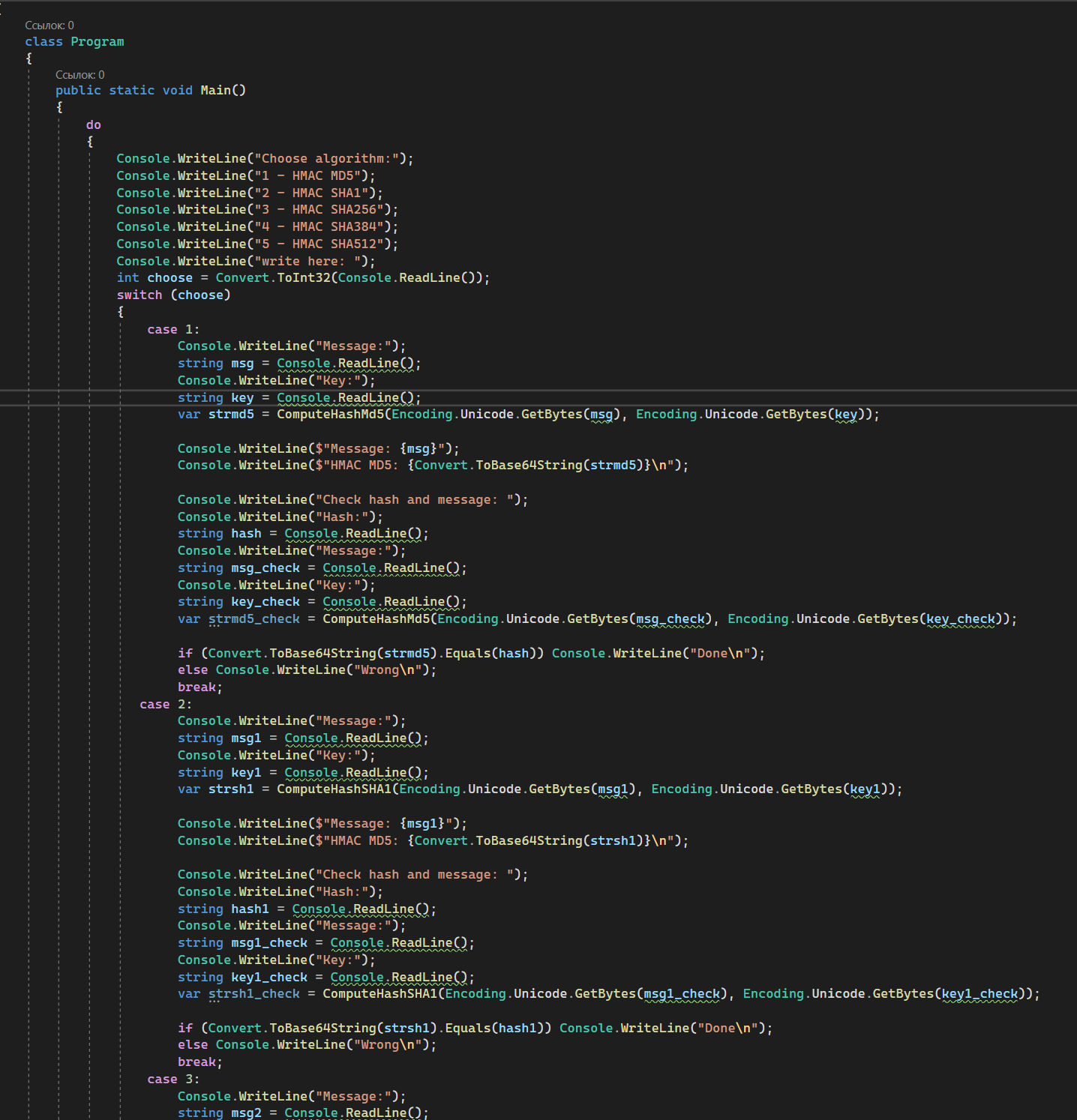
****

В цьому коді я використав цикл фор для пассивного перебору пароля для всіх восьмизначних чисел. Всередині циклу кожну ітерацію “I” перетворюємо в послідовність байтів і обчислюємо хеш код. Далі перетворюємо хеш в рядок і звіряємо з хешем в умові.

