Міністерство освіти і науки

Київський національний університет імені Тараса Григоровича Шевченка

Кафедра Мережевих та Інтернет технологій

**Звіт**

з практичної роботи **№8**

з дисципліни: “Основи інформаційної безпеки”

**«Обмін зашифрованими повідомленнями»**

Виконав:

Студент групи МІТ-21

Горбун О. М.

**Результати виконання завдань роботи:**

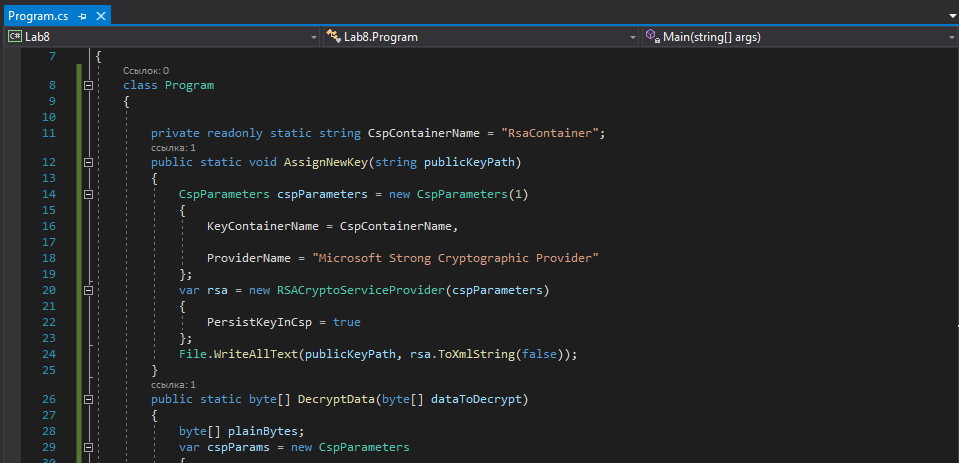
За завданнями практичної роботи було створено програму, яку можна переглянути за посиланням:

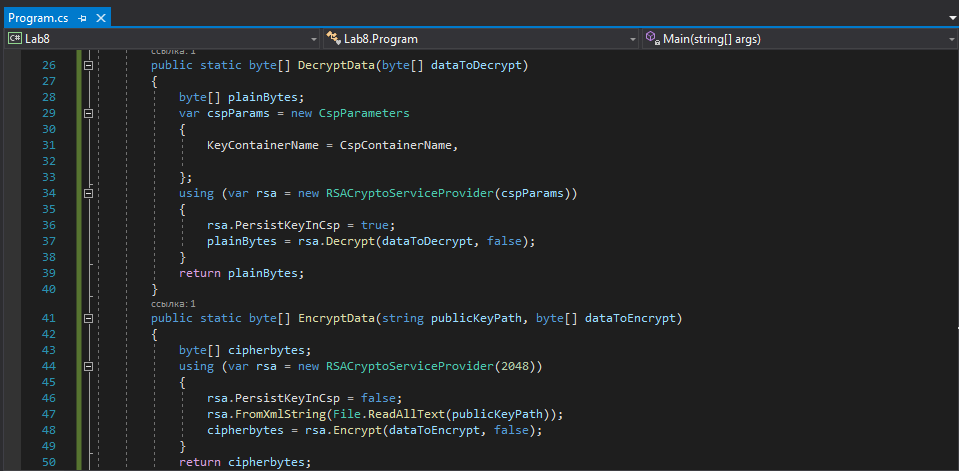
<https://github.com/OleksandrHorbun/Basics_Cybersecurity.git> (Посилання на відкритий репозиторій у веб-сервісі GitHub) завдання у вітці (Branch) Homework\_8.

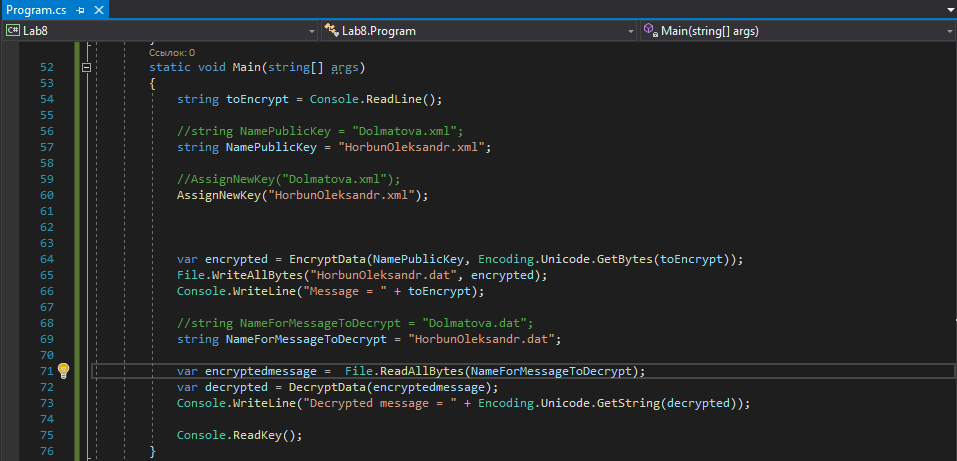
**I частина (третє завдання у завданні з практичної №7)**

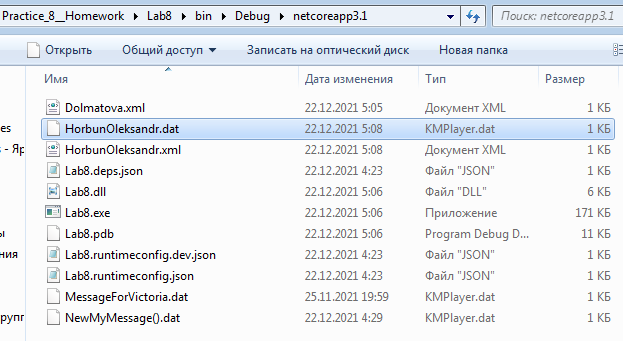
Як можна побачити у програмі можна ввести повідомлення, яке буде зашифровано за допомогою певного ключа, назву файлу.xml з якого публічний ключ буде імпортований це значення *NamePublicKey =* … Також треба створити ключ для розшифрування. Назву файлу куди його експортувати треба ввести у *AssignNewKey(…)*. При цьому буде застосована однойменна функція (вище написано рядок з її викликом у *Main*) *AssignNewKey* (вже була описана в минулих практичних) Повідомлення з ключем передаються для шифрування в функцію *EncryptData* (теж була описана у минулих практичних). Зашифроване повідомлення передається назад у основну частину програми та записується. Після цього змінна з зашифрованим повідомленням буде експортована до файлу. Назву файлу куди експортувати треба вписати у *File.WriteAllBytes("…",encrypted)*. Повідомлення (до шифрування) буде виведено додатково на екран. Наступним рядком іде змінна, куди треба вписати назву або адресу файлу для розшифрування. Тобто, це рядок *string NameForMessageToDecrypt = "…".* Зашифроване повідомлення зчитується з файлу й передається у функцію *DecryptData* (теж була вже багаторазово використана у минулих практичних роботах). У разі успіху розшифроване повідомлення буде виведено на екран.

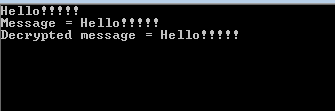
Все описане вище можна побачити на знімках екрану:











**Висновок:**

Виконуючи цю роботу я навчився приймати та відправляти зашифровані повідомлення, імпортувати та експортувати ключі для розшифрування або шифрування повідомлень та отримав базове уявлення як відбувається обмін зашифрованими повідомленнями у мережі Інтернет.