Міністерство освіти і науки

Київський національний університет імені Тараса Григоровича Шевченка

Кафедра Мережевих та Інтернет технологій

**Звіт**

з практичної роботи **№9-10**

з дисципліни: “Основи інформаційної безпеки”

**«Електронні цифрові підписи»**

Виконав:

Студент групи МІТ-21

Горбун О. М.

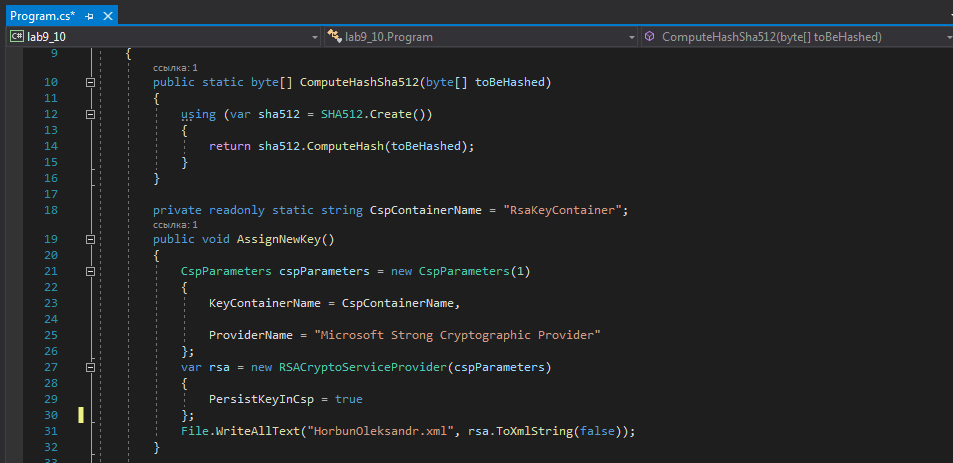
**Результати виконання завдань роботи:**

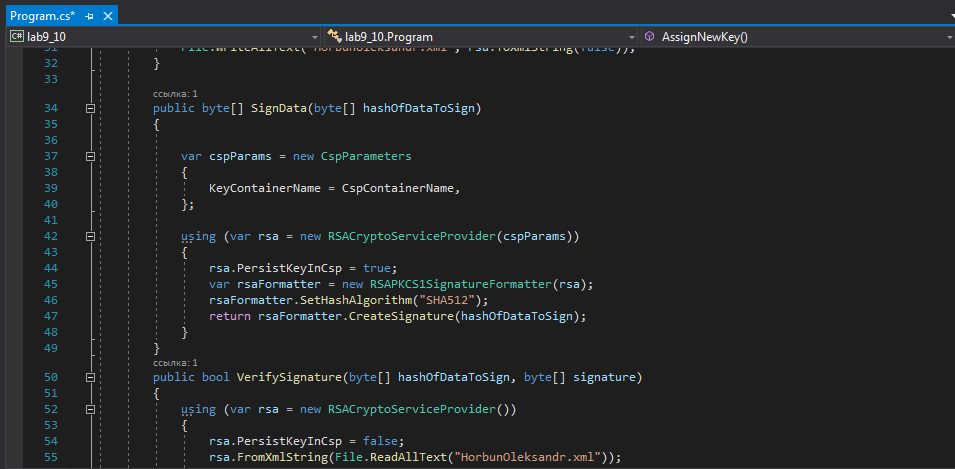
За завданнями практичної роботи було створено програму, яку можна переглянути за посиланням: <https://github.com/OleksandrHorbun/Basics_Cybersecurity.git> (Посилання на відкритий репозиторій у веб-сервісі GitHub) завдання у вітці (Branch) Homework\_9\_10.

