МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное автономное
образовательное учреждение высшего образования
«Университет ИТМО»

ФАКУЛЬТЕТ ПРОГРАММНОЙ ИНЖЕНЕРИИ И КОМПЬЮТЕРНОЙ ТЕХНИКИ

ЛАБОРАТОРНАЯ РАБОТА № 2.3

по дисциплине

‘Информационная безопасность’

‘Атака на алгоритм шифрования RSA методом бесключевого чтения’

Вариант №19

Выполнил:
Студент группы P34111
Павлов Александр
Сергеевич
Преподаватель:
Маркина Т.А.

Санкт-Петербург, 2024

Цель работы

Изучить атаку на алгоритм шифрования RSA посредством бесключевого чтения.

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	500984306287	470149	267797	274230487503	176943898057
				6821302647	272954693703
				172152295595	141643708385
				454539302130	238296127866
				462305524774	270971764501
				73589652382	389314459147
				274794725040	476866404163
				295185494003	295344931481
				159348742119	288885538254
				62021560582	144738759088
				311827395163	52793710114
				159638616315	416204845784

Ход работы

1. Решаем уравнение $e_1 r - e_2 s = \pm 1$ с помощью расширенного алгоритма Евклида. Получаем $C = s = -145100$ и $D = r = 82649$
2. Производим дешифрацию: $(c_1 r * c_2 s)\ mod\ N$
3. Переводим дешифрацию шифрблока в текстовый вид
4. Переходим к пункту 2, пока блок не расшифрован полностью.

Листинг разработанной программы с комментариями

```
N = 500984306287

e1 = 470149

e2 = 267797

C1 = '''274230487503

6821302647

172152295595

454539302130

462305524774
```

```
73589652382
274794725040
295185494003
159348742119
62021560582
311827395163
159638616315'''
C2 = '''176943898057
272954693703
141643708385
238296127866
270971764501
389314459147
476866404163
295344931481
288885538254
144738759088
52793710114
416204845784'''

answer = ""

def extended_gcd(a, b):
    if a == 0:
        return b, 0, 1
    else:
        gcd, x1, y1 = extended_gcd(b % a, a)
        x = y1 - (b // a) * x1
        y = x1
    return gcd, x, y

c1 = C1.split("\n")
```

```
c2 = C2.split("\n")


a, s, r = extended_gcd(e2, e1)

print(f"s = {s}, r = {r}")


for i in range(len(c1)):
    m = (pow(int(c1[i]), r, N) * pow(int(c2[i]), s, N)) % N
    part = m.to_bytes(4, byteorder='big').decode('cp1251')
    answer += part


print(f"answer = {answer}")
```

Результаты работы программы

```
PS C:\only_labs_java\infobez\lab2.3> python -u "c:\only_labs_java\infobez\lab2.3\main.py"
s = -145100, r = 82649
answer = также может указать серверу максимальный размер
```

Выводы по работе

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