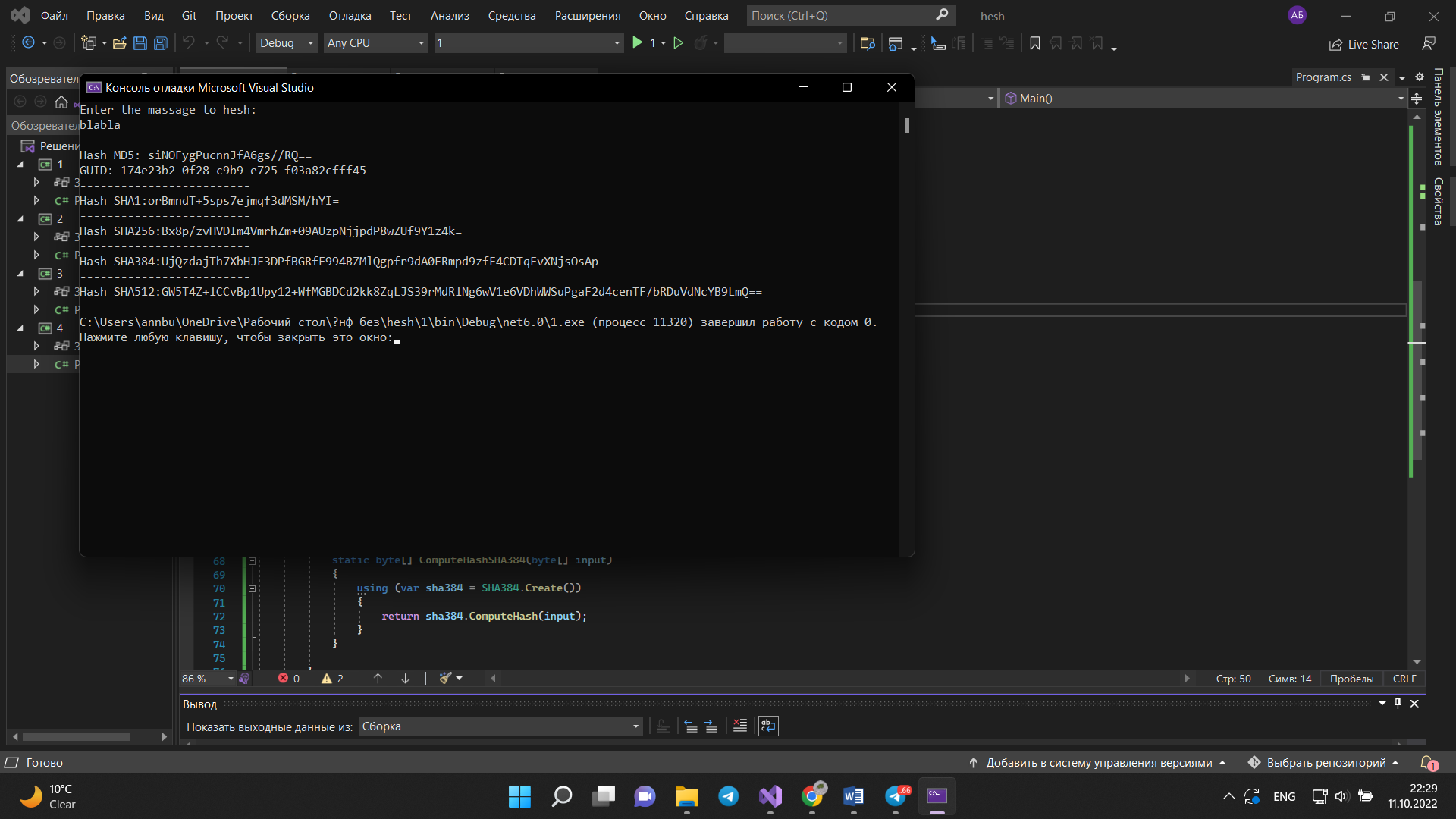
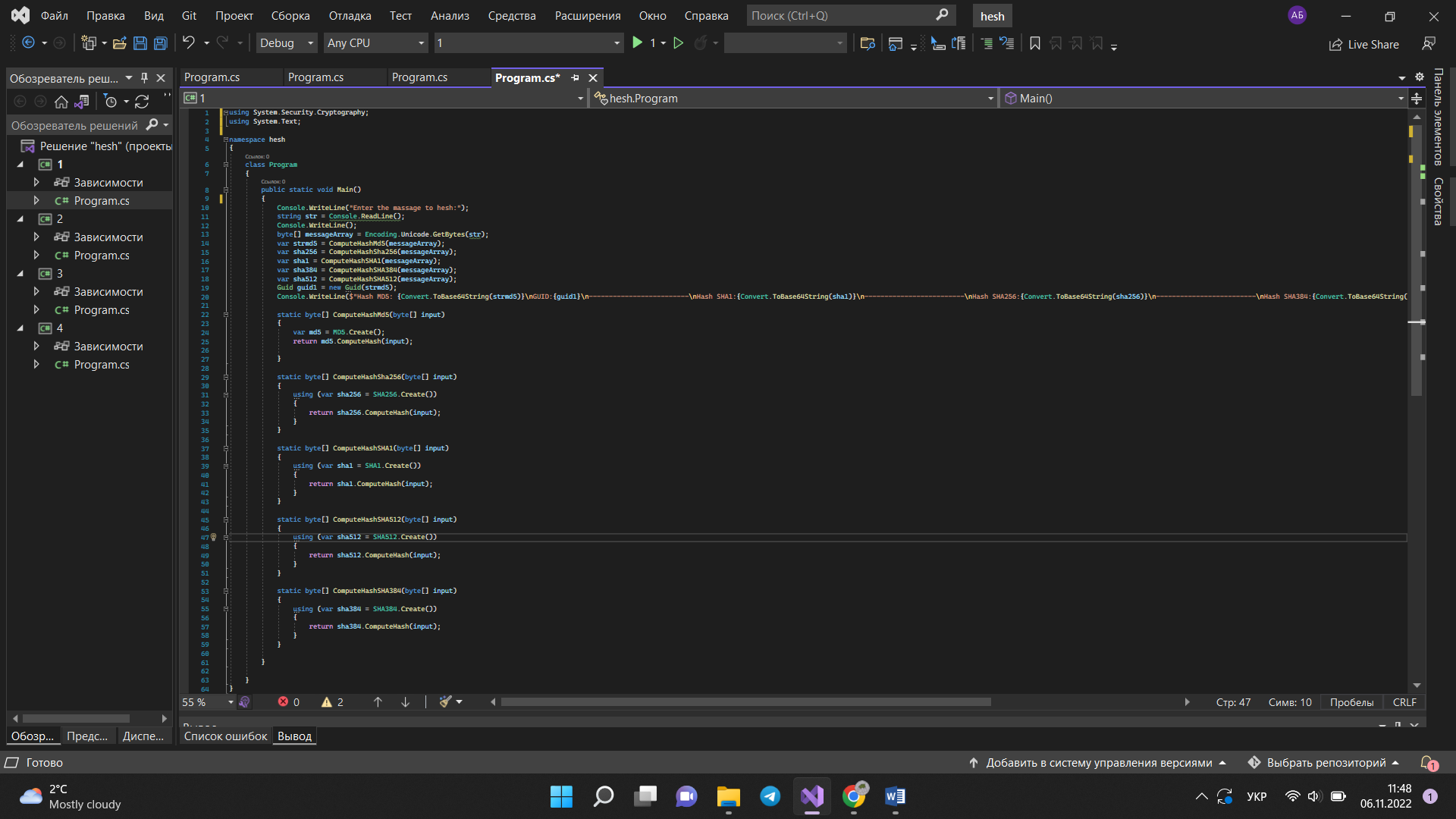
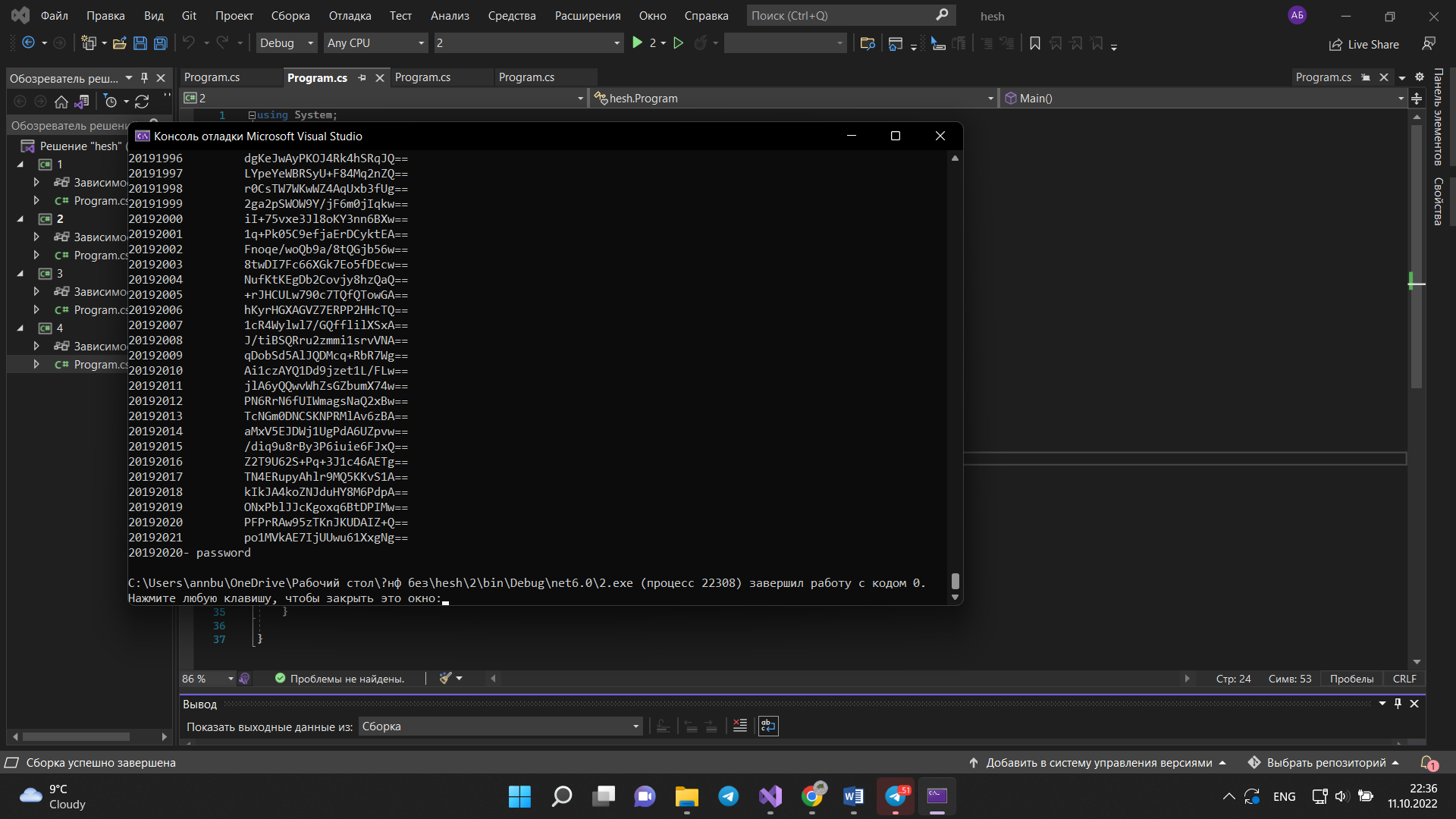
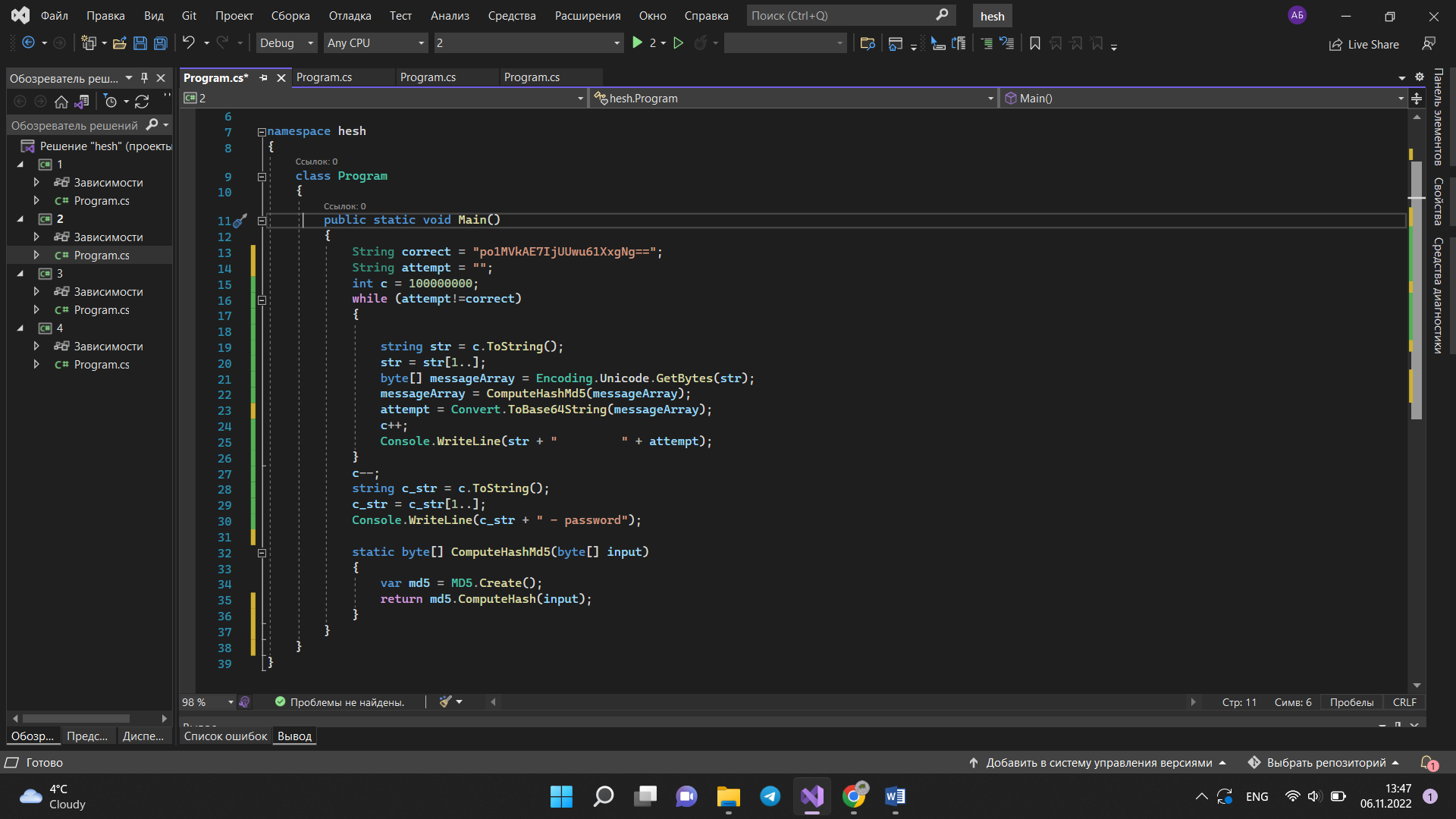
***Практичне заняття №3***

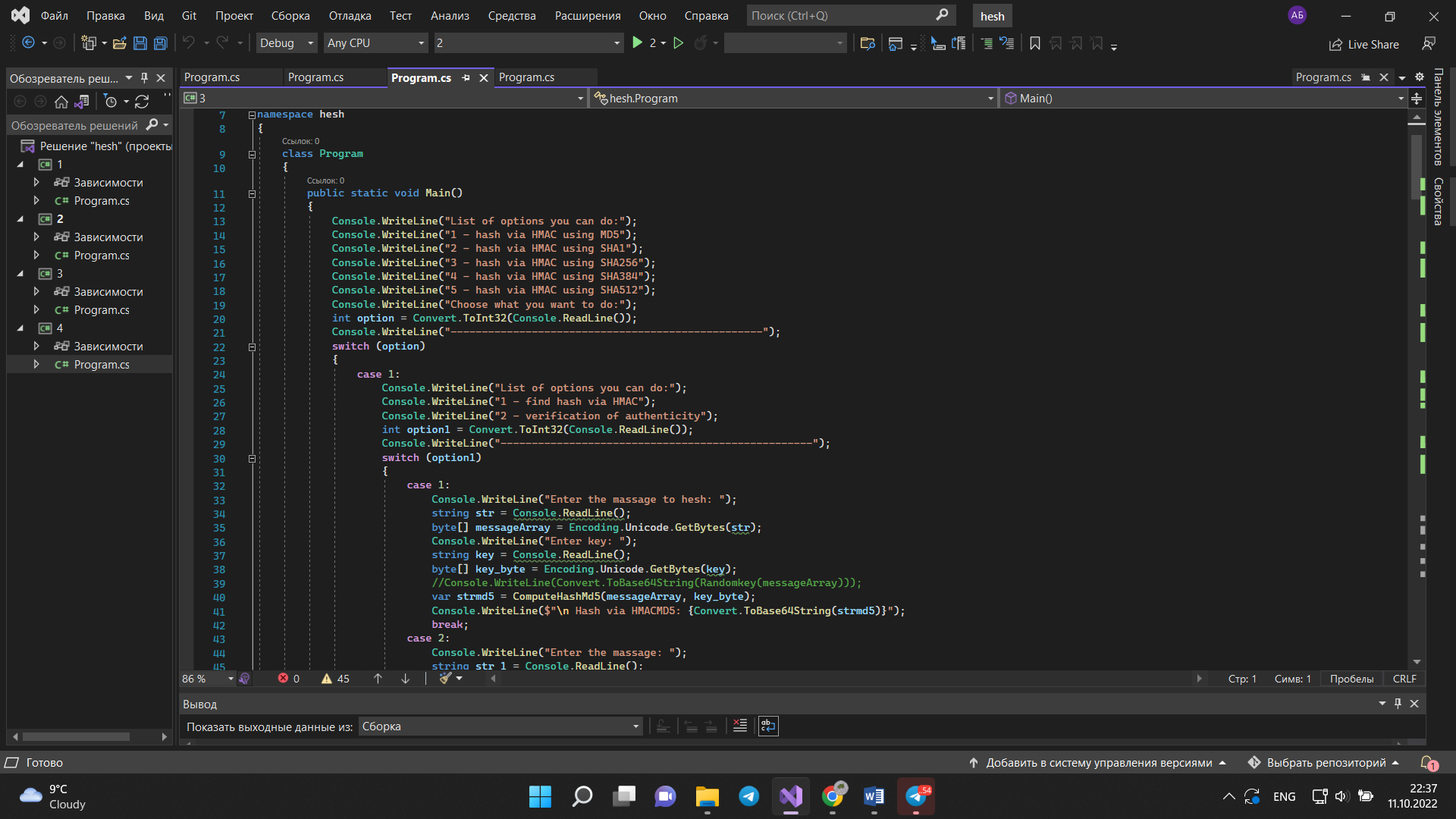
