Звіт ПЗ\_7

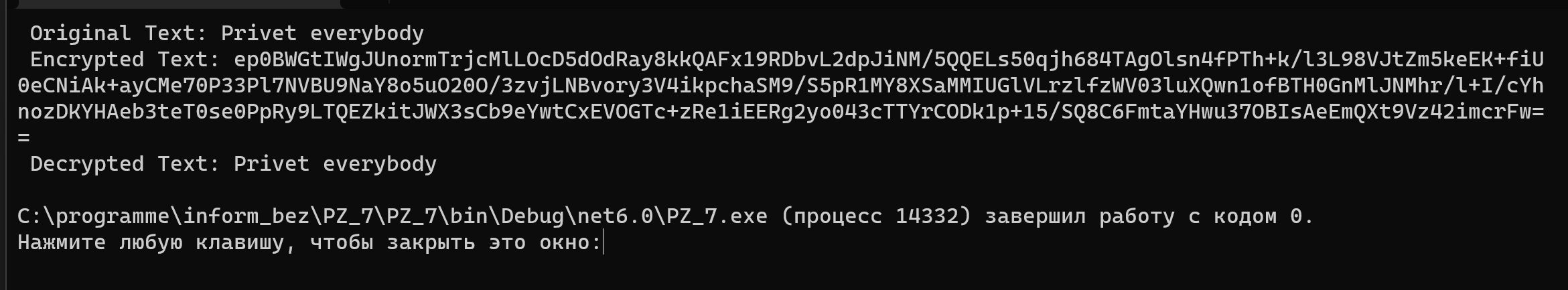
МІТ-21 Квартюк Олексій

Тема: **«Асиметричне шифрування як засіб забезпечення конфіденційності інформації»**

1) Написати програму, яка виконує зашифровування та розшифровування даних з використанням алгоритмів асиметричного шифрування RSA. Пара ключів зберігається у пам’яті.



У цьому коді пара ключів зберігається у пам’яті за допомогою \_publicKey, \_privateKey з довжинаю 2048 біт.



2-3) Для програми з п.1. реалізувати можливість збереження відкритого ключа у файлі. Реалізувати можливість зашифровувати повідомлення за допомогою файлів відкритих ключів інших користувачів.

Згенерувати відкритий (!!!) ключ *RSA 2048bit* та зберегти у файл з іменем, що відповідає транслітерації прізвища, та розширенням *xml*. Поділитися збереженим відкритим ключем у Телеграм-каналі. Зашифрувати та надіслати вітання двом (наступним за списком) студентам. Отримані вітання розшифрувати та вивести на екран.

