Криптографія

Комп’ютерний практикум №4

Вивчення криптосистеми RSA та алгоритму електронного підпису;

ознайомлення з методами генерації параметрів для асиметричних

криптосистем

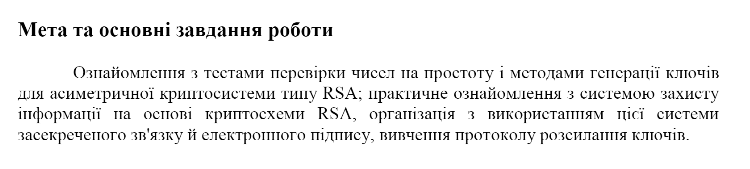
Виконали

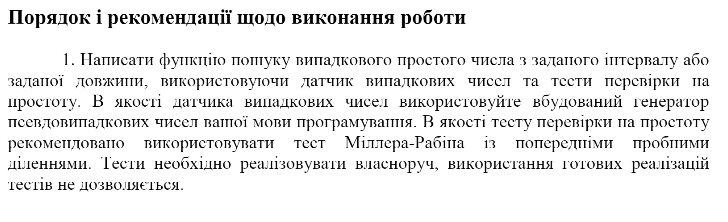
Студенти 3-го курсу

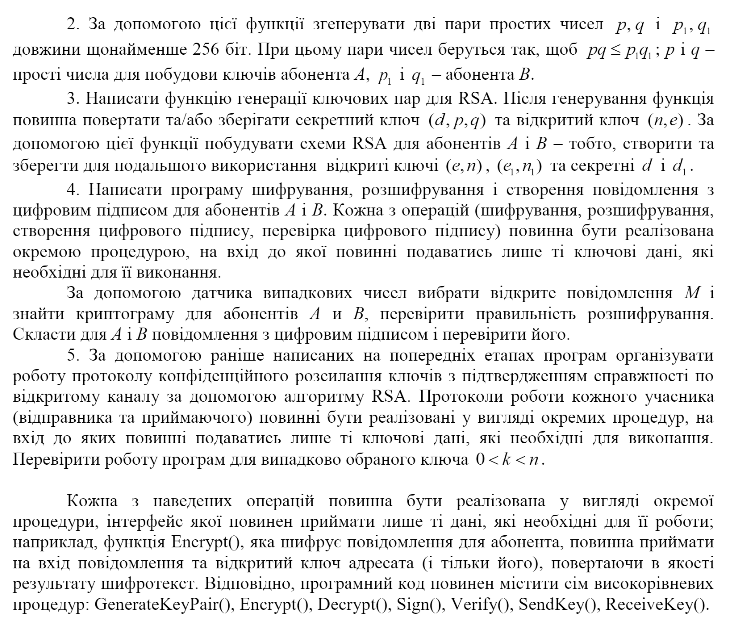
Групи ФБ-02

Замрій Денис та

Гнатюк Максим



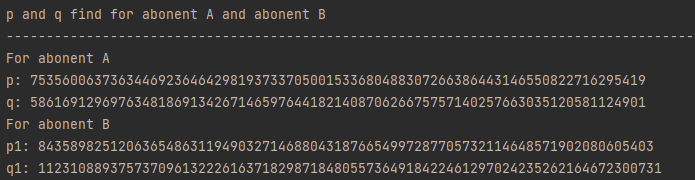




**Хід роботи**

Реалізували функції Gen\_random\_number() та Miller-Rabin() для генерації p та q, p1 та q1,

та перевірки їх на простоту.

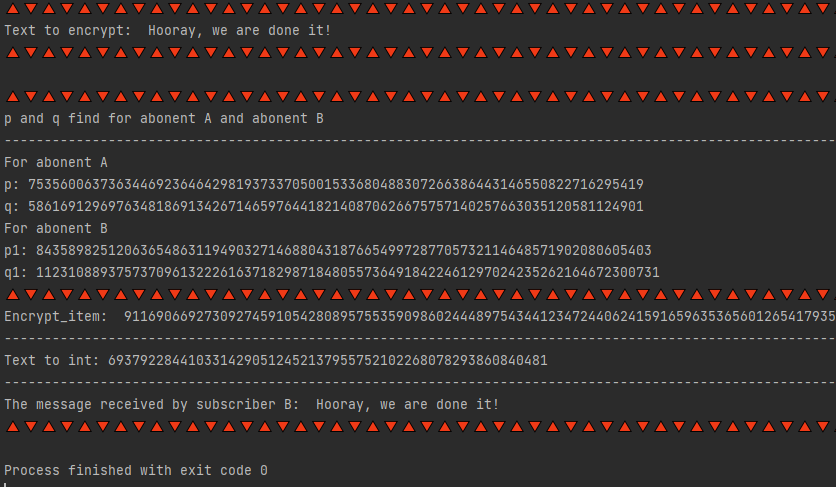


Також написали функцію GenerateKeyPair() для пошуку n, phi(n), e, d

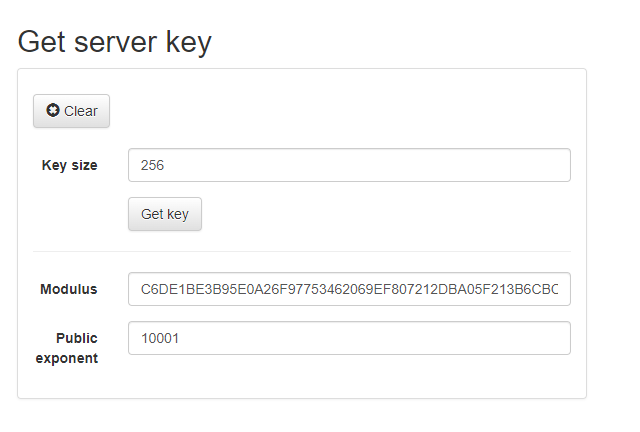
Де n = p\*q, phi(n) – функція Ейлера, e – відкритий ключ, d – таємний ключ

