МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО».

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ

АТАКА НА АЛГОРИТМ ШИФРОВАНИЯ RSA ПОСРЕДСТВОМ МЕТОДА ФЕРМА

ВАРИАНТ 8

|  |  |  |
| --- | --- | --- |
| выполнил  преподаватель |  | Студент 4 курса  факультета Программной инженерии и компьютерной техники  Группы P34121  Карапетян Эрик Акопович  Старший преподаватель (квалификационная категория "старший преподаватель"), факультета программной инженерии и компьютерной техники  Маркина Татьяна Анатольевна |

Санкт-Петербург

2023 г.

Название и цель работы

Название: Атака на алгоритм шифрования RSA посредством метода Ферма

Цель работы: изучить атаку на алгоритм шифрования RSA посредством метода Ферма.

Вариант задания

Вариант: 8

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Листинг разработанной программы с комментариями

import math

def ferma(N, e, C):

message = ""

# выбираем S

s = int(math.sqrt(N) // 1)

# ищем целый корень T

i = 0

while True:

i += 1

t = s + i

print("t(" + str(i) + ")=" + str(t))

w = t \*\* 2 - N

print("w(" + str(i) + ")=" + str(w))

w\_sqrt = math.sqrt(w)

print("w\_sqrt(" + str(i) + ")=" + str(w\_sqrt))

if math.sqrt(w) % 1 == 0:

break

p = t + w\_sqrt

print("p=" + str(p))

q = t - w\_sqrt

print("q=" + str(q))

phi\_N = int((p - 1) \* (q - 1))

print("phi(N)=" + str(phi\_N))

d = pow(e, -1, phi\_N)

print("d=" + str(d))

# дешефруем rsa полученной секретной комбинацией

for w in C.split():

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

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

message += sub\_str

print(f"message = {message}")

N = 81177745546021

e = 2711039

C = '''

61553353723258

11339642237403

55951185642146

38561524032018

34517298669793

33641624424571

78428225355946

50176820404544

68017840453091

5507834749606

26675763943141

47457759065088

'''

ferma(N, e, C)

Результаты работы программы (с найденным решением)

t(1)=9009870

w(1)=11870879

w\_sqrt(1)=3445.4141986124105

t(2)=9009871

w(2)=29890620

w\_sqrt(2)=5467.23147488745

t(3)=9009872

w(3)=47910363

w\_sqrt(3)=6921.731214082211

t(4)=9009873

w(4)=65930108

w\_sqrt(4)=8119.735709984654

t(5)=9009874

w(5)=83949855

w\_sqrt(5)=9162.415347494349

t(6)=9009875

w(6)=101969604

w\_sqrt(6)=10098.0

p=9019973.0

q=8999777.0

phi(N)=81177727526272

d=43367626334719

message = несколько раз в среде с параллельными мостами. \_**Вывод**

В этой лабораторной работе познакомился с принципом работы алгоритма RSA, а так же возможностями его взлома по методу Ферма при неудачно подобранных параметрах.