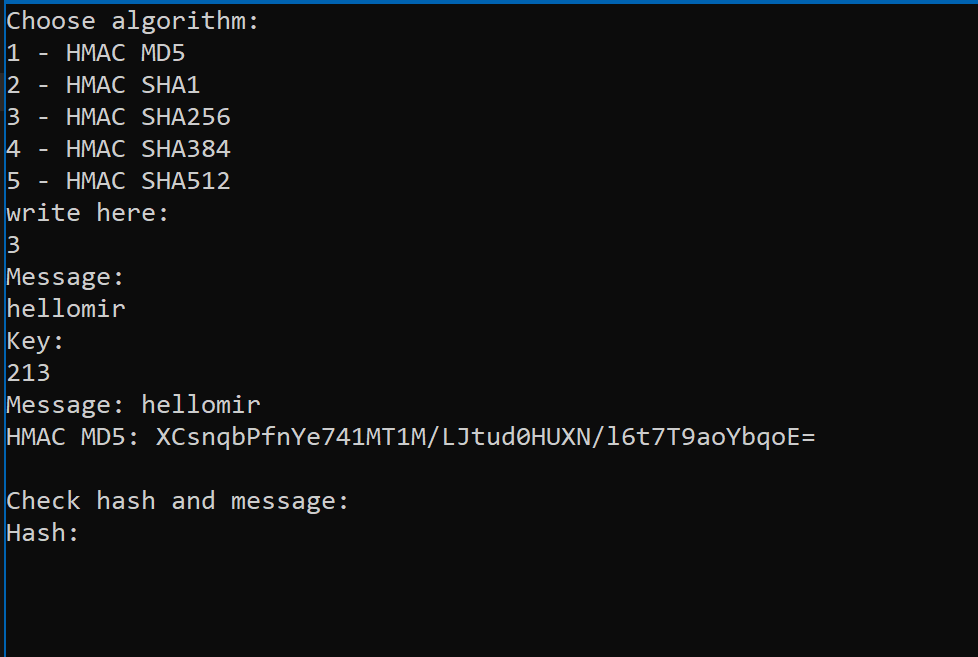


Після встановлення пароля, можемо зробити висновок, що такий пароль не є надійним.

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

****

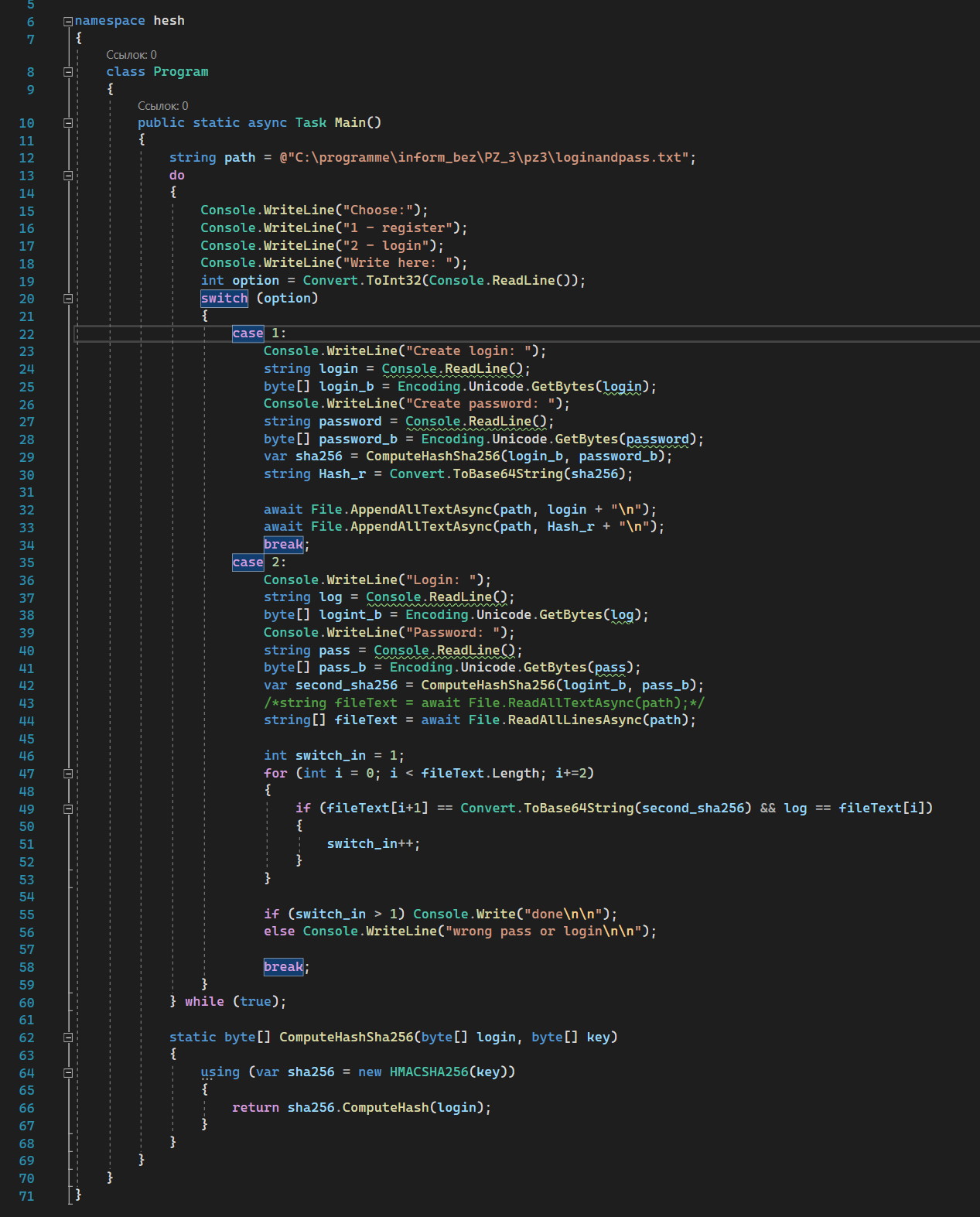
Змоделюємо ситуацію: захешуємо повідомлення одним з алгоритмів та передамо хеш і повідомлення довірені людині, що знає пароль.

