МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»

Фізико-технічний інститут

Криптографія

Комп’ютерний практикум №4

Виконали:

Студенти групи ФБ-05

Сапожник М.В.

Карась Б.І.

Київ - 2022

**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.

**Хід роботи:**

В рамках виконання практикуму було створено функції:

sign - функція для підпису повідомлення

SiCh - перевірка надісланого підпису

Encrypt- зашифровує повідомлення

Decrypt-розшифровує повідомлення

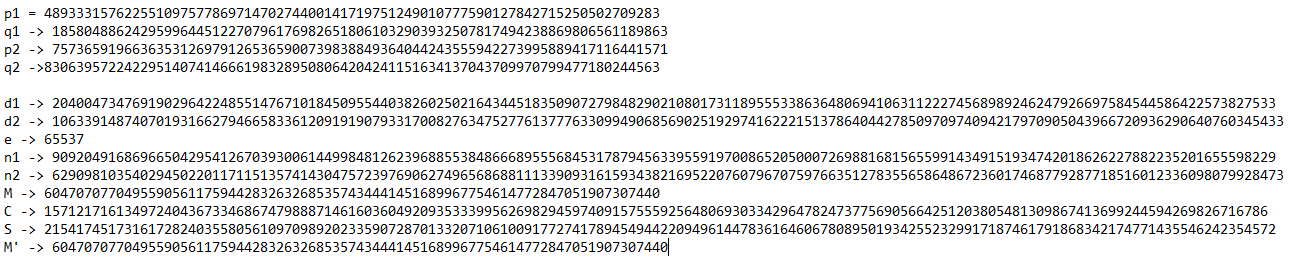
rsa\_pair - генеруватиме d,n,e

TestPrime – тестує початкове число на простоту

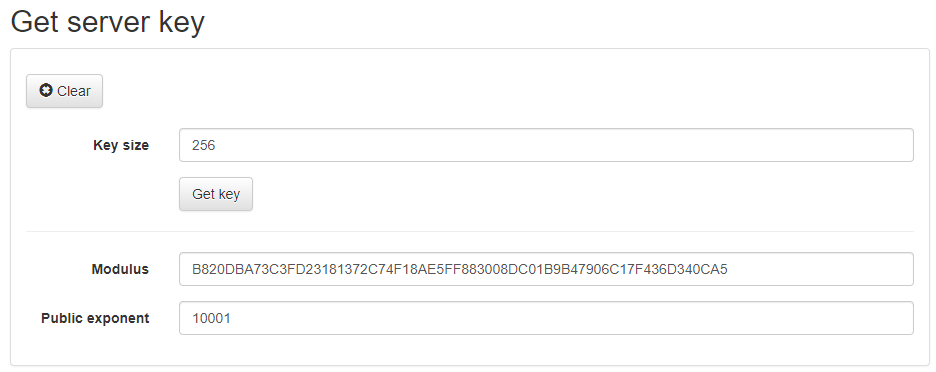
g\_c\_d – розширений алгоритм Евкліда

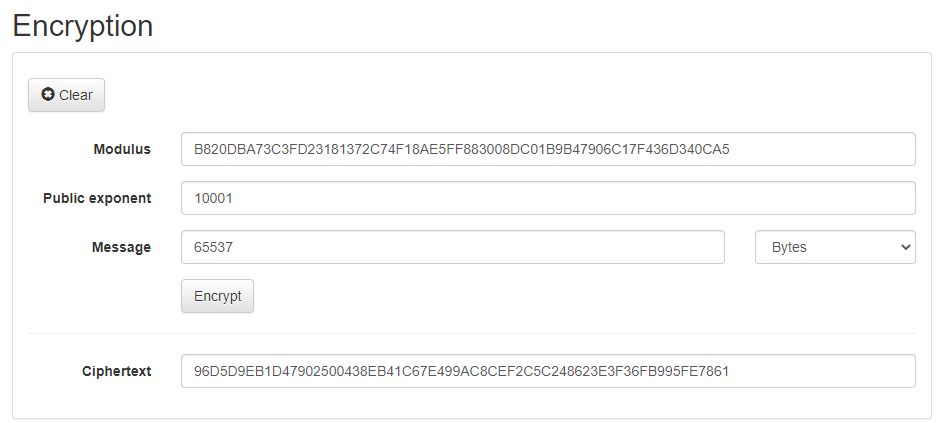
f\_unc –перевірка шляхом теста Міллера

