Звіт

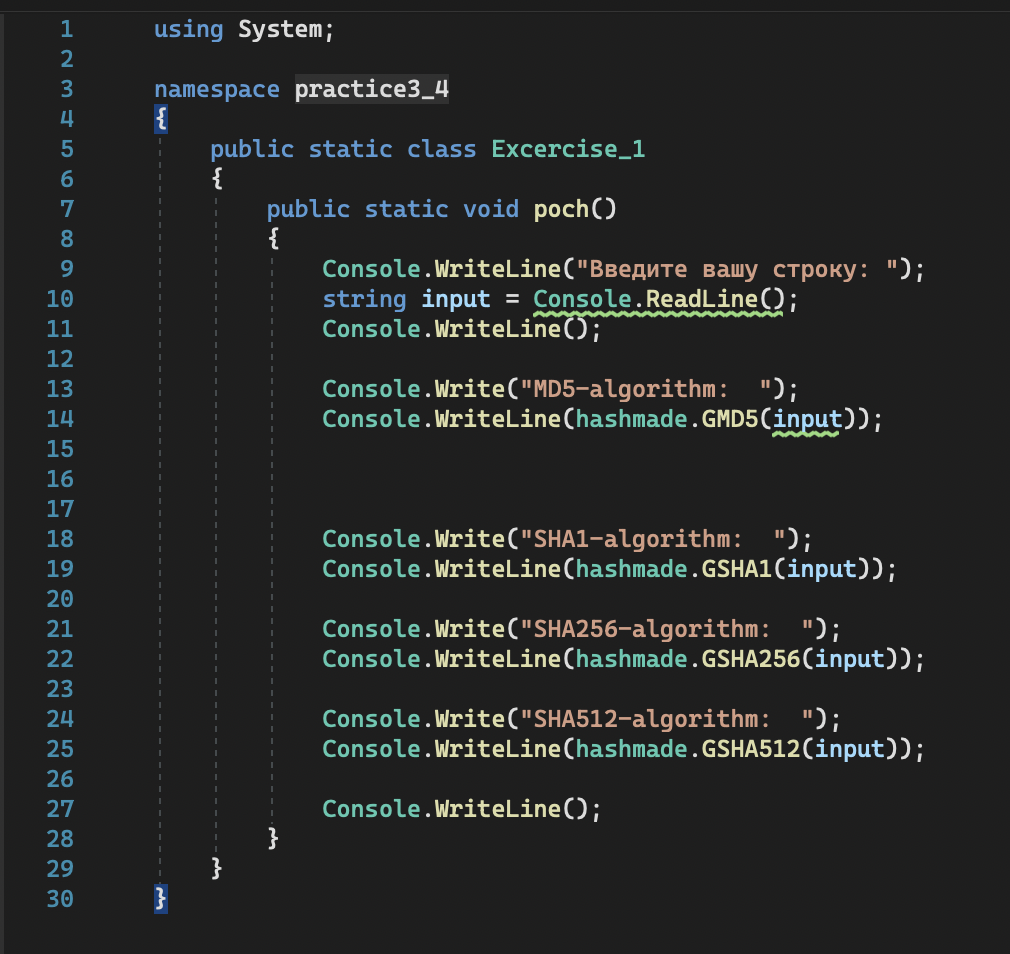
До практичного заняття №3-4 з дисципліни:  
«Основи захисту інформації» з теми:

**«Хеш-функції та перевірка цілісності інформації»**

Голомозик Кирило МІТ-21

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

Завдання 1



Використовую файл, який хешує строки, до нього звертаюся у всіх завданнях  


Порівняв хеш при 5 знаках і при 8 знаках  
При 5: 

