**МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»**

ФІЗИКО- ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра інформаційної безпеки

# КОМП’ЮТЕРНИЙ ПРАКТИКУМ №4

з дисципліни Криптографія

# З теми: «Вивчення криптосистеми RSA та алгоритму електронного підпису; ознайомлення з методами генерації параметрів для асиметричних криптосистем»

Перевірила: Виконав студент

групи ФБ-94

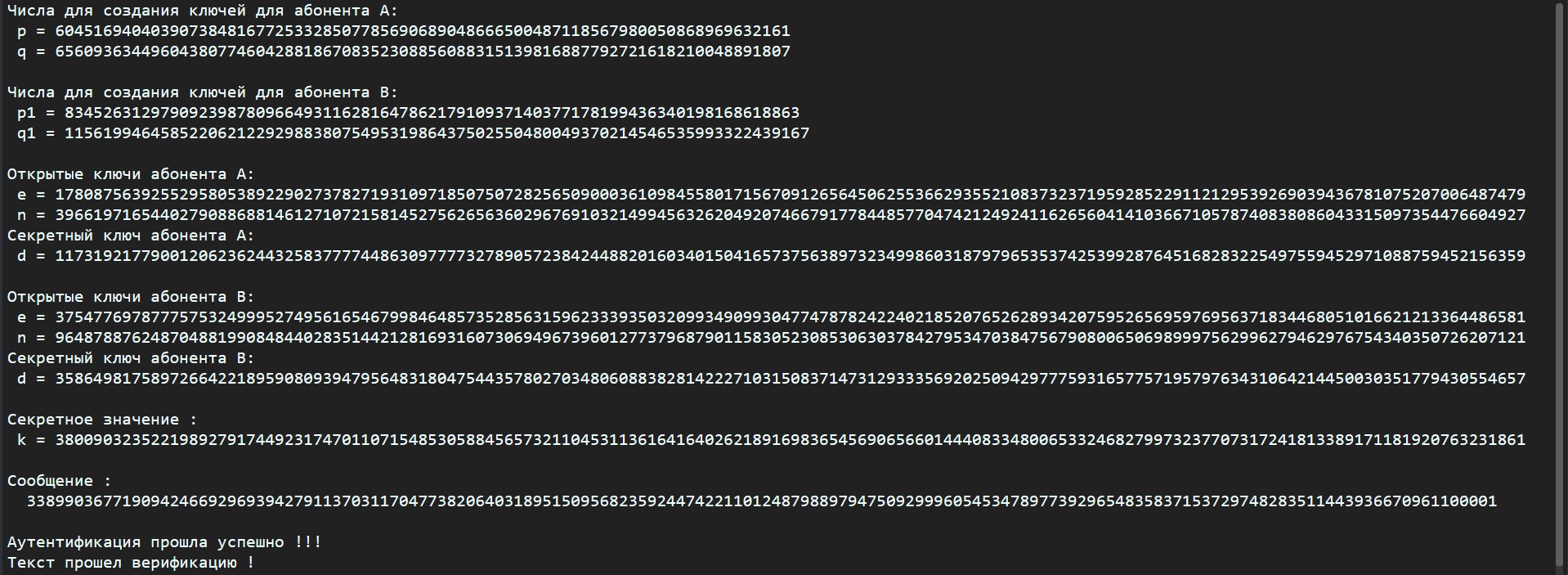
Селюх П.В Артюшенко В.В.

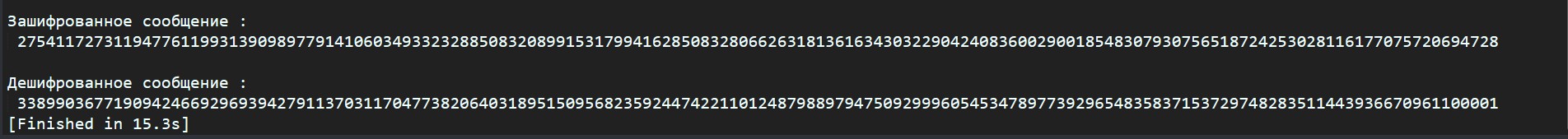
## Мета та основні завдання роботи:

