**Основи інформаційної безпеки**

Практичне заняття №5

Тема: **«Безпечне зберігання паролів»**

Звіт студента групи МІТ-21 Вовка Дмитра

Варіант №6

Основні способи зберігання паролів:

1) Зберігання паролів у відкритому вигляді

2) Шифрування паролів

3) Хешування паролів

4) Використання хешу та солі для зберігання пароля

5) Використання спеціальних функцій

**Зберігання паролів у відкритому вигляді**

Зберігати паролі у відкритому вигляді є дуже небезпечним. Цей метод не захищає дані і їми можуть легко заволодіти зловмисники.

**Шифрування паролів**

За допомогою шифрування, ви шифруєте пароль за допомогою секретного ключа й розшифровуєте за допомогою цього ж ключа. Якщо зловмисники отримають цей ключ, то вони с легкістю зможуть дізнатися всі паролі, що може призвести до втрати конфеденційності та взлому акаунтів користувачів.

**Хешування паролів**

Хешування паролів є значно кращим медотом ніж шифрування, так як після переведення паролю у хеш, повернення у початковий вигляд є неможливим. Але цей метод має свої 2 важливі недоліки. Перший це використання зловмисниками райдужних таблиць, а другий це підбор паролю методом губої сили, коли зловмислики по черзі перебирають усі можливі паролі.

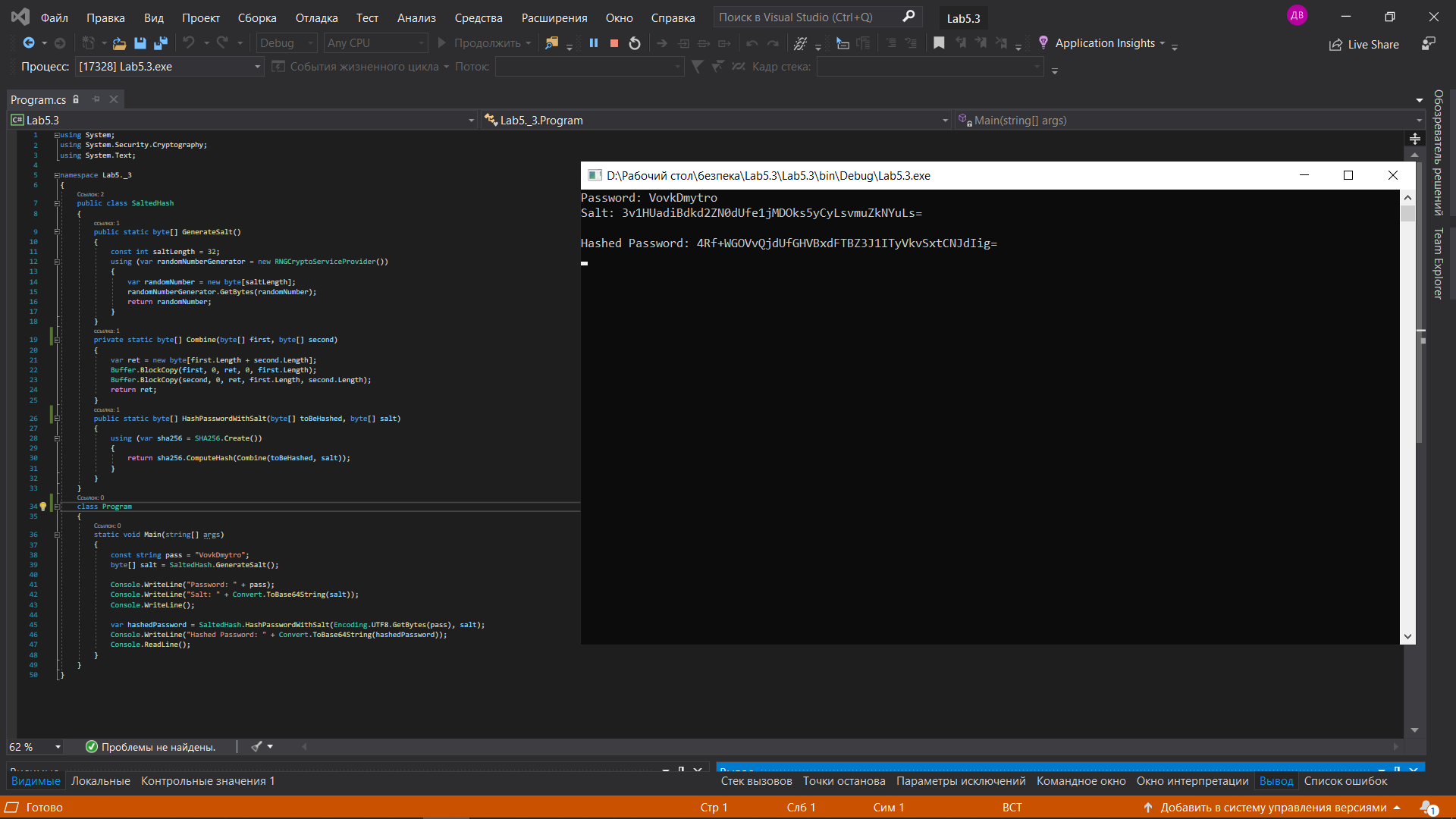
**Використання хешу та солі для зберігання пароля**

