Министерство образования и науки РФ

Федеральное государственное автономное

образовательное учреждение высшего образования

«Университет ИТМО»

**факультет программной инженерии и компьютерной техники**

**ЛАБОРАТОРНАЯ РАБОТА № 2.2**

по дисциплине

‘Информационная безопасность’

‘Атака на алгоритм шифрования RSA методом повторного шифрования’

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 повторного шифрования.

# 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. Если переходим к первому пункту по формуле
3. - искомое сообщение. Переводим его в текстовый вид.

# Листинг разработанной программы с комментариями

N = 762930465497

e = 369197

C = '''272601390768

146191862405

56417639739

25010208392

569176485965

292815488501

152909580675

634319609453

578700740159

648142948177

39319966771

517127377434

490584971826'''

answer = ""

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

    y = pow(int(num), e, N)

    res = 0

    while y != int(num):

        res = y

        y = pow(y, e, N)

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

    answer += part

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 повторного шифрования.