УНИВЕРСИТЕТ ИТМО

Факультет программной инженерии и компьютерной техники

Направление подготовки 09.03.04 Программная инженерия

**Лабораторная работа №2.3**

Дисциплина «Информационная безопасность»

Вариант 13

**Выполнил: студент группы P34131**

*Кузнецов Максим Александрович*

**Преподаватель:**

*Маркина Татьяна Анатольевна*

Санкт-Петербург, 2023 г.

Цель работы

Изучить атаку на алгоритм шифрования RSA посредством метода бесключевого чтения.

Задание

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Вариант | Модуль, N | Экспоненты | | | Блоки зашифрованного текста | |
|  | |  |  |  |
| 13 | 518587807081 | 293177 | 1209781 | | 373852443734 447989059513 140756140384 207791711792 252160015422 151272799305 431450717984 252882800366 112417596471 301753741810 480461056512 334158277030 368394150653 | 22286870422 343015689591 281801228231 360270382562 264253306719 128520421967 399665129411 448878989738 70913527757 295285211952 247990966487 202711954425 201121363025 |

Ход работы

1. Решаем уравнение
2. Построчно производим дешифрацию: возводим в степень , а в степень по модулю 𝑁.
3. Перемножаем полученные числа и берем модуль по 𝑁.
4. Преобразуем результат в текст.
5. Повторяем шаги 2–4 для каждой строки и получаем итоговый текст.

Для решения задачи была разработана программа на Python.

Листинг разработанной программы

import math

N = 518587807081

e1 = 293177

e2 = 1209781

C1 = '''

373852443734

447989059513

140756140384

207791711792

252160015422

151272799305

431450717984

252882800366

112417596471

301753741810

480461056512

334158277030

368394150653

'''

C2 = '''

22286870422

343015689591

281801228231

360270382562

264253306719

128520421967

399665129411

448878989738

70913527757

295285211952

247990966487

202711954425

201121363025

'''

def gcd\_extended(num1, num2):

if num1 == 0:

return num2, 0, 1

else:

div, x, y = gcd\_extended(num2 % num1, num1)

return div, y - (num2 // num1) \* x, x

c\_1 = list(map(int, C1.split()))

c\_2 = list(map(int, C2.split()))

a, r, s = gcd\_extended(e1, e2)

print(f"1. Шаг первый: r = {r}, s = {s}")

output = ""

for i in range(len(c\_1)):

c\_1\_pow\_r = pow(c\_1[i], r, N)

c\_2\_pow\_s = pow(c\_2[i], s, N)

print(f"2. Шаг второй: c\_1\_pow\_r = {c\_1\_pow\_r}, c\_2\_pow\_s = {c\_2\_pow\_s}")

res = (c\_1\_pow\_r \* c\_2\_pow\_s) % N

print(f"3. Шаг третий: (c\_1\_pow \* c\_2\_pow\_s) mod N = {res}")

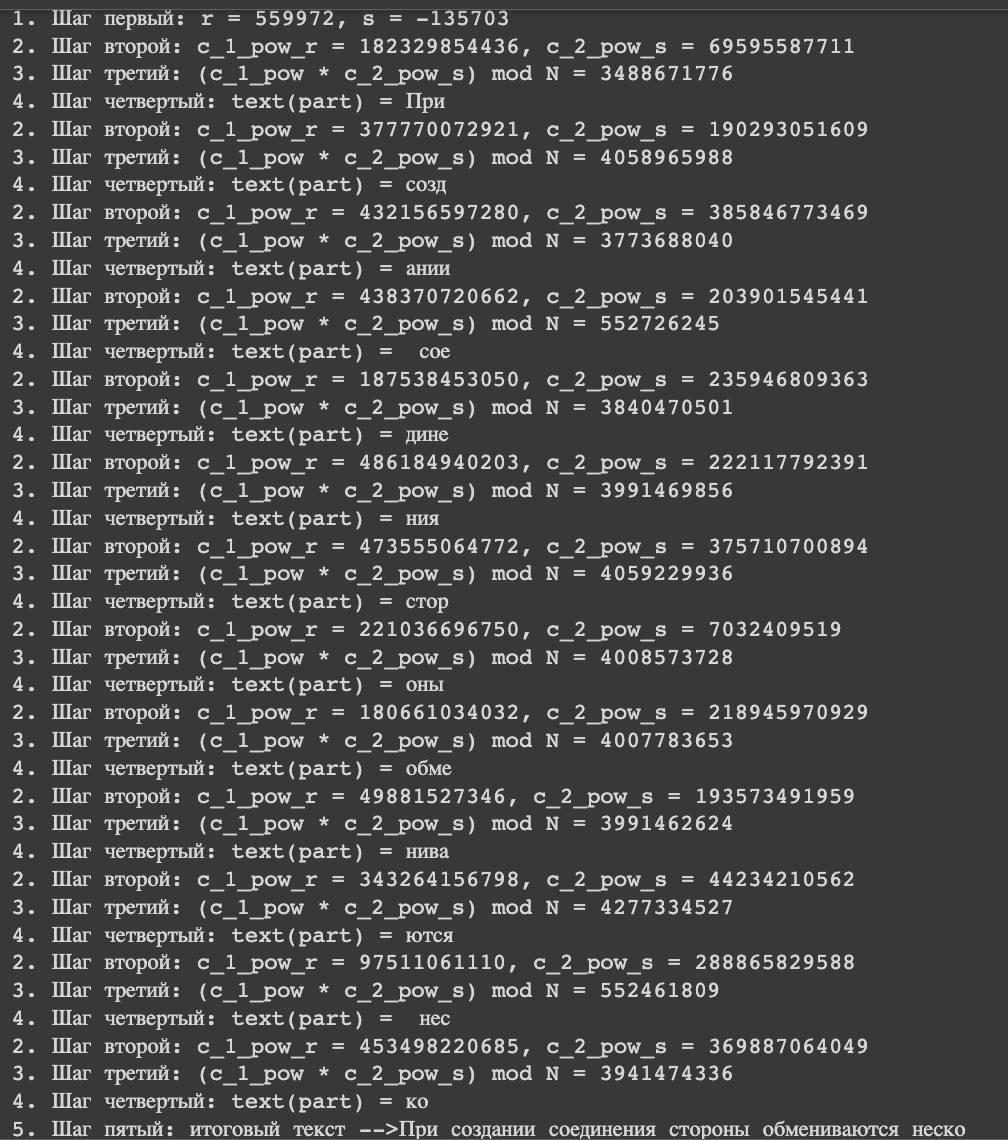
msg = res.to\_bytes(4, byteorder='big').decode('cp1251')

print(f"4. Шаг четвертый: text(part) = {msg}")

output += msg

print(f"5. Шаг пятый: итоговый текст -->{output}")

Результат работы программы:



Итоговый текст: При создании соединения стороны обмениваются неско

Вывод

В ходе выполнения данной лабораторной работы я:

* ознакомился с методом бесключевого чтения для атаки на алгоритм шифрования RSA
* Реализовал данный метод на языке Python.