Сіль – це випадкова комбінація байтів, яка додається до кожного пароля введеного користувачем. Так як сіль це випадкова комбінація байтів, то для кожного пароля вона буде різною, що значно ускладнить підбор паролю грубою силою.

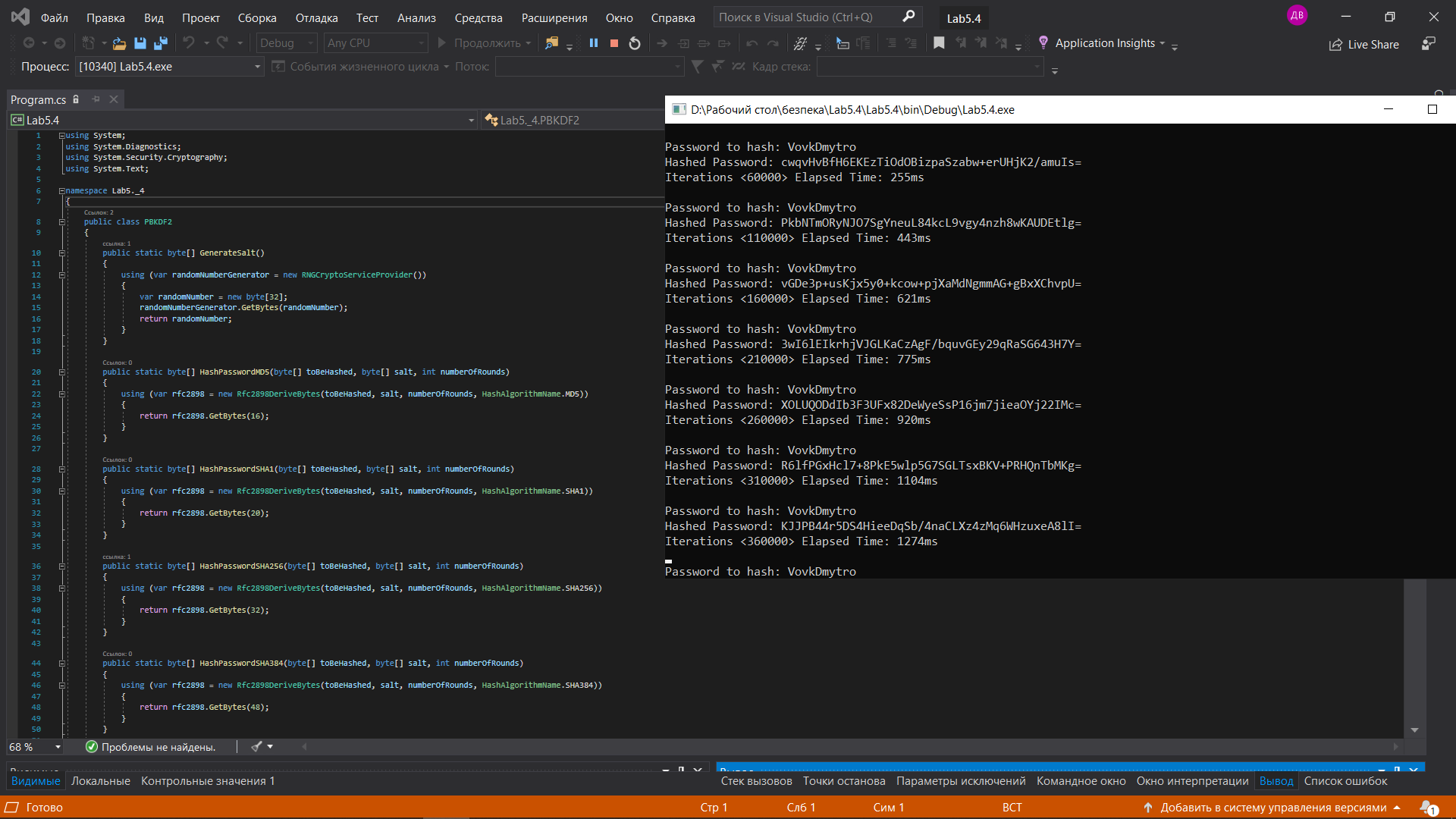