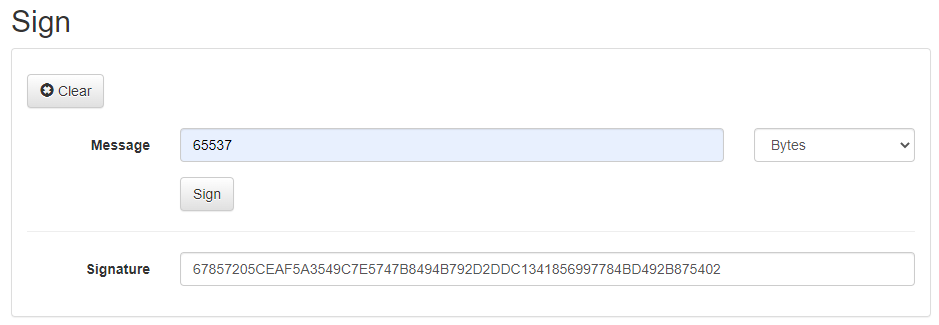
Вивід виконання програми:

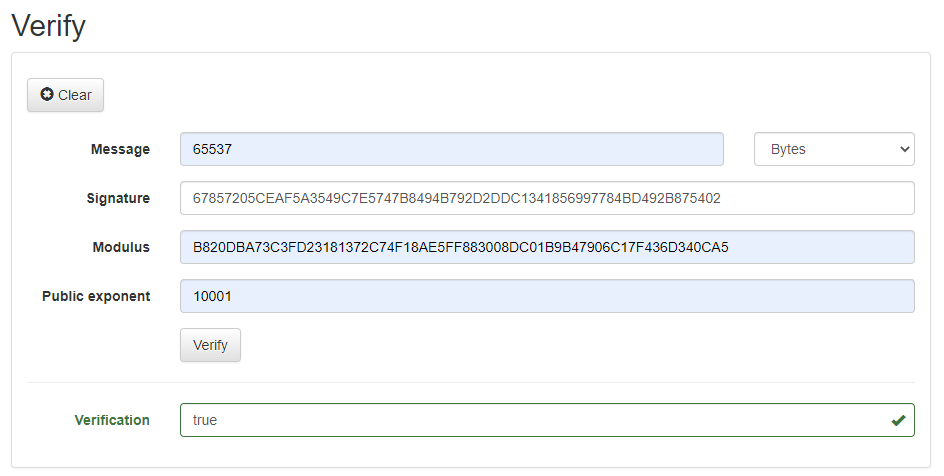


Починаємо перевірку за сайтом

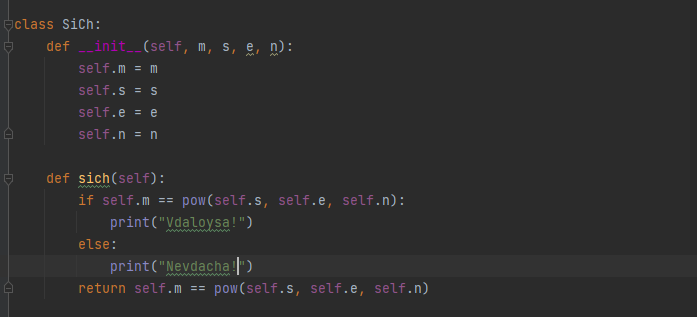


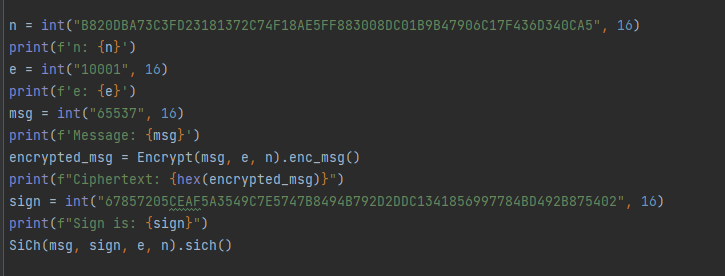


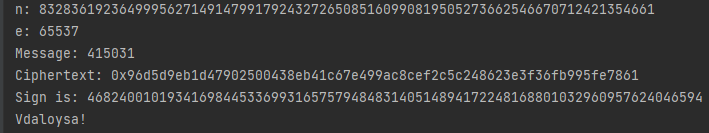




Переробимо деякі моменти у коді для перевірки та додамо деякі значення:







**Висновки**

В результаті виконання практикуму ми практично ознайомились з системою захисту інформації на основі криптосхеми RSA. Було засвоєно і практично використано тест Міллера-Рабіна для перевірки чисел на простоту і генерації простих чисел. Мали змогу використати Asym Crypto Lab Environment і з його допомогою перевірити нами створені функції криптосхеми RSA.