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.

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

19	553399203289	555525439597	556783358239	532587529932	453172264962	283795978048
				466776013367	295084884945	548212520352
				194393214430	184687156359	50623875598
				551419753294	110229199835	45628043554
				235808018295	452343899082	374654069771

43

				521345765147	61700963597	454067424044
				62408122881	371846842	140771995786
				238014267850	184524760412	230698987467
				282320724474	349901424433	416727167751
				421626850723	66575580602	87650410693
				477001857725	38470059268	75414175302
				59354292288	27434041612	305387967882

Ход работы

1. Последовательно вычисляем значения:

$$M_0 = N_1 * N_2 * N_3$$
$$= 17117042437424027087942652438486738 7$$
$$m_1 = N_2 * N_3 = 309307319846014406789683$$
$$m_2 = N_1 * N_3 = 308123466854036474048071$$
$$m_3 = N_1 * N_2 = 307427335679751293234533$$

$$n_1 = m_1^{-1}\ mod\ N_1 = 434914147184$$
$$n_2 = m_2^{-1}\ mod\ N_2 = 692351062$$
$$n_3 = m_3^{-1}\ mod\ N_3 = 118515698858$$

2. Вычисляем

$$S = c_1 * n_1 * m_1 + c_2 * n_2 * m_2 + c_3 * n_3 * m_3$$
$$S\ mod\ M_0$$
$$M = (S\ mod\ M_0)^{\left(\frac{1}{e}\right)}$$

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

```
PS C:\only_labs_java\infobez\lab2.4> python -u "c:\only_labs_java\infobez\lab2.4\main.py"
M0 = 171170424374240270879426524384867387
m1 = 309307319846014406789683
m2 = 308123466854036474048071
m3 = 307427335679751293234533
n1 = 434914147184
n2 = 692351062
n3 = 118515698858

answer = часто переносят в      память рабочей станции
```

Выводы по работе

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