Лабораторна робота з криптології

Виконав Поліщук Олександр ІПС-32

Варіант 13

У обох завданнях вхідний метод – start().

Щоб перевірити виконання завдання, потрібно створити об’єкт класу відповідного завдання та викликати метод start() (див. main.py).

Значення параметрів потрібно змінювати безпосередньо в класах.

1. RSA (клас RSA)

Нам потрібно зашифрувати та розшифрувати повідомлення (натуральне число)

Алгоритм виконання:

1. Обираємо прості числа:

E = 1289  
Q = 1283  
P = 1279

E, P\*Q – частини відкритого ключа

1. Знаходимо обернене число до E за модулем за допомогою методу A\_find\_d()
2. Шифруємо та розшифровуємо повідомлення за допомогою методів B\_encrypt\_message та A\_decrypt\_message відповідно
3. Diffie-Hellman Protocol (клас DHP)

Завдання: створити симетричні ключі для Аліси та Боба.   
Алгоритм:

1. Обираємо випадковим чином приватні ключі для Аліси та Боба

Alices\_private\_key = random.randint(2, 40)  
Bobs\_private\_key = random.randint(2, 40)

1. Обчислюємо публічні ключі на основі приватних

compute\_public\_key(self,power)

1. Обмінюємось ключами та знаходимо симетричні ключі

compute\_symmetric\_key(self,public\_key, private\_key)