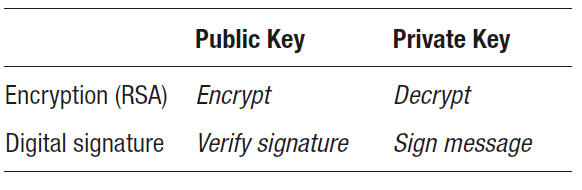
Звіт ПЗ\_9

МІТ-21 Квартюк Олексій

Тема: **«Електронний цифровий підпис»**

1. Написати програму, яка виконує підписування повідомлення та перевірку ЕЦП з використанням алгоритму асиметричного шифрування *RSA*. Відкритий ключ імпортується із XML-файлу, секретний – береться із контейнера.

****

Вимоги ЕЦП:

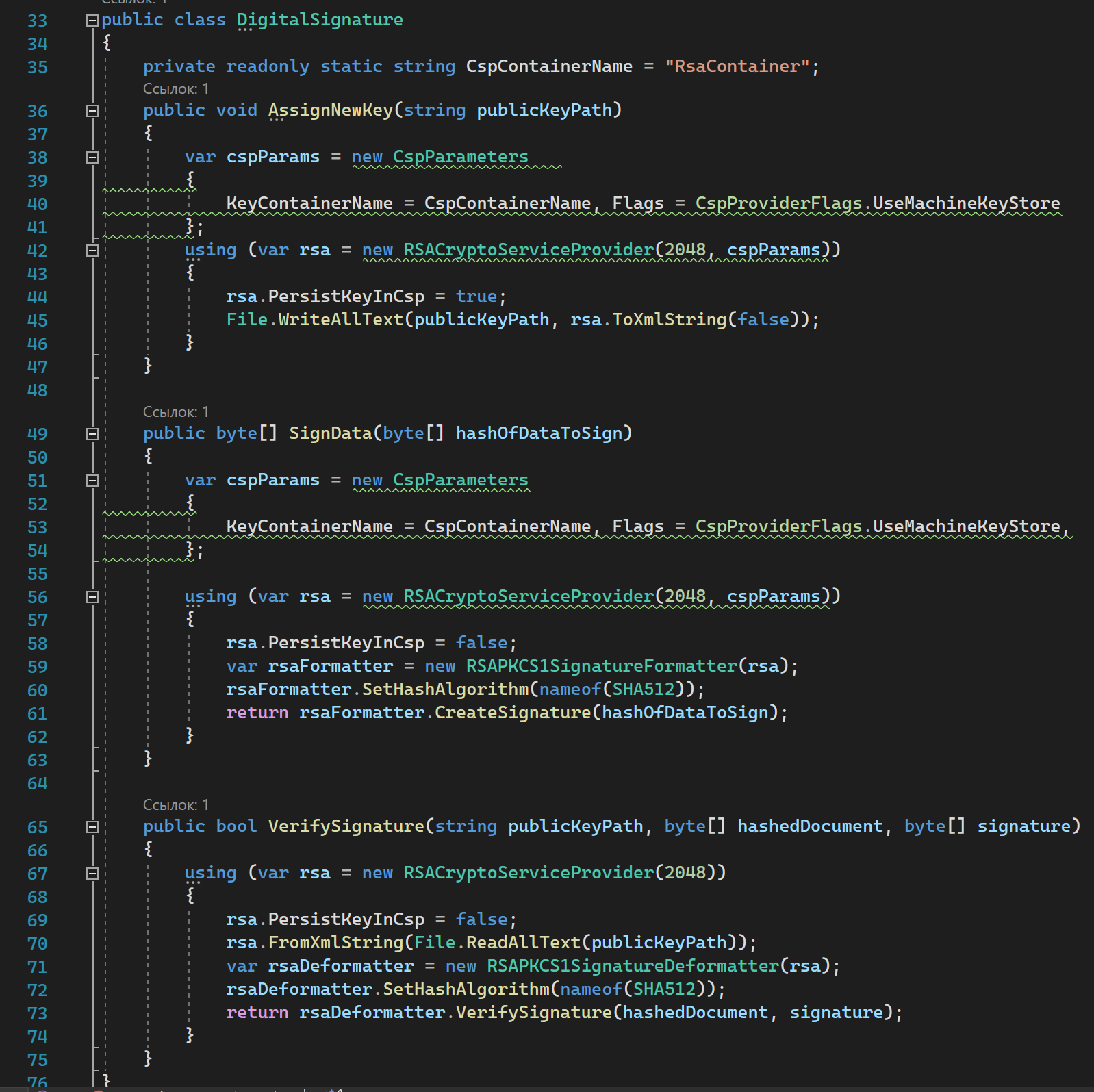
1) цифровий підпис має доводити, що саме законний автор, і ніхто інший, свідомо підписав документ;

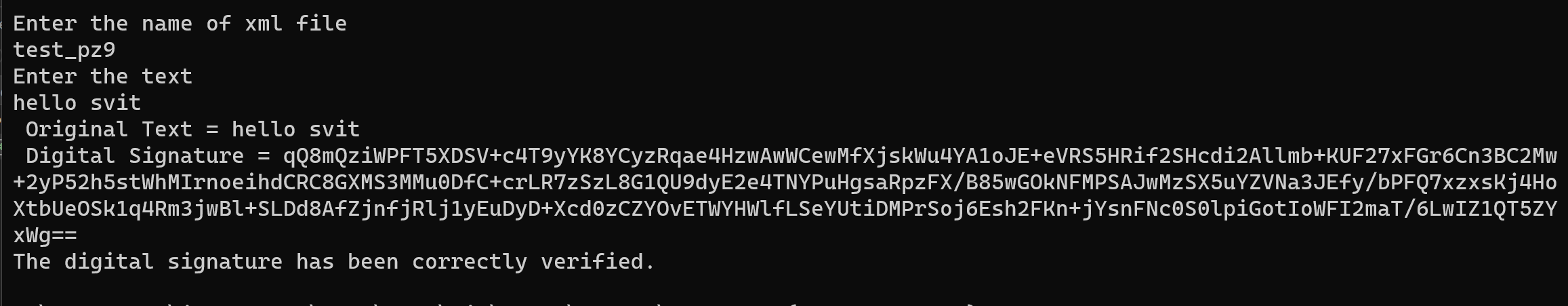
2) цифровий підпис має представляти собою невід’ємну частину документа. Має бути неможливим відокремлення підпису від документа і використання його для підписання інших документів;

3) цифровий підпис повинен забезпечувати неможливість зміни підписаного документа (в тому числі і для самого автора);

4) факт підписання документа повинен бути юридично-доказовим (забезпечення автентичності).







Опис коду:

В коді ми зберігаємо відкритий ключ в хмл файл, що вказали в консолі, а секретний ключ у контейнері. В основній програмі ми створюємо ключі модулем “AssignKey”. Хешуємо повідомлення, що отримали від вводу в консоль та передаємо ці данні у “SignData”, що обчислює ЕЦП. Далі у “VerifySignature” порівнюємо початковий відбиток з одержаним і виводимо на екран відповідний текст.

Висновок: Отже, ми навчились робити ЕЦП та перевіряти його на хибність, створивши відповідні програми.