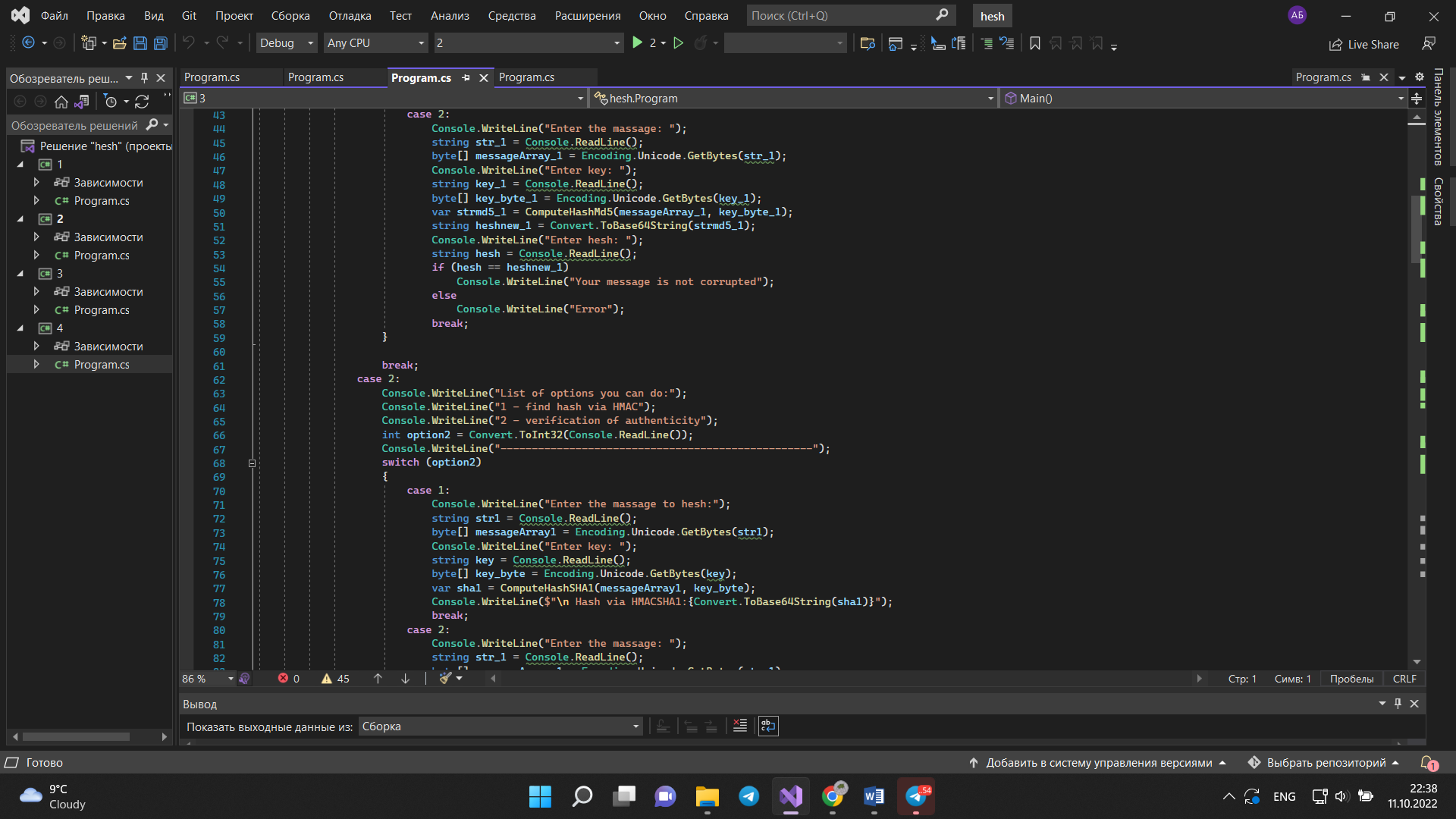
«Хеш-функції та перевірка цілісності інформації»

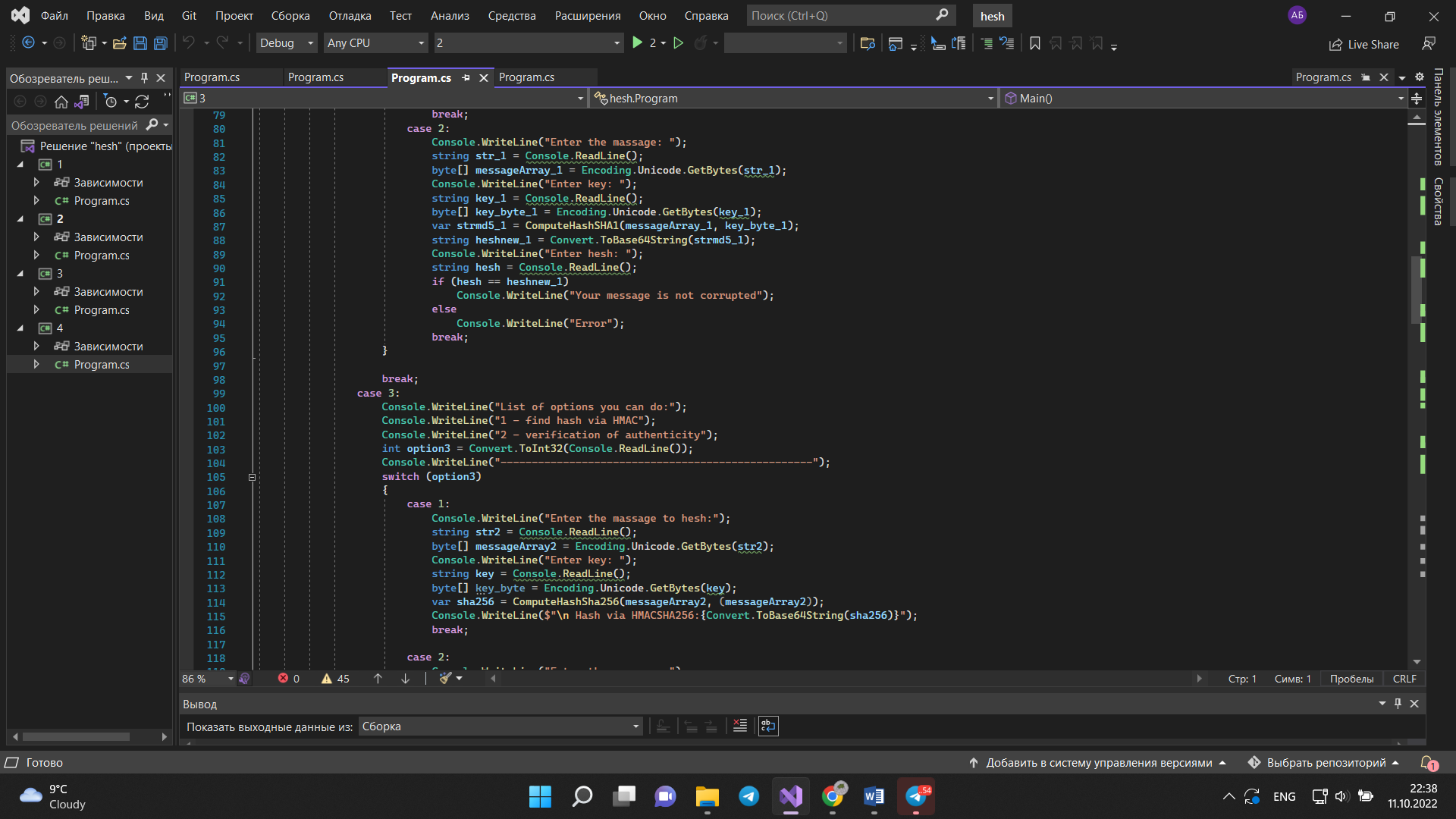
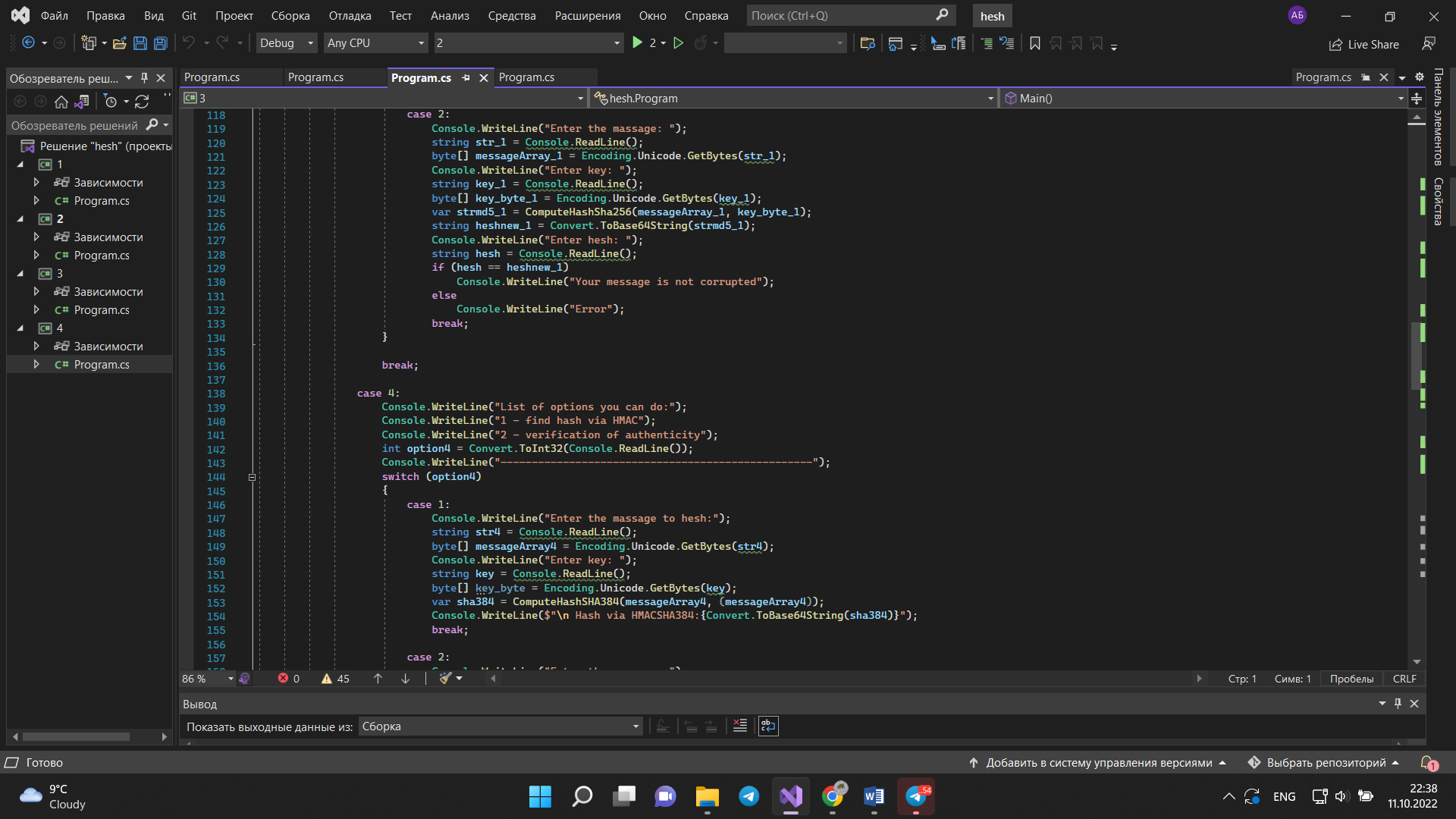
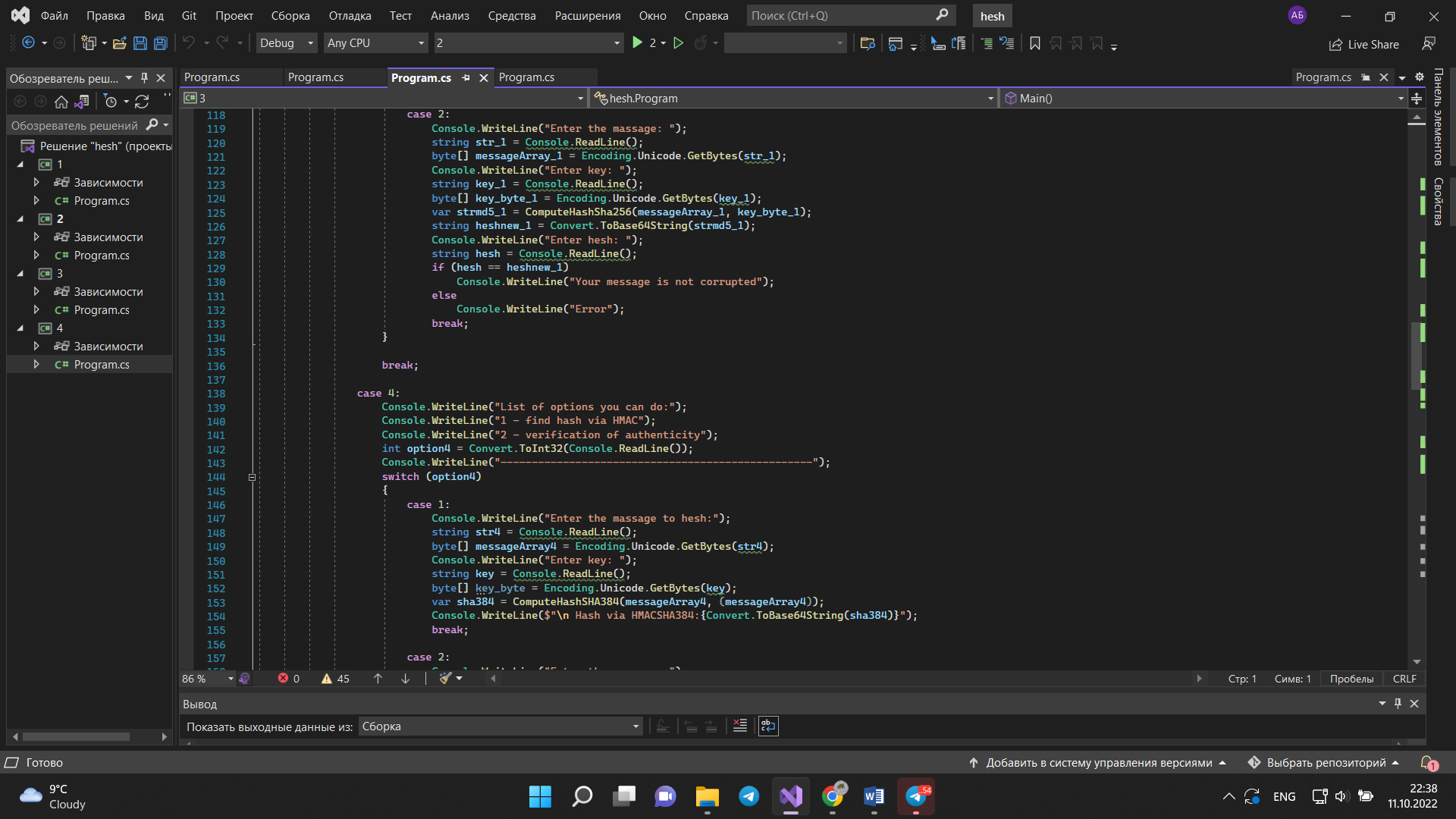
