Протокол лабораторної роботи №4

Вивчення криптосистеми RSA та алгоритму електронного

підпису; ознайомлення з методами генерації параметрів для

асиметричних криптосистем

Варіант №7

Виконав

Студент 3 курсу

Групи ФБ-13

Короткевич Іван

**Мета 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.

Код програми:

Створення 256 битного числа та перевірка числа на простосту:

A screen shot of a computer program

Description automatically generated

Знаходження простого чилса:

A screenshot of a computer program

Description automatically generated

Шифрування, дешифрування, створення підпису та перевірка повідомлення:

A screen shot of a computer program

Description automatically generated

Відправлення та отримання ключа:

A screenshot of a computer program

Description automatically generated

Приклад роботи програми:

A black background with white and blue lines

Description automatically generated

Програма може зберігати ключі у спеціальному файлі keys.json

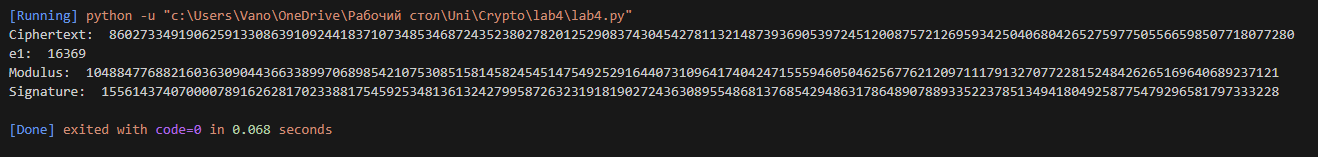
Перевірка роботи:

Повідомлення: 12345

Для перевірки роботи значення треба було перевести в 16-ти систему счислення:

A screenshot of a computer

Description automatically generated



A screenshot of a calculator

Description automatically generated

A black background with colorful text

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated

A black screen with white text

Description automatically generated