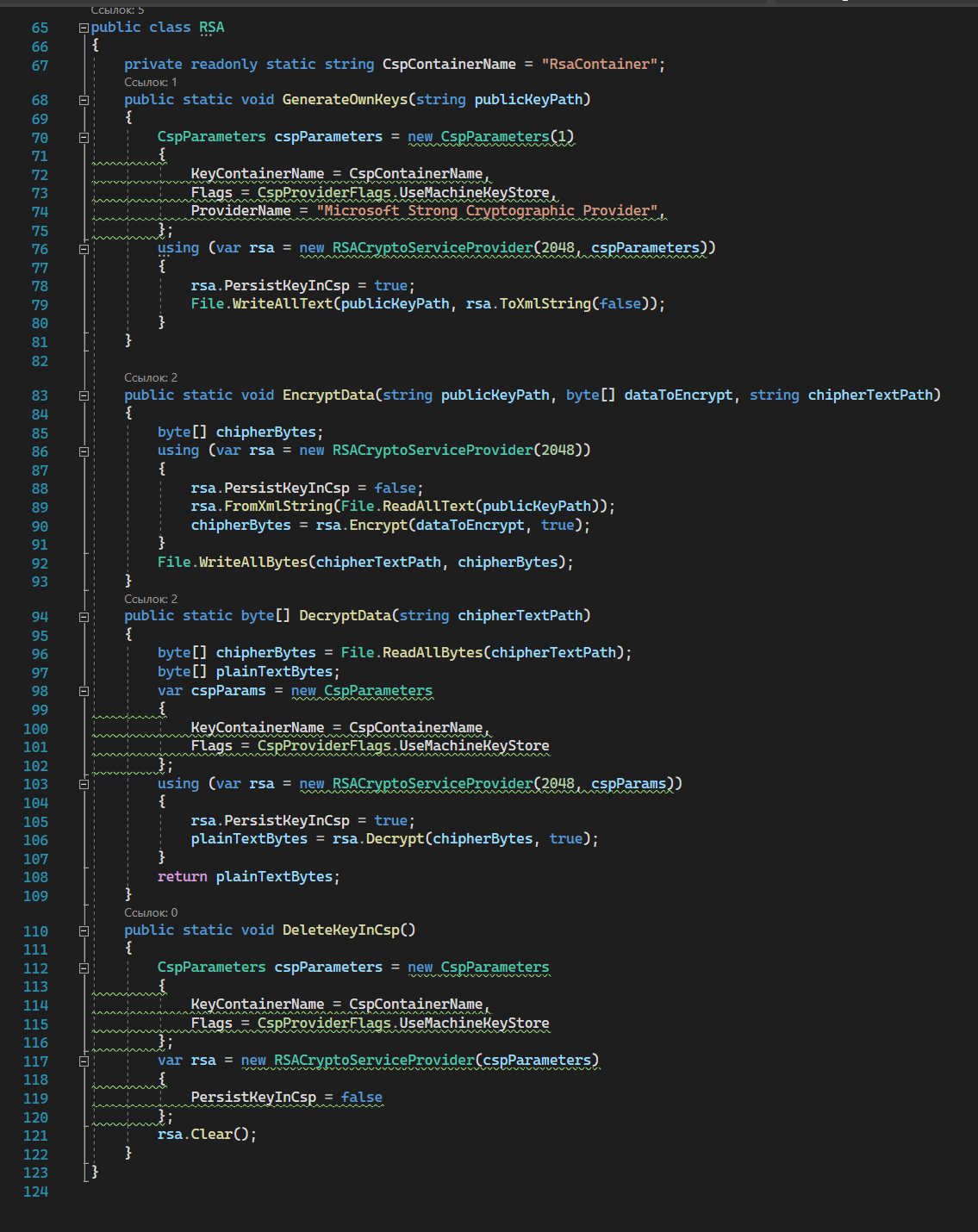
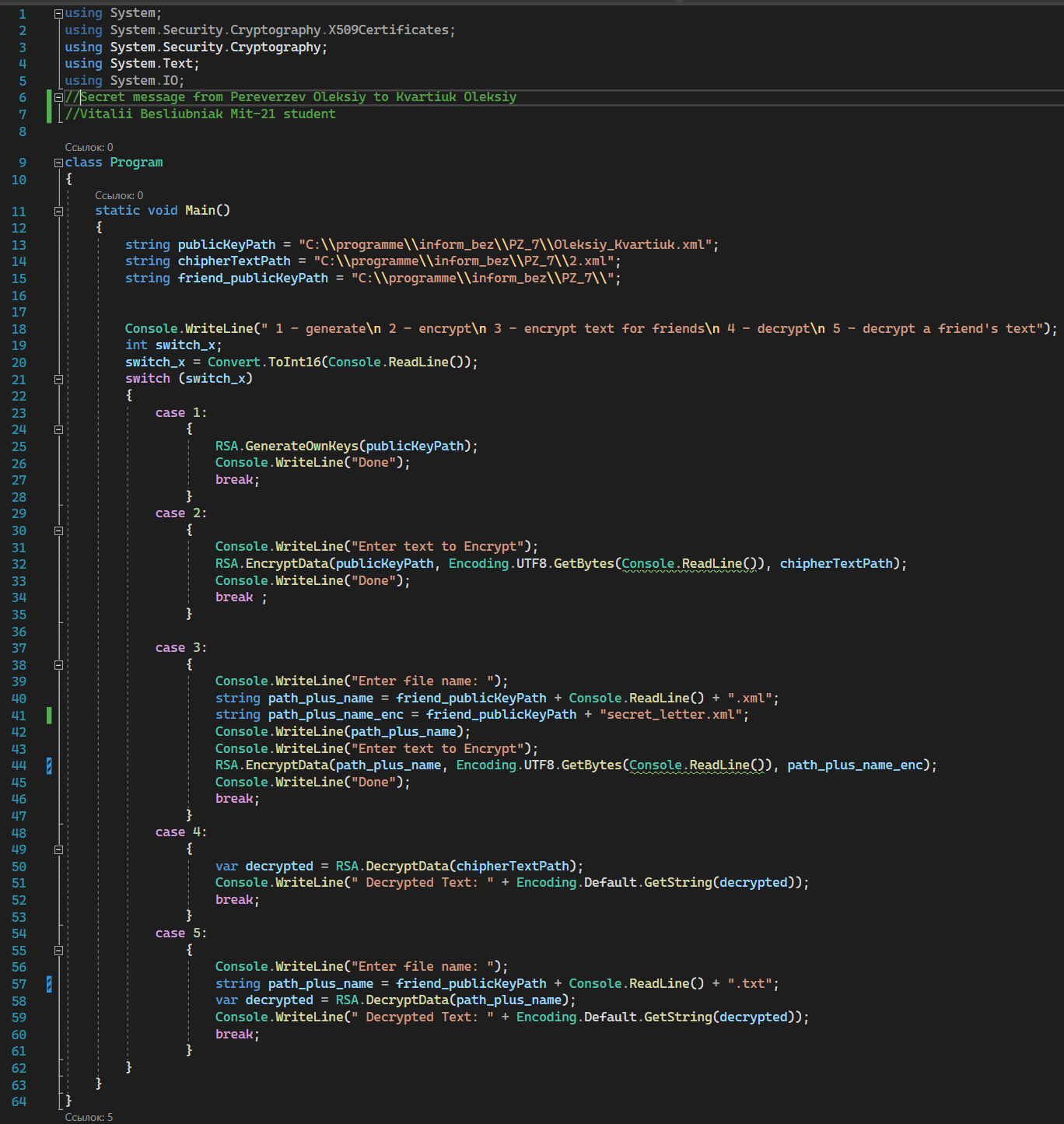
Вже у цьому коді після виконання методу “**generate**” відкритий ключ зберігається в xml файл, а закритий у контейнер, що називається cryptographic service provider.

