Министерство образования и науки РФ

Федеральное государственное автономное

образовательное учреждение высшего образования

«Университет ИТМО»

**факультет программной инженерии и компьютерной техники**

**ЛАБОРАТОРНАЯ РАБОТА № 2.4**

по дисциплине

‘Информационная безопасность’

‘Атака на алгоритм шифрования RSA, основанная на Китайской теореме об отстатках’

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, основанной на Китайской теореме об остатках.

# 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, Параллельный, Шрифт

Автоматически созданное описание

# Ход работы

1. Последовательно вычисляем значения:
2. Вычисляем
3. Переводим дешифрацию шифрблока в текстовый вид
4. Переходим к пункту 2, пока блок не расшифрован полностью.

# Листинг разработанной программы с комментариями

N1 = 553399203289

N2 = 555525439597

N3 = 556783358239

C1 = '''532587529932

466776013367

194393214430

551419753294

235808018295

521345765147

62408122881

238014267850

282320724474

421626850723

477001857725

59354292288'''

C2 = '''453172264962

295084884945

184687156359

110229199835

452343899082

61700963597

371846842

184524760412

349901424433

66575580602

38470059268

27434041612'''

C3 = '''283795978048

548212520352

50623875598

45628043554

374654069771

454067424044

140771995786

230698987467

416727167751

87650410693

75414175302

305387967882'''

answer = ''

c1 = C1.split("\n")

c2 = C2.split("\n")

c3 = C3.split("\n")

M0 = N1 \* N2 \* N3

m1 = N2 \* N3

m2 = N1 \* N3

m3 = N1 \* N2

n1 = pow(m1, -1, N1)

n2 = pow(m2, -1, N2)

n3 = pow(m3, -1, N3)

print(f"M0 = {M0}")

print(f"m1 = {m1}")

print(f"m2 = {m2}")

print(f"m3 = {m3}")

print(f"n1 = {n1}")

print(f"n2 = {n2}")

print(f"n3 = {n3}")

print()

for i in range(len(c1)):

    S = (int(c1[i]) \* n1 \* m1) + (int(c2[i]) \* n2 \* m2) + (int(c3[i]) \* n3 \* m3)

    M = round((S % M0) \*\* (1/3))

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

    answer += part

print(f"answer = {answer}")

# Результаты работы программы

Изображение выглядит как текст, снимок экрана, Шрифт, программное обеспечение

Автоматически созданное описание

# Выводы по работе

В ходе выполнения данной лабораторной работы я ознакомился с атакой на алгоритм шифрования RSA, основанной на Китайской теореме об отстатках.