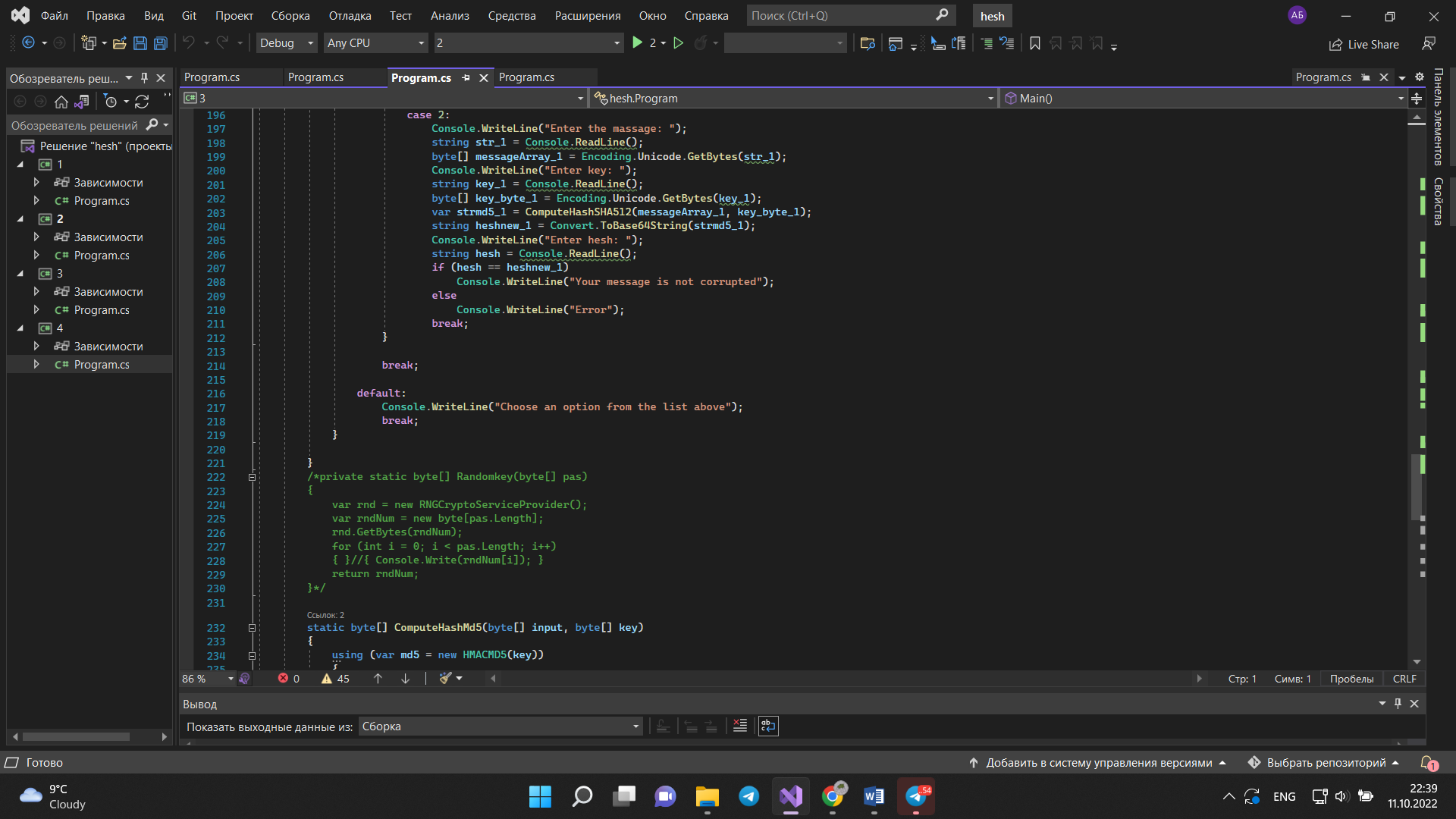
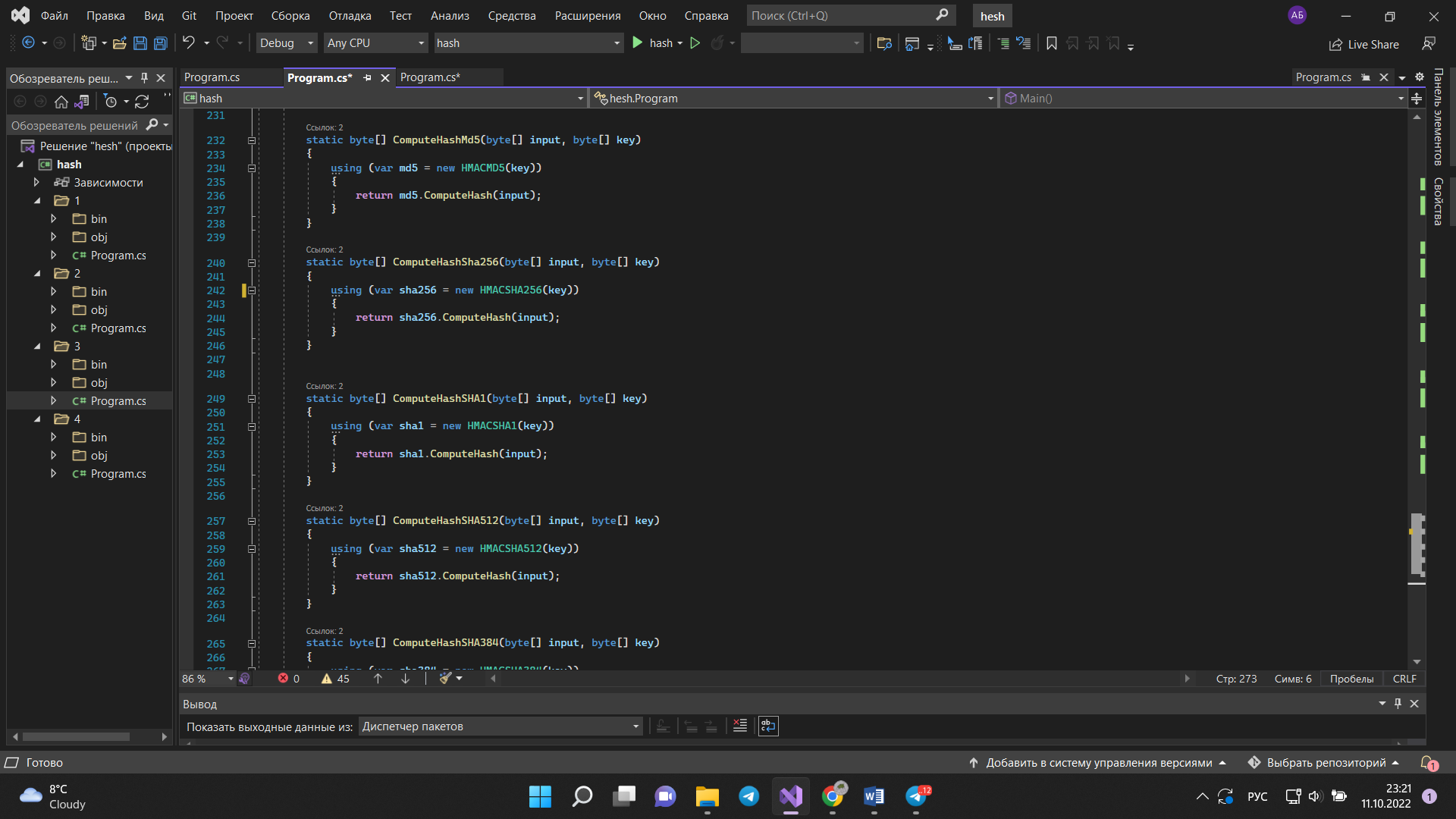
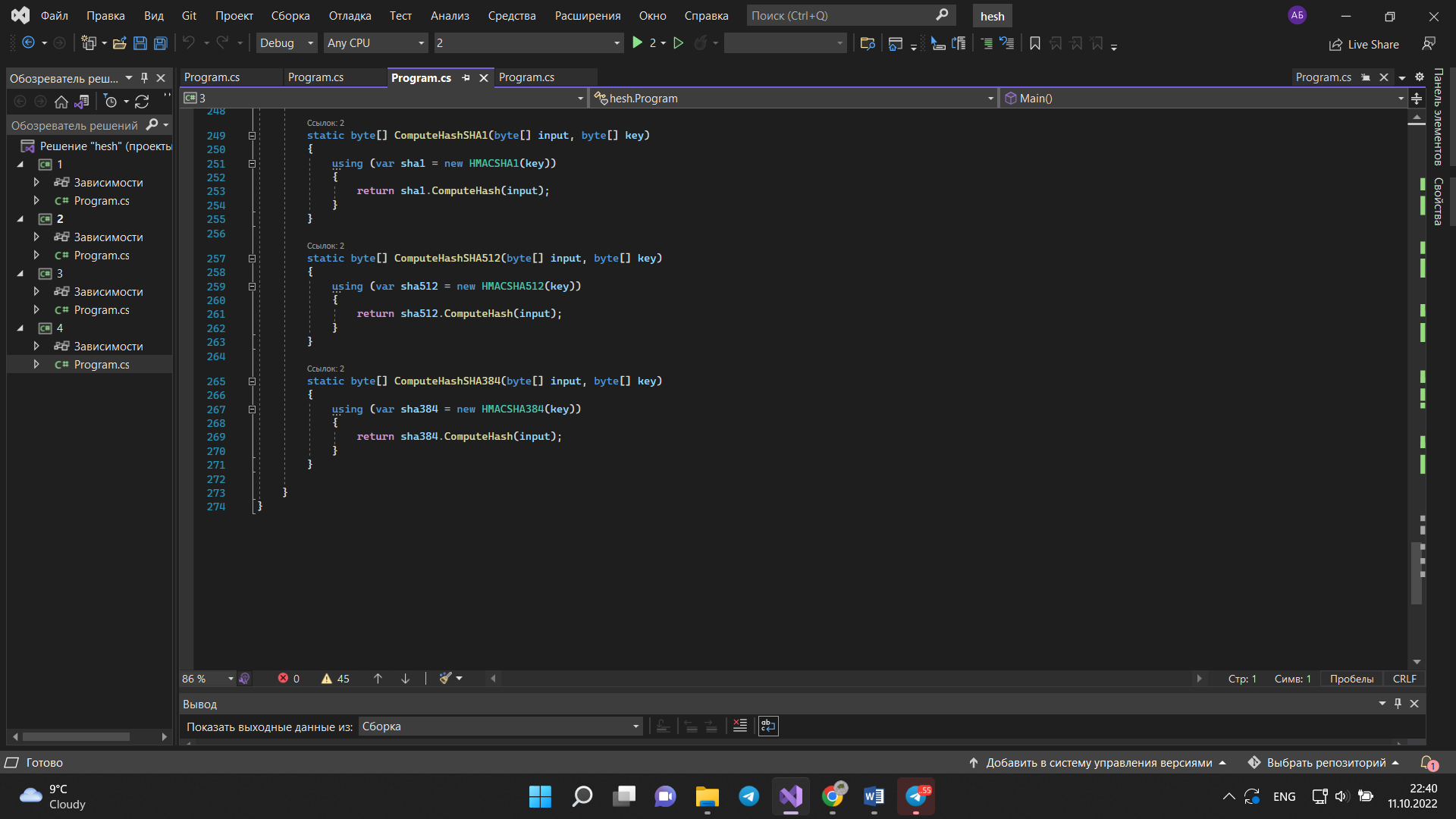
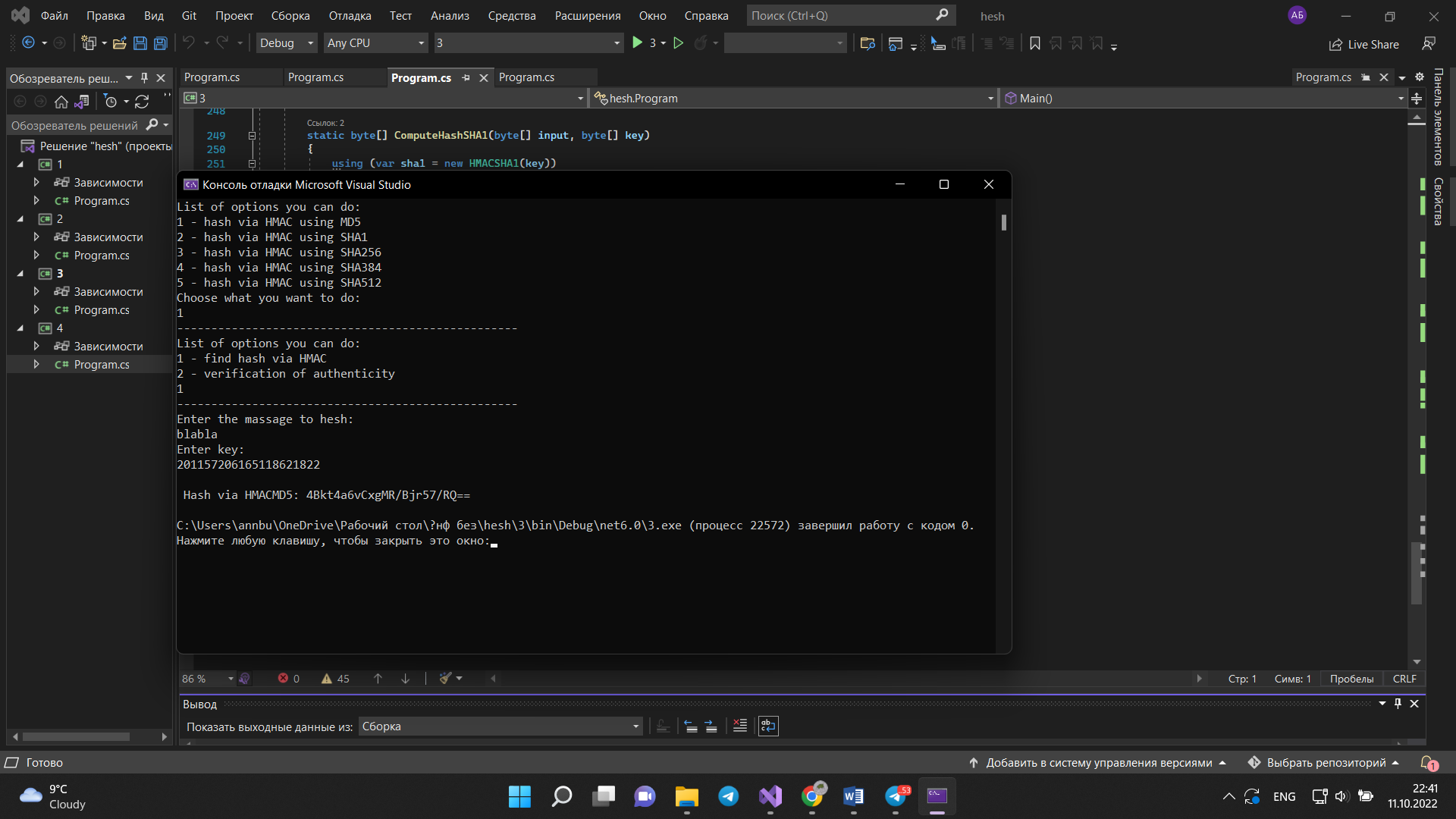
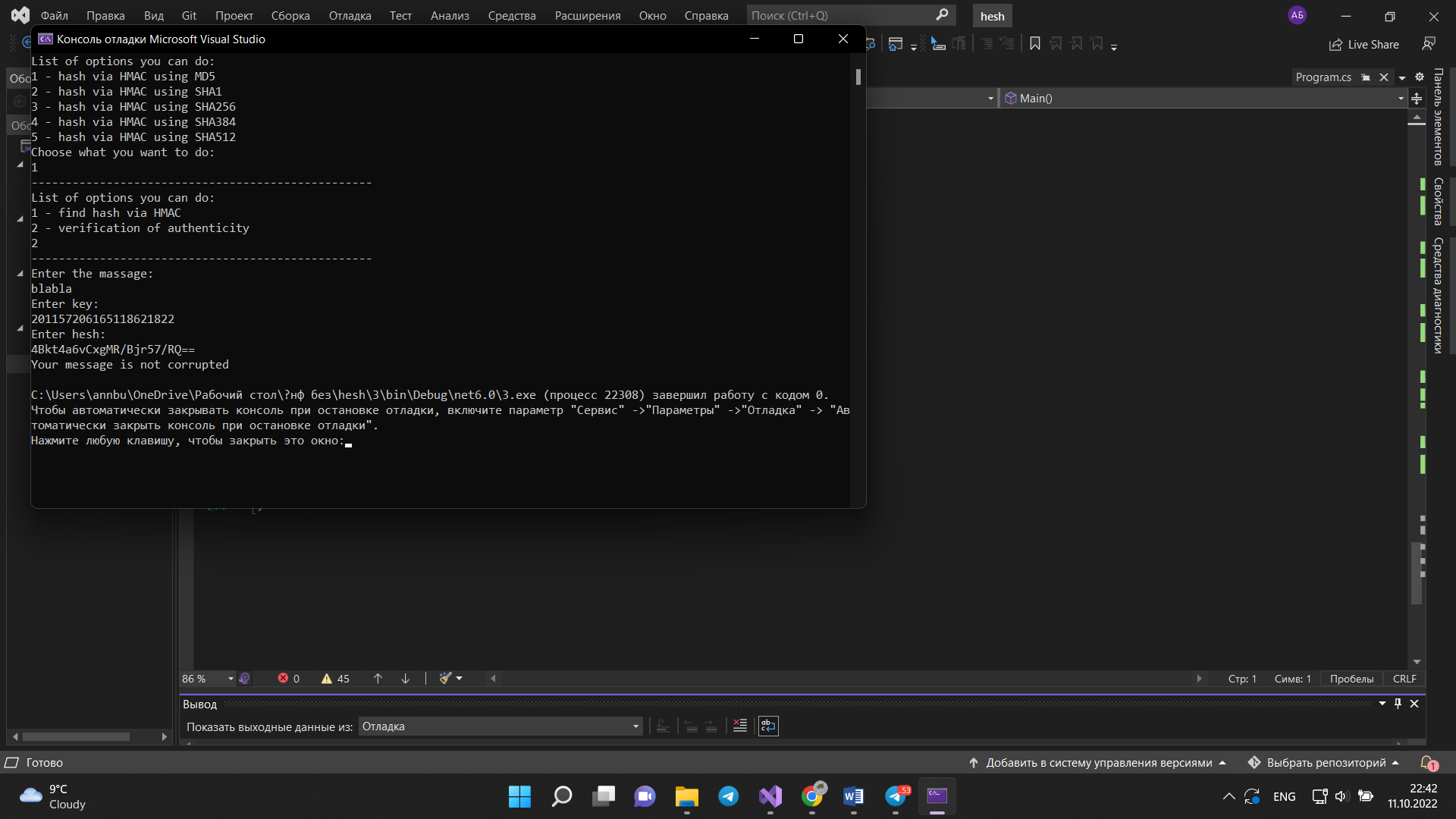