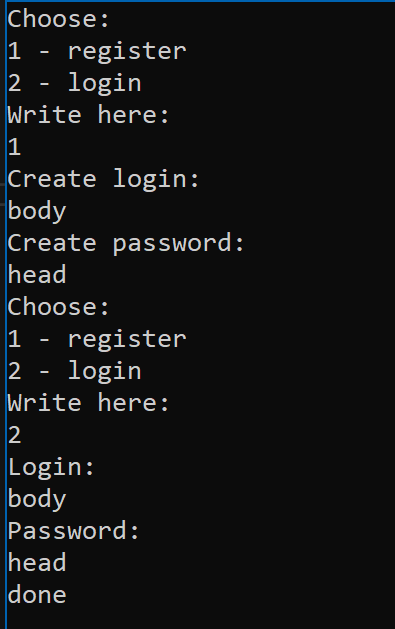
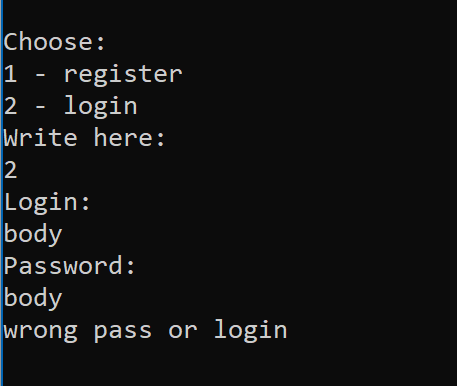
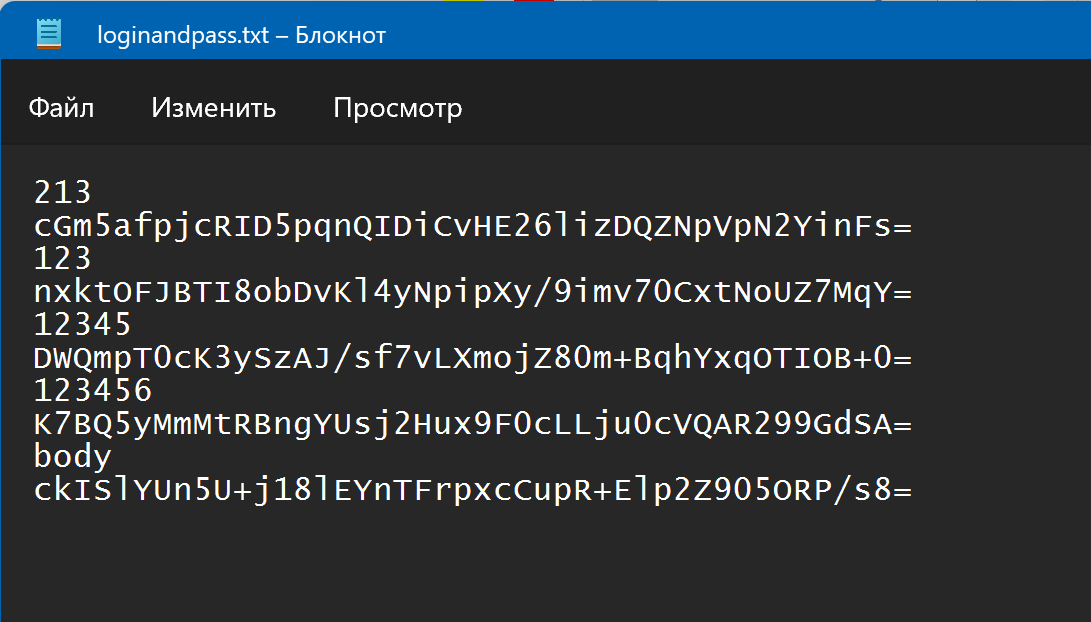
****

Для аунтифікації повідомлення інша довірена особа повинна ввести отриманий хеш та повідомлення + підставити свій ключ. Побачивши, що хеши співпадають, можна зробити висновок, що повідомлення не підроблене та відправлене від довіреної особи.

****

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

****

**** **** 

У цій программі я використовував текстовий документ для запису логіну та паролю у вилгяді hmac.

Ключем для HMAC був сам пароль, а повідоамлення – логін.

При входженні в свій аккаунт цикл for порівнює логін та хеш із текстового документу.

P.s : Після повторного відкриття програми файл не перезаписується.

Висновок: Отже, в ході виконання 3 практичного завдання ми детальніше ознайомились з алгоритмами хешування md та sha. Навчилися використовувати автефіковане хешування та визначились з сферою використання різних алгоритмів.