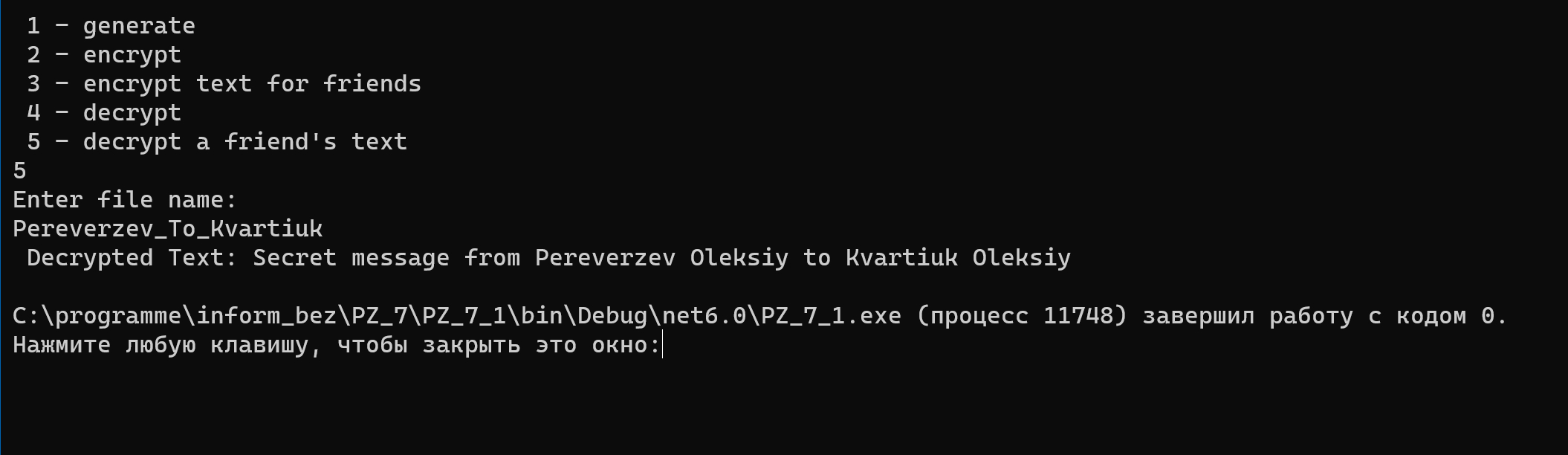
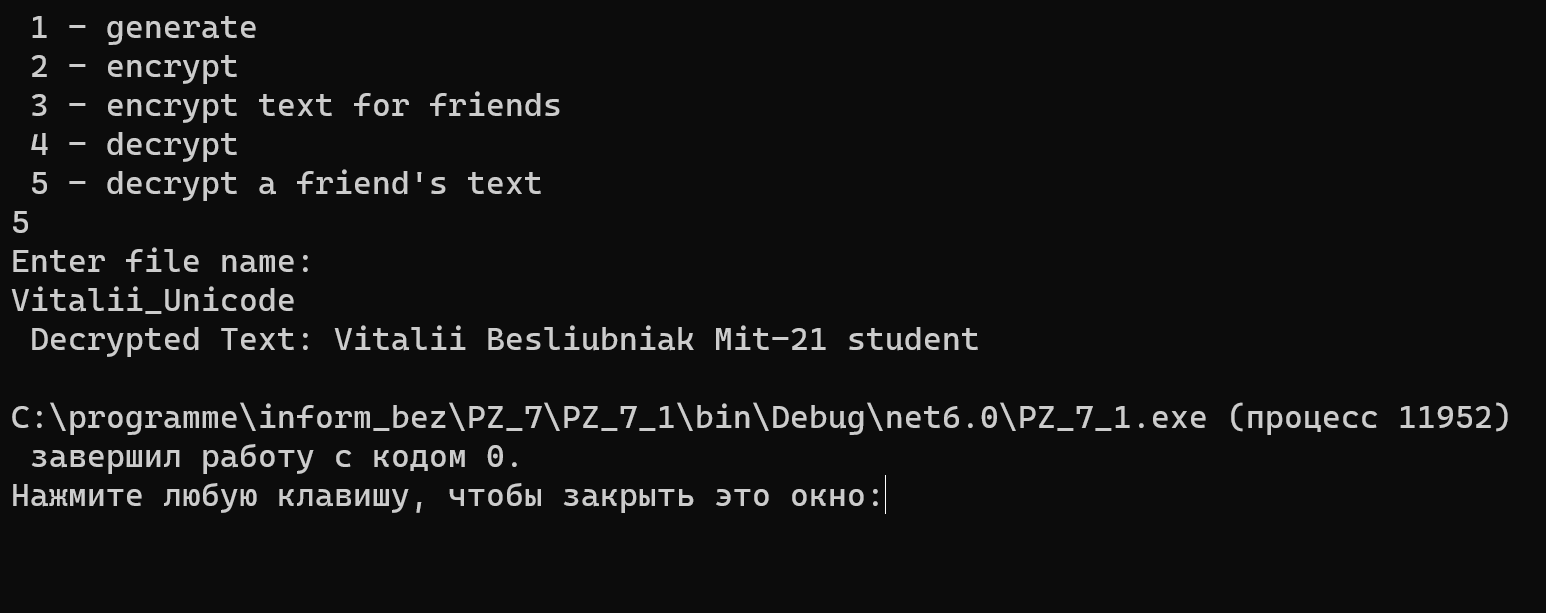
Метод “**encrypt**” використовує раніше згенерований відкритий ключ та текст, що в подальшому шифруються, після чого зашифроване повідовлення заноситься в xml файл.

**Encrypt for friends** робить теж саме, що й encrypt, проте використовую відкритий ключ, що ми отримали від одногрупників. Далі надсилаємо це повідомлення відправнику ключа, щоб він розшифрував його.

**Decrypt** розшифровує раніше зашифроване повідомлення(у нашому коді enctypt і decrypt працюють разом), а **decrypt a friend's text** потрібен для розшифрування повідомлення від одногрупників.

Отже, я надіслав у наш телеграм свій відкритий ключ, після чого отримав та розшифрував повідомлення від Переверзева Олексія та Беслюбняка Віталія(скріни нижче).





**Висновок:** Отже, ми навчилися використовувати асиметричне шифрування з використанням контейнера. А також обмінялися повідомленнями та ключами з групою для перевірки працездатності кода на практиці.