Министерство образования и науки РФ

Федеральное государственное автономное

образовательное учреждение высшего образования

«Университет ИТМО»

**факультет программной инженерии и компьютерной техники**

**ЛАБОРАТОРНАЯ РАБОТА № 2.1**

по дисциплине

‘Информационная безопасность’

‘Атака на алгоритм шифрования RSA посредством метода Ферма’

Вариант №19

*Выполнил:*

Студент группы P34111

Павлов Александр Сергеевич

*Преподаватель:*

Маркина Т.А.

Изображение выглядит как Шрифт, логотип, Графика, белый

Автоматически созданное описание

Санкт-Петербург, 2024

# Цель работы

Изучить атаку на алгоритм шифрования RSA посредством метода Ферма.

# Программные и аппаратные средства

Процессор: Intel Core i5-11400F 2.6GHz 12 ядер

Видеокарта: NVIDIA GeForce RTX 2060

Объем оперативной памяти: 32 GB

Язык программирования: Python

# Задание

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

# Ход работы

1. Вычисляем
2. Вычисляем
3. Возводим в квадрат
4. Вычисляем
5. Проверяем, если – квадрат целого числа. Если нет – возвращаемся ко второму пункту
6. Вычисляем
7. Вычисляем
8. Вычисляем
9. Вычисляем
10. Производим дешифрацию шифрблока
11. Переводим дешифрацию шифрблока в текстовый вид

# Листинг разработанной программы с комментариями

from math import sqrt

N = 59046883376179

e = 4044583

C = '''32279109612093

17838629182964

4165776716262

13093284635895

20048651313008

54626454832531

12801053743903

54675332003643

4544911979279

31928373564570

798945495513

19569174668782'''

answer = ""

n = int(sqrt(N)) + 1

i = 0

while True:

    i += 1

    t = n + i

    w = t \*\* 2 - N

    if int(w \*\* 0.5) != w \*\* 0.5:

        continue

    sqrt\_w = w \*\* 0.5

    break

p = t + sqrt\_w

q = t - sqrt\_w

phi = (p - 1) \* (q - 1)

d = pow(e, -1, int(phi))

i = 0

for num in C.split("\n"):

    i += 1

    m = pow(int(num), d, N)

    part = m.to\_bytes(4, byteorder='big').decode('cp1251')

    answer += part

print(f"n = {n}")

print(f"p = {p}")

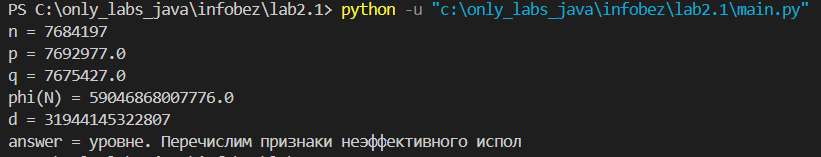
print(f"q = {q}")

print(f"phi(N) = {phi}")

print(f"d = {d}")

print(f"answer = {answer}")

# Результаты работы программы



# Выводы по работе

В ходе выполнения данной лабораторной работы я ознакомился с атакой на алгоритм шифрования RSA посредством метода Ферма.