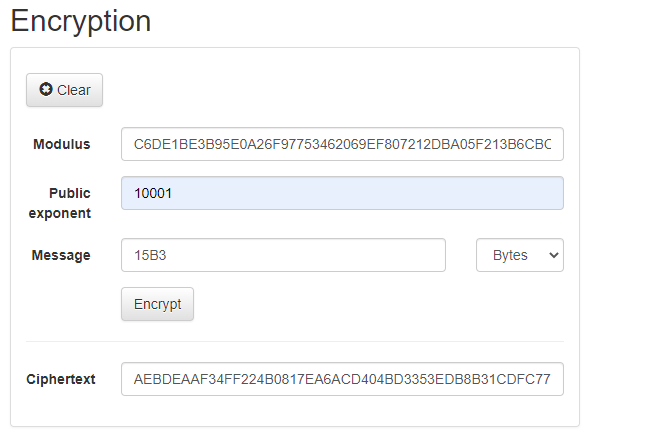
Далі шифруємо наше повідомлення

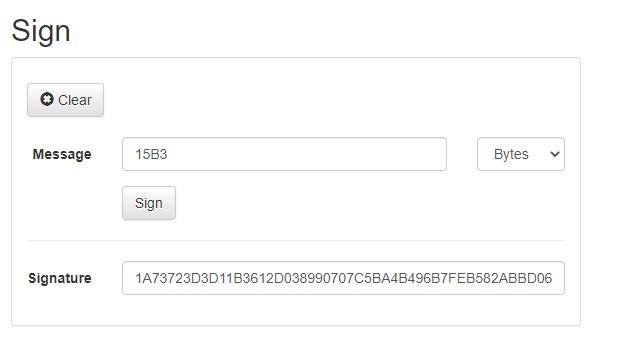
Для прикладу взяли текст «Hooray, we are done it!»

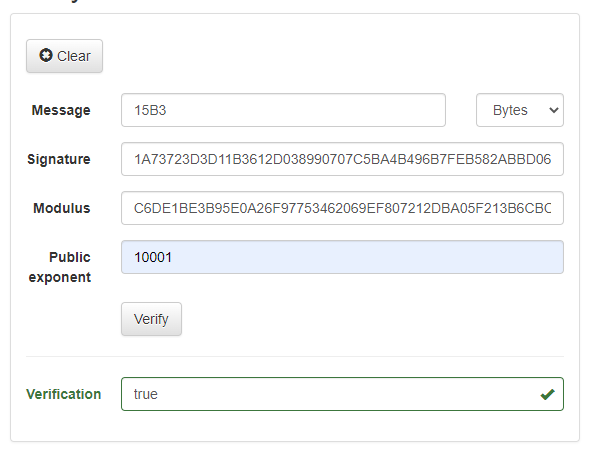


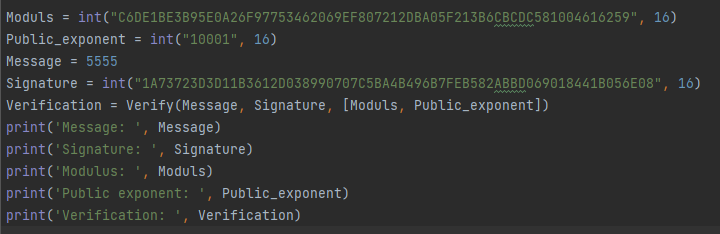


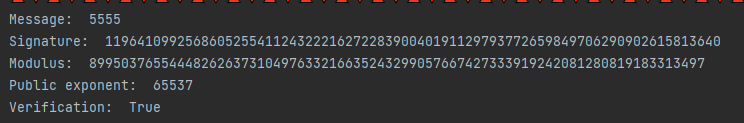


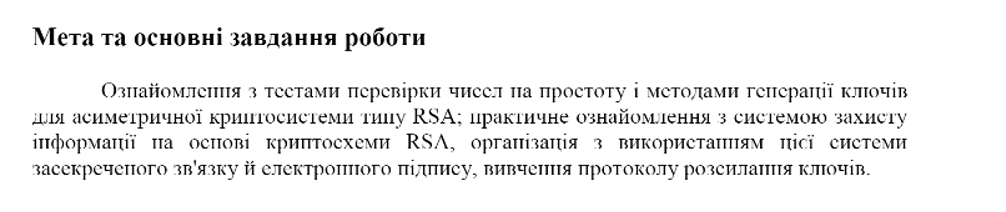












**Висновок:**

**В ході цієї лабораторної роботи ми ознайомилися з тестами чисел на простоту і методами генерації ключів для асиметричної криптосистеми RSA, та практично закріпили знання.**

**Навчилися створювати електронний підпис.**