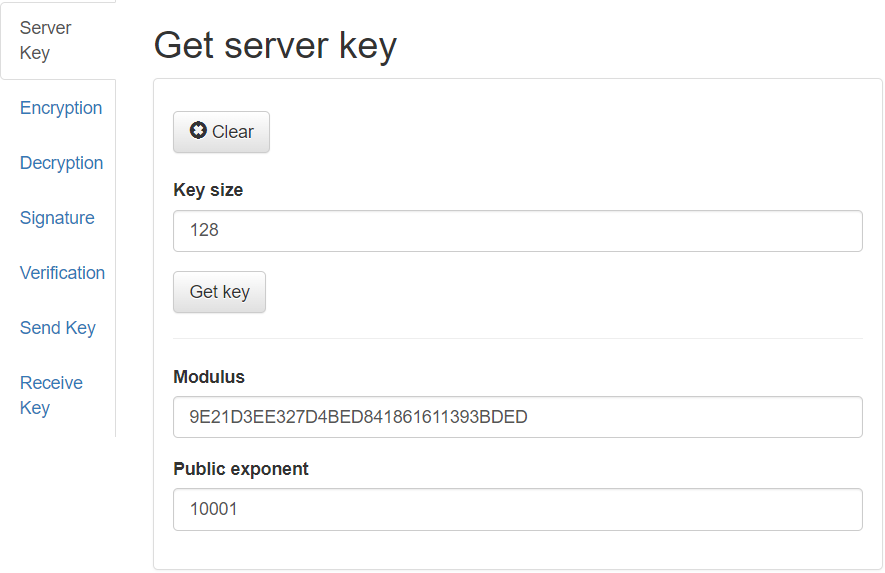
Ознайомлення з тестами перевірки чисел на простоту і методами генерації ключів для асиметричної криптосистеми типу RSA; практичне ознайомлення з системою захисту

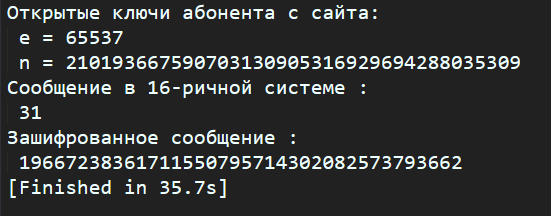
інформації на основі криптосхеми RSA, організація з використанням цієї системи засекреченого зв'язку й електронного підпису, вивчення протоколу розсилання ключів.

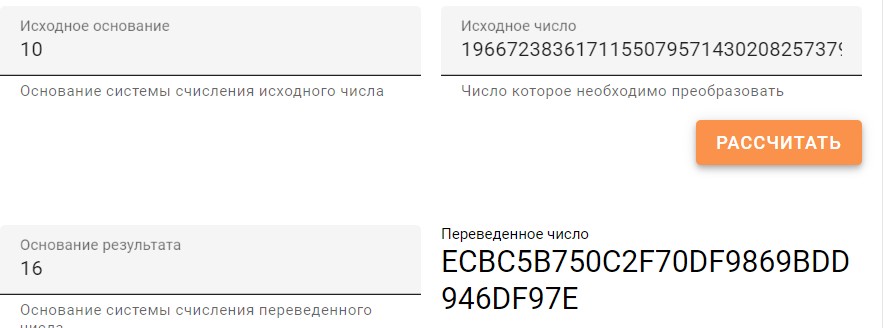
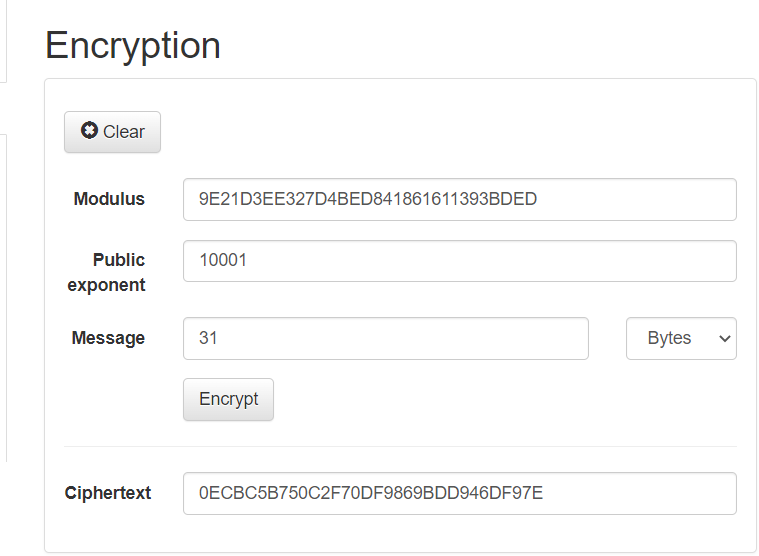
## Результат роботи програми:

