Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

Криптографія

Лабораторна робота №4

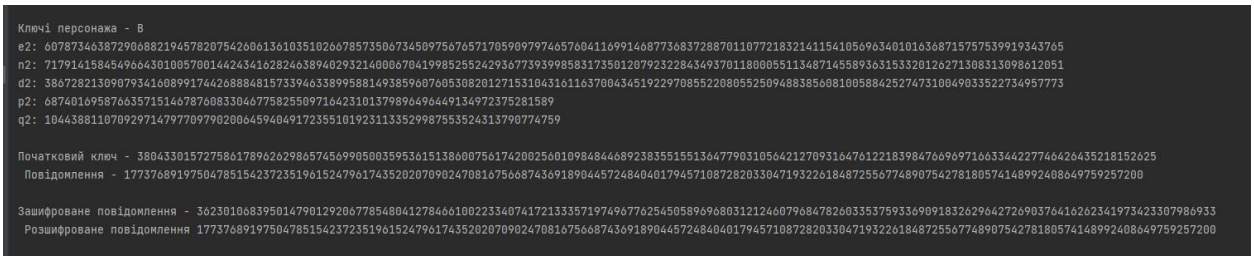
Варіант 8

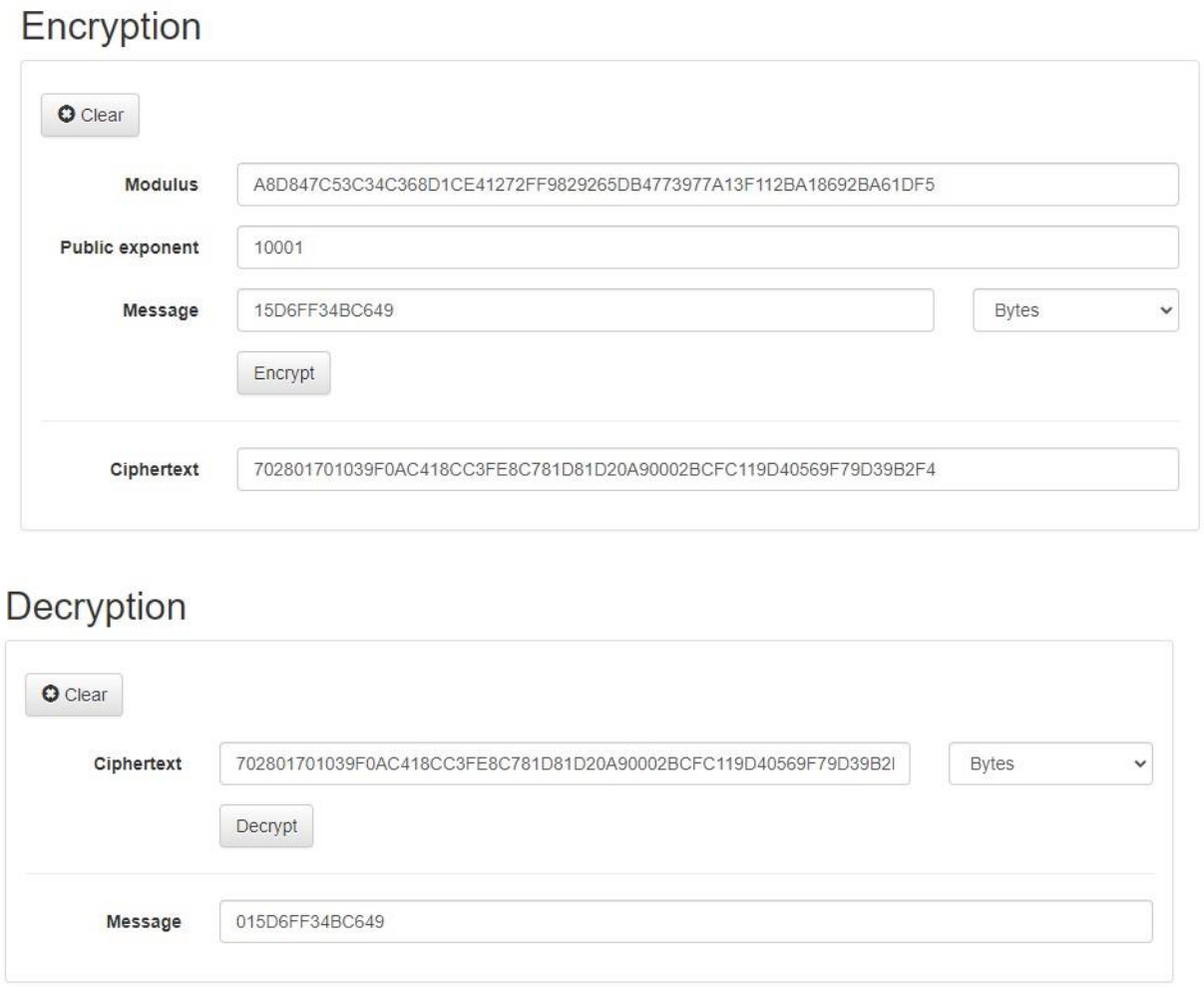
Виконав:
студент 3 курсу ФТІ
групи ФБ-05
Тимченко Юрій

Перевірила:
Селюх П.В.

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.





Висновки : під час виконання лабораторної роботи ми отримали навички реалізації та розуміння роботи критпосистеми RSA, алгоритму електронного підпису та генерації ключів та простих чисел, їх перевірка на простоту ймовірнісним тестом Міллера-Рабіна.