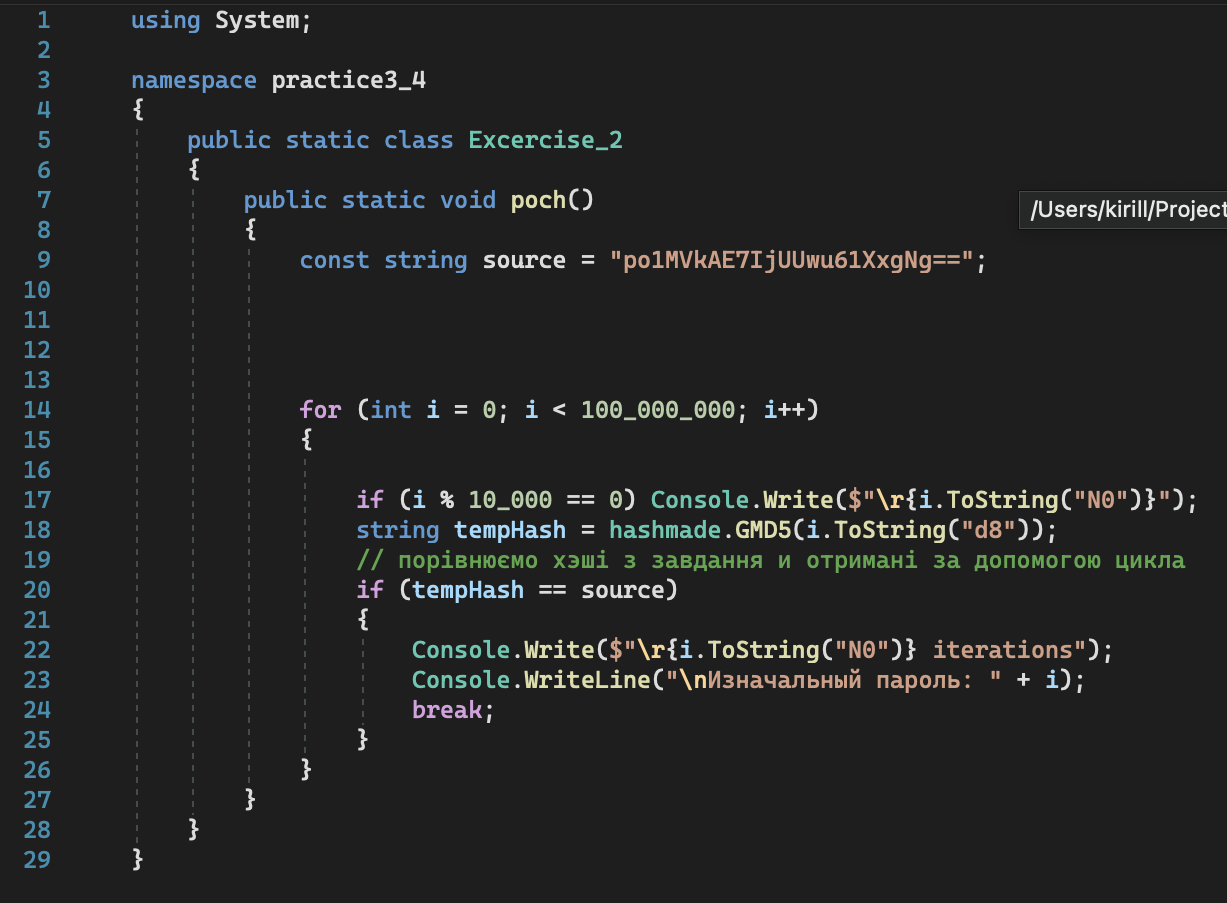
При 10:



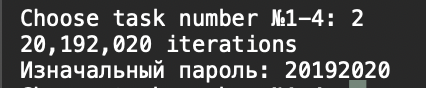
Висновок: розмір хешу однаковий при різних об'ємах інформації, це залежить від алгоритму хешування.

ЗАВДАННЯ 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.



Там тільки літери, тому було не так важко, як було б з літерами  
зробив лічильник для розуміння стадії процессу.



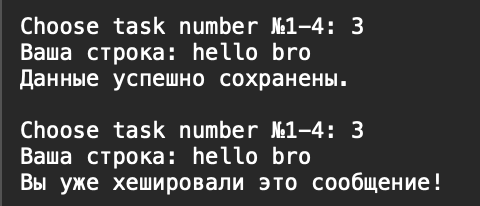
Бачимо, що було проведено 20 192 020 операцій.

Завдання 3:

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



Створюємо файл для запису в нього хешу   
потім за допомогою файлу hashmade хешуємо введену інформацію, перевіряємо чи не була вона введена до цього, якщо так, то виводимо повідомлення про це на екран.



ЗАВДАННЯ 4

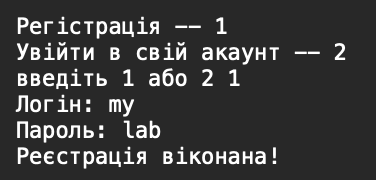
Написати програму для реєстрації користувача за логіном/паролем та авторизації шляхом співставлення відповідних логінів і паролів. Зберігання пароля у відкритому вигляді неприпустиме.



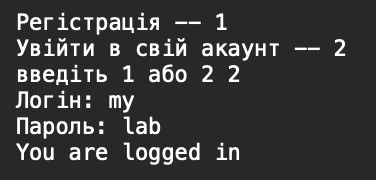
Зробив меню для регістрації та логіну

Спочатку реєструємося

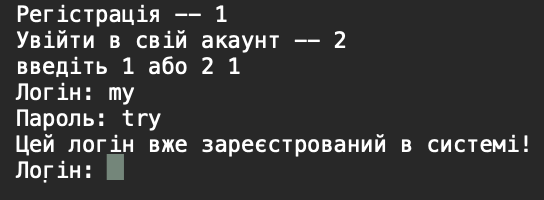
Вводимо логін, та пароль  
пароль хешується, та записується з логіном в файл через пробіл



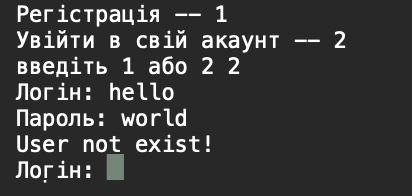
Далі виконаємо вхід в наш аккаунт  
це відбувається через те, що в нас є словник, де логін-ключ, а хеш паролю-значення



Якщо при реєстрації введемо логін, яким вже користувалися, то отримаємо повідомлення про це



Якщо захочемо увійти без реєстрації, то отримаємо наступне:



Готово!