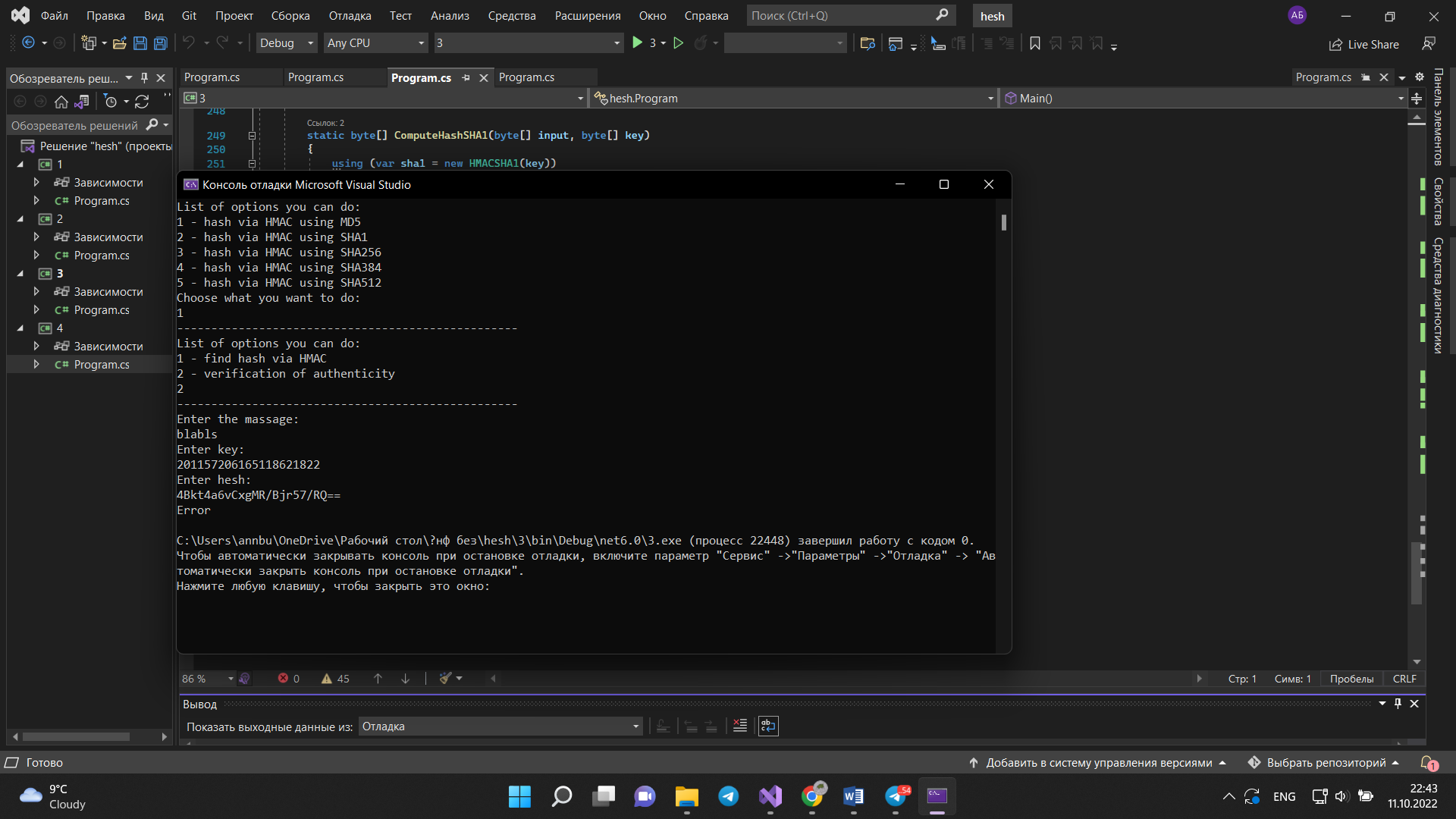
Виконала студентка групи МІТ-21 Булгакова Анна

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. Виконавши це завдання ми вивчили декілька алгоритмів хешування. І можемо примітити, що кожен відрізняється своєю довжиною. Концепція SHA така ж, як і у MD5 алгоритму, але алгоритми суттєво відрізняються. SHA хеш-коди більш довші та більш стійкі. Який саме із 4-х алгоритмів SHA використовувати залежить від преференцій швидкодії, обсягу пам’яті для зберігання хеш-коду та стійкості до колізій.

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. Виконавши друге завдання ми відновили пароль користувача – 20192020. Можемо зробити висновки, що цей пароль дуже не надійний тому, що складається з восьми символів і це лише цифри та взломати такого користувача дуже легко. Пароль має буде довший та включати в себе різні символи для більшої надіності.