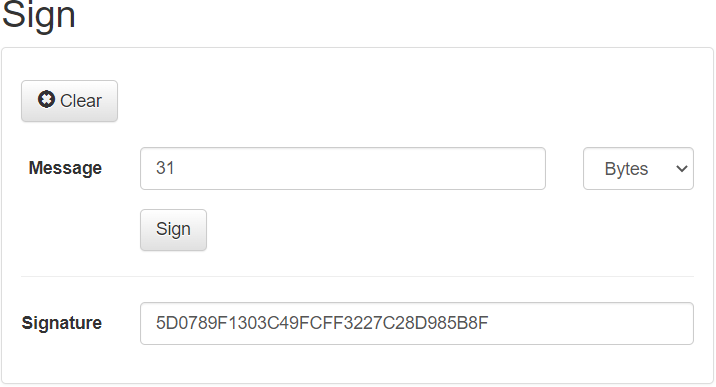


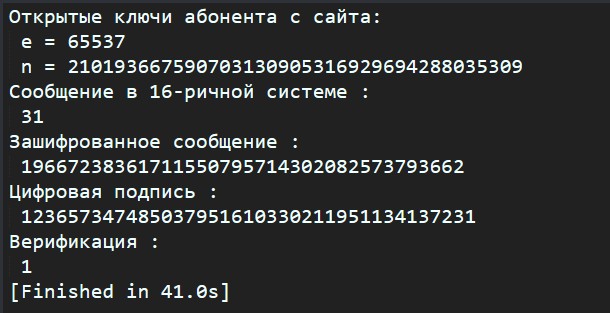
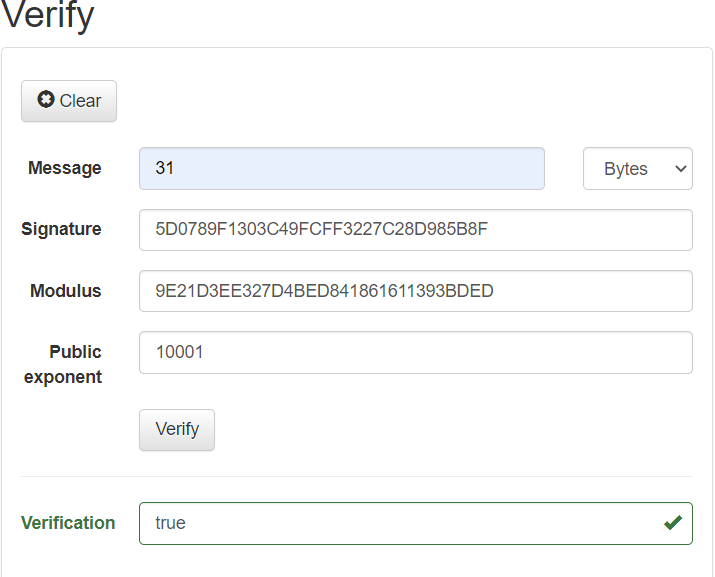




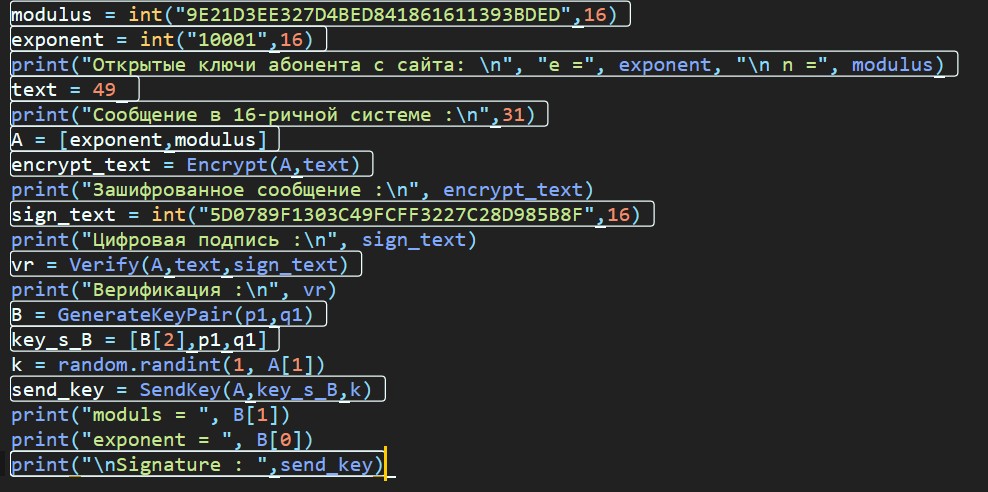








**Код:**



## Висновок:

Під час виконання комп’ютерного практикуму я ознайомився з тестами перевірки

чисел на простоту і методами генерації ключів для асиметричної криптосистеми типу RSA. А також з системою захисту інформації на основі криптосхеми RSA, з використанням цієї системи засекреченого зв'язку й електронного підпису.

Вивчив протокол розсилання ключів.