**Використання спеціальних функцій**

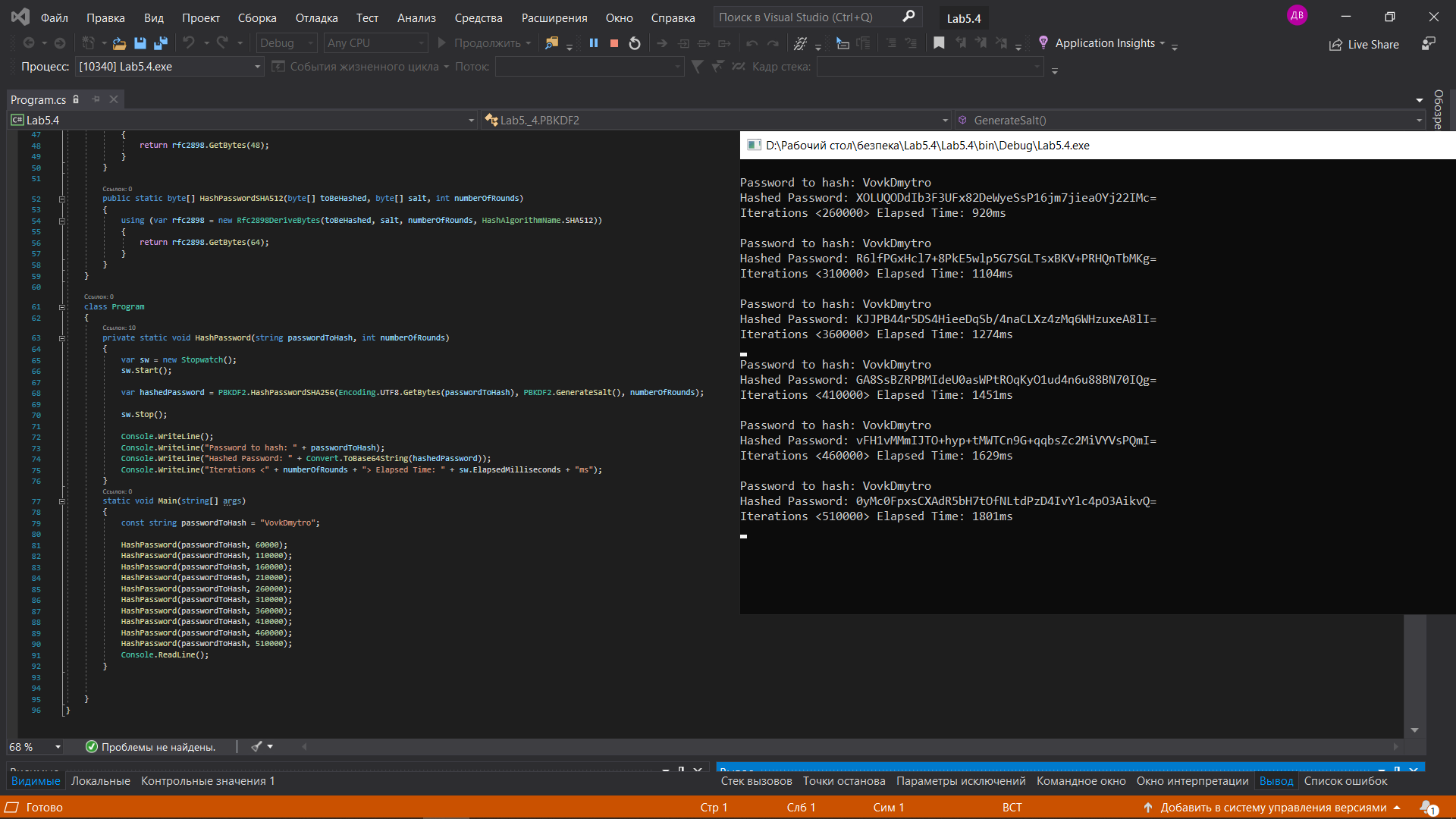
Цей метод є найбезпечнішим на данний момент для зберігання паролів, так як функції хешують вже захешовані паролі з сіллю десятки тисяч разів, що робить майже неможливим підбор паролю методом грубої сили.

