УНИВЕРСИТЕТ ИТМО

Факультет программной инженерии и компьютерной техники

Направление подготовки 09.03.04 Программная инженерия

**Лабораторная работа №2.1**

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 Ферма.

Задание

|  |  |  |  |
| --- | --- | --- | --- |
| Вариант | Модуль, N | Экспонента, е | Блок зашифрованного текста, C |
| 13 | 72903890242273 | 3261683 | 37429454018574 65632293727338 71955235122455 71474662312159 18537435780920 58372142077460 68330829196451 60882917270796 24142764117328 31238010810556 66143215653810 30769266886306 |

Ход работы

1. Вычисляем .
2. Вычисляем и далее .
3. Проверяем, является ли *d* квадратом целого числа. Повторяем шаги 2-3, пока не получится квадрат целого числа.
4. Вычисляем .
5. Вычисляем .
6. Вычисляем .
7. Вычисляем *d*, как обратный к *e*: .
8. Построчно выполняем дешифрацию текста. На каждую строку блока C вычисляем .
9. Переводим *М* в текстовый вид.

Для решения задачи была разработана программа на Python.

Листинг разработанной программы

import math

N = 72903890242273

e = 3261683

C = '''

37429454018574

65632293727338

71955235122455

71474662312159

18537435780920

58372142077460

68330829196451

60882917270796

24142764117328

31238010810556

66143215653810

30769266886306

'''

n = int(math.sqrt(N) // 1 + 1)

print(f"1. Шаг первый: n = [sqrt(N)] + 1 = {n}")

step = 0

while True:

step += 1

t = n + step

d = t \*\* 2 - N

sqrt = math.sqrt(d)

print(f"2. Шаг второй, попытка ({step}): t = {t}, d = {d}, sqrt = {sqrt}")

if sqrt % 1 == 0:

sqrt = int(sqrt)

print("3. Шаг третий: получен квадрат целого числа.")

break

else:

print("3. Шаг третий: повторение шага 2.")

pass

p = t + sqrt

q = t - sqrt

phi = round((p - 1) \* (q - 1))

d = pow(e, -1, phi)

print(f"4. Шаг четвертый: p = {p}")

print(f"5. Шаг пятый: q = {q}")

print(f"6. Шаг шестой: phi = {phi}")

print(f"7. Шаг седьмой: d = {d}")

output = ""

for i, c in enumerate(C.split()):

m = pow(int(c), d, N)

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

print(f'8. Шаг восьмой: {m} = {msg}')

output += msg

print(f"9. Шаг девятый: итоговый текст --> {output}")

Результат работы программы:

Изображение выглядит как текст, снимок экрана, черно-белый, дизайн

Автоматически созданное описание

Итоговый текст: сылки на транспортном уровне - проявляется на \_\_

Ссылка на программу: [ссылка](https://colab.research.google.com/drive/1jRvN9u6LY3CAbumiujrt9i_mKNCux9Db?usp=sharing)

Вывод

В ходе выполнения данной лабораторной работы я:

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