Федеральное государственное бюджетное образовательное учреждение
высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА
И ГОСУДАРСТВЕННОЙ СЛУЖБЫ
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

НИЖЕГОРОДСКИЙ ИНСТИТУТ УПРАВЛЕНИЯ – филиал РАНХиГС

Факультет управления
Кафедра Информатики и информационных технологий
Направление подготовки / специальность: 09.04.03 Прикладная информатика

Отчет по лабораторной работе

по дисциплине: Информационная безопасность

АВТОР
Обучающаяся 3 курса группы ИК-732
заочной формы обучения

_____ Насурллаев И. Е.
(подпись) *(фамилия, инициалы)*

РУКОВОДИТЕЛИ
Гордеев Андрей Борисович
(ученая степень, ученое звание)

оценка _____
«_____» _____ 2024 г.
(дата защиты)

_____ Гордеев А.Б..
(подпись) *(фамилия, инициалы)*

Нижний Новгород, 2024г.

Оглавление

Лабораторная работа 3 3
Выполнение задания: 4
Приложение 5

Лабораторная работа 3

Название: Ассиметричные алгоритмы шифрования данных

Цель: освоить методику работы ассиметричных алгоритмов шифрования, где существует два ключа – один для шифрования, другой для дешифрования.

Вариант: 7

Задание:
Разработать консольное приложение для генерации ключей.

Комментарий:

Класс RSA, который содержит переменные:

- p и q - простые различных числа;
- n – произведение простых чисел p и q;
- t – НОК для p и q;
- e – произвольное число такое, что $1 < e < \Phi(n)$ и не имеет общих делителей, кроме 1 (взаимно простое) с числом $(p – 1) \cdot (q – 1)$;
- d – вычисляется методом Евклида таким образом, что $(e \cdot d – 1)$ делится на $(p – 1) \cdot (q – 1)$.

Методы _n(), _t(), _e() и _d() выполняют соответствующие операции над этими переменными, а метод _super_metod объединяет их значения. Конструктор init() принимает параметры p и q и вызывает метод _super_metod(). Метод see() выводит информацию о значениях переменных, выводя открытую пару и закрытую пару ключей.

Два числа (e, n) публикуются как открытый ключ.

Число d хранится в секрете – закрытый ключ есть пара (d, n), который позволит читать все послания, зашифрованные с помощью пары чисел (e, n).

Выполнение задания:
Код представлен в приложении.

Результат работы алгоритма:

```
p =  12
q =  13

p = 12
q = 13
n = 156
t = 132
e = 19
d = 7

open_duo(19,156)
close_duo(7,156)
```

Приложение

```
from math import lcm, gcd
from random import choice
class RSA:
    p = 0
    q = 0
    n = 0
    t = 0
    e = 0
    d = 0

    def _n(self):
        self.n = self.p * self.q

    def _t(self):
        self.t = lcm((self.p-1), (self.q-1))

    def _e(self):
        e_list = []
        for e in range(2, self.n):
            if gcd(e, self.t) == 1 and e > 1 and e < self.t:
                e_list.append(e)
        self.e = choice(e_list)

    def _d(self):
        self.d = pow(self.e, -1, self.t)

    def _super_metod(self):
        self._n()
        self._t()
        self._e()
        self._d()



    def __init__(self, p, q):
        self.p = p
        self.q = q
        self._super_metod()
```

```
    def see(self):
        print(f"""
p = {self.p}
q = {self.q}
n = {self.n}
t = {self.t}
e = {self.e}
d = {self.d}

open_duo({self.e},{self.n})
close_duo({self.d},{self.n})
        """)

p = int(input("p = "))
q = int(input("q = "))
rsa = RSA(p, q)
rsa.see()
```