Завдання 3



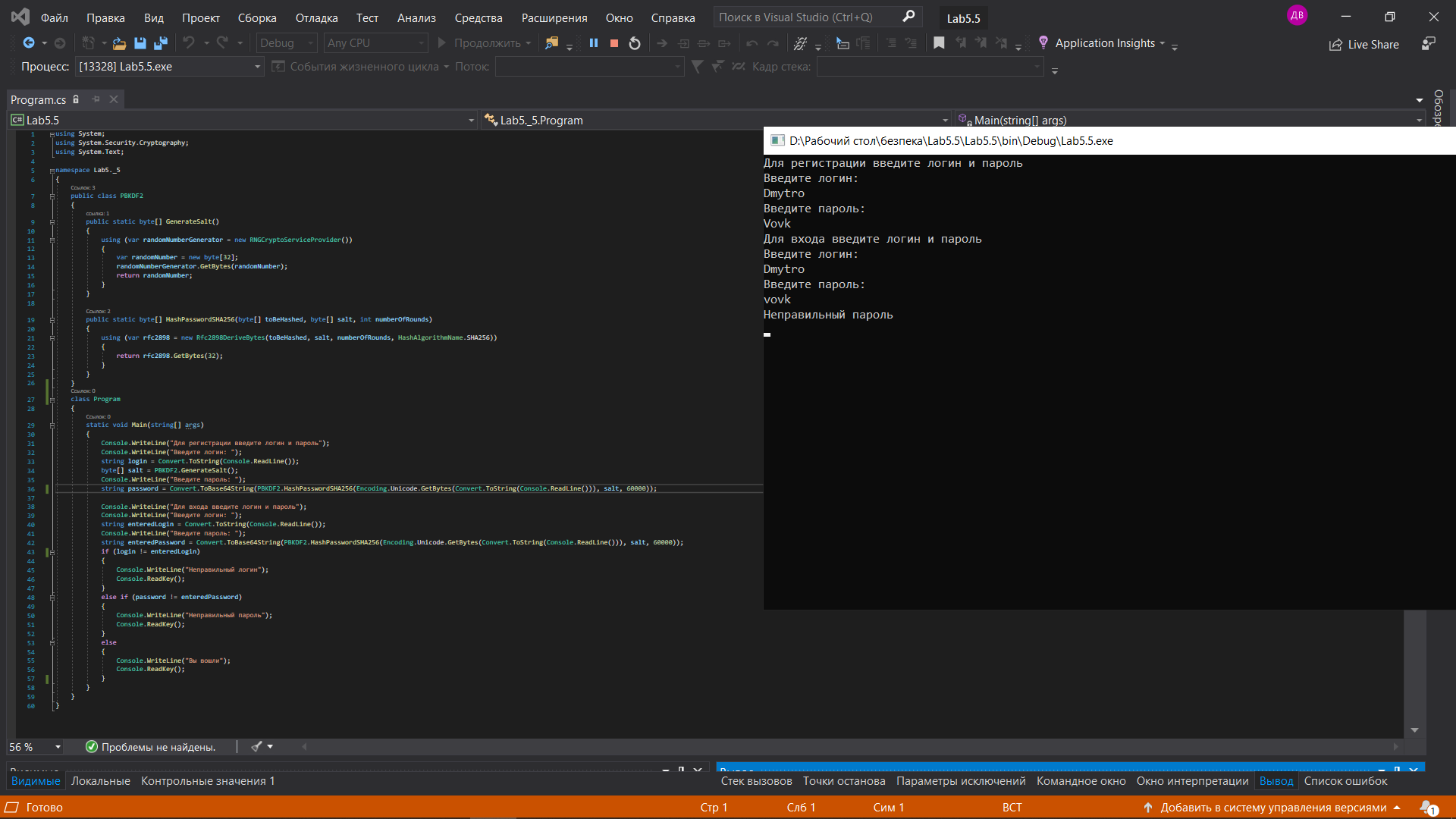
Завдання 4







Завдання 5



Висновки: під час виконання практичної роботи я навчився генерувати випадкову сіль, розібрався у різних методах зберігання паролів. Також я навчився хешувати паролі разом із сілюю, а також за допомогою спеціальних функцій реалізував найнадійніший метод зберігання.