МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

ІКТА

кафедра ЗІ



З В І Т

до лабораторноїроботи №5

з курсу: «Основи криптографічного захисту інформації»

на тему: «Електронний цифровий підпис»

Виконала: ст. гр. УІ-42

Симоненко Д.С.

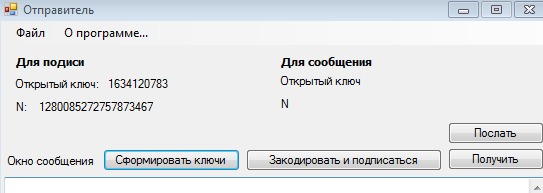
Прийняв: Шандра З.А.

Львів – 2017

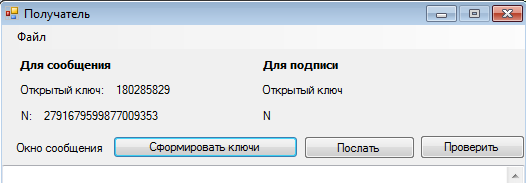
**Мета роботи:** ознайомлення із задачами, які розв’язує електронний цифровий підпис (ЕЦП), вивчення протоколу створення ЕЦП методом застосування алгоритму RSA.

**Виконання**

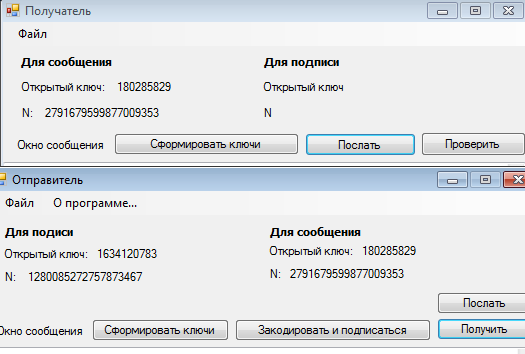
Згенерувати ключі відправника А, на екрані висвітлюється тільки відкритий ключ А.



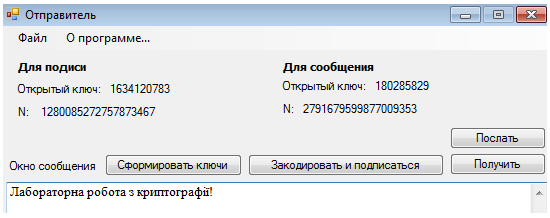
Згенерувати ключі отримувача B, на екрані висвітлюється тільки відкритий ключ B.

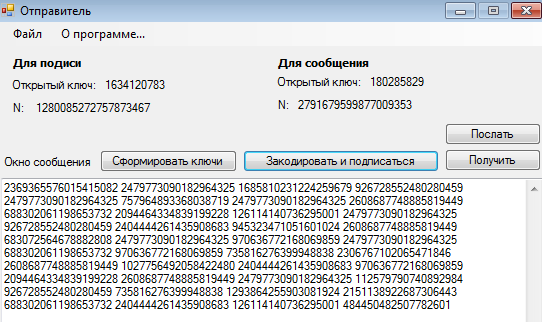


Послати відкритий ключ B відправнику А, після чого натиснути «отримати » відправником А. На екрані А висвітлюється відкритий ключ B.

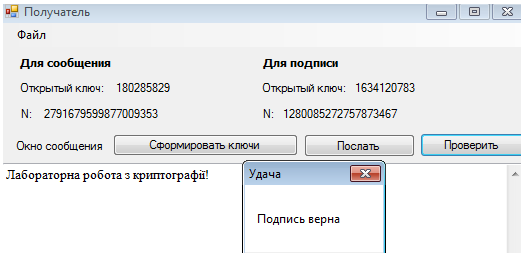


Відправник А створює повідомлення, шифрує його і надсилає отримувачу B (кнопка «надіслати»).





Отримувач B перевіряє справжність отриманого від А повідомлення, результат перевірки подається в окремому віконці.



Отримувач B спочатку сам обчислює хеш-значення H отриманого документа, далі дешифрує отримане хеш-значення з використанням відкритого ключа відправника A, після чого порівнює обидва значення.

**Висновок:** під час лабораторної роботи я ознайомилась із задачами, які розв’язує електронний цифровий підпис (ЕЦП), вивчила протокол створення ЕЦП методом застосування алгоритму RSA.