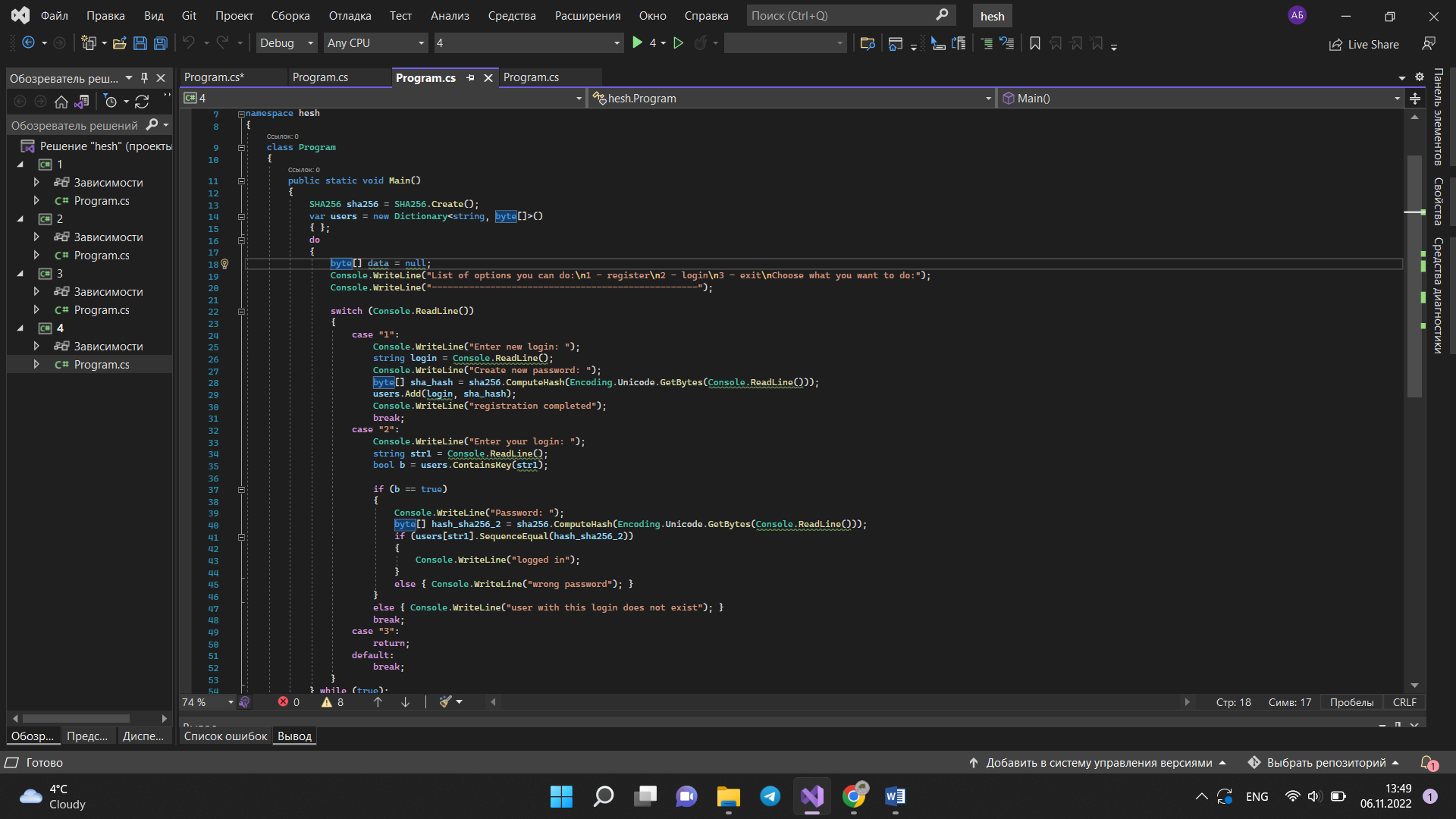
3. Написати програму для обчислення хеш-коду автентифікації повідомлення, а також реалізувати можливість перевірки автентичності повідомлення.

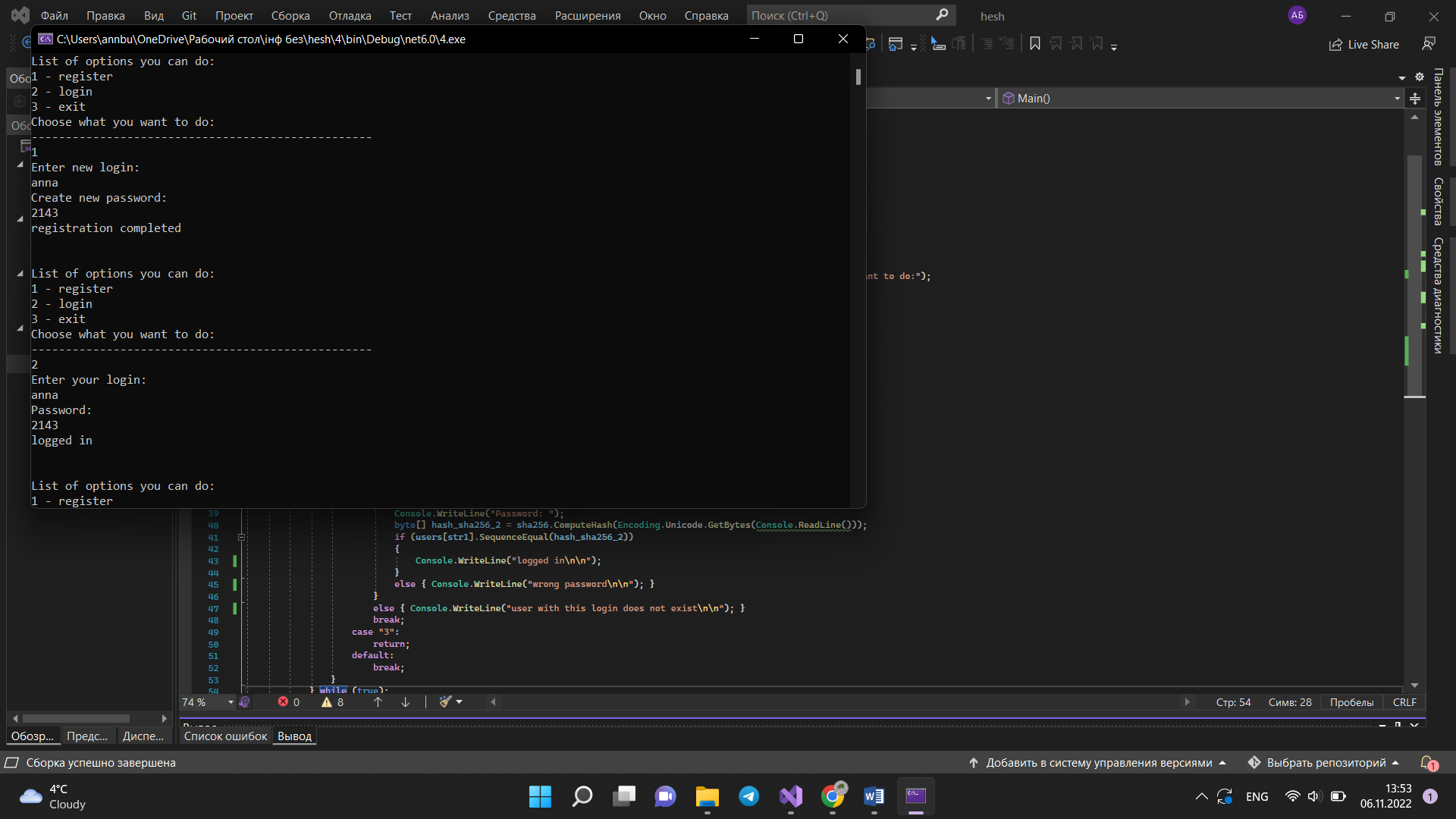


Виконавши завдання 3, за його допомогою можна виконувати автентифіковане хешування. Тепер ми можемо забезпечити перевірку цілісності даних для визначення чи були дані з підроблені або пошкоджені та забезпечити потребу в автентифікації, що звичайним чином випливає із забезпечення цілісності даних. Тобто потрібно мати можливість переконатися, що дані, які ми отримали, надіслані автентифікованою особою.

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





Програма із завдання 4 це простенький варіант реєстації та авторизації користувачів. В даному випадку я обрала використання словників, тому, що воно нас не обмежує в кількості користувачів.

Висновок: На даній практичній роботі ми познайомилися та вивчили різні алгоритми та сімейства хеш-функцій та навчилися перевіряти цілісность інформації.