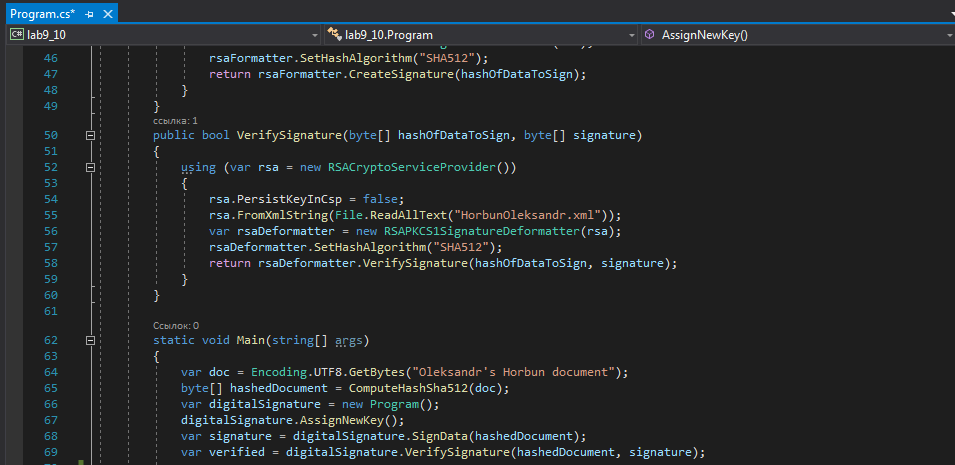
**I частина (перше завдання)**

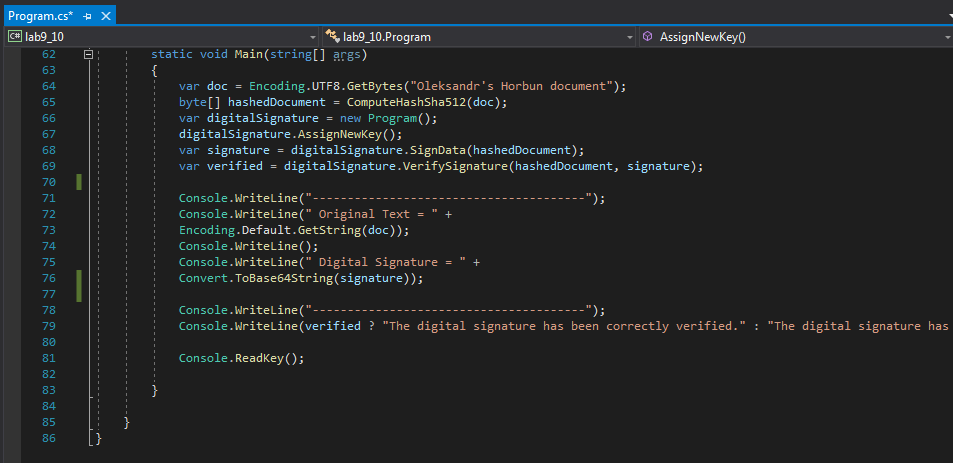
Як можна побачити, спочатку в програмі наявний деякий текст, який передається у функцію *ComputeHashSha512* (хешування за алгоритмом SHA512), отриманий хеш повертається у основну програму, після цього створюється змінна для цифрового підпису, яка є об’єктом класу програми, за допомогою функції *AssignNewKey* (отриманий результат також зберігається у контейнері ключів RSA) створюється новий цифровий підпис, після того як з’явився підпис, його можна накласти на документ за допомогою функції *SignData* (при цьому використовується RSAPKCS1SignatureFormatter). Далі можна перевірити підпис який тільки що був накладений на файл. Для цього була створена функція *VerifySignature* (після звірки підпису буде повернено boolean значення, якщо правильно - true). Ну і останнім кроком результат роботи програми буде виведено на екран.

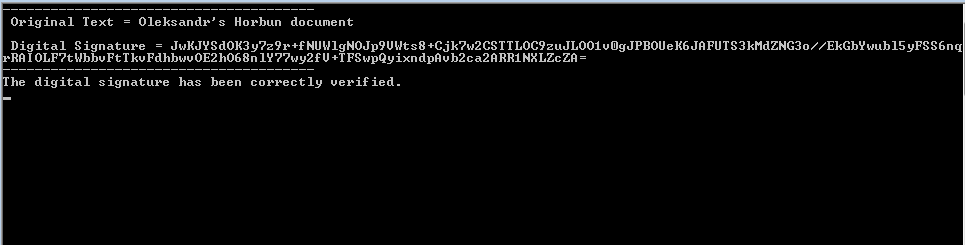
Все описане вище можна побачити на знімках екрану:











**Висновок:**

Виконуючи цю роботу я навчився проводити перевірку електронного цифрового підпису (ЕЦП) з використанням алгоритму асиметричного шифрування RSA, а також зрозумів як написати програму для створення цифрового підпису.