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 11

|  |  |  |
| --- | --- | --- |
| выполнил  преподаватель |  | Студент 4 курса  факультета Программной инженерии и компьютерной техники  Группы P34121  Кустарев Иван Павлович  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: 11

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Листинг разработанной программы с комментариями

import math

N = 7533841359567

e = 3063167

C = '''

20373576587572

48282448633797

2859826820449

30302044163645

30736783387104

5008734894376

23296448238734

41172678840173

58656690066465

44574048719827

21962937148701

38826220113907

'''

# выбираем стартовое значение A

if math.sqrt(N) % 1 != 0:

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

else:

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

# итерируемся по возможным значениям в поисках целого корня B

i = 0

while True:

t = a + i

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

b = t \*\* 2 - N

print("s" + str(i) + "=" + str(b))

b\_sqrt = math.sqrt(b)

print("s\_sqrt" + str(i) + "=" + str(b\_sqrt))

i += 1

if b\_sqrt % 1 == 0:

break

if i == 100:

raise Exception("Не найден целый корень")

# получили p и q на основе A и B

p = t + b\_sqrt

q = t - b\_sqrt

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

d = pow(e, -1, phi)

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

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

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

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

# дешефруем rsa полученной секретной комбинацией

res = ""

for b in C.split():

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

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

sub\_str = sub\_str\_bytes.decode('cp1251')

res += sub\_str

print(f"message = {res}")

Результаты работы программы (с найденным решением)

t0=8642984

s0=7156337

s\_sqrt0=2675.1330808017756

t1=8642985

s1=24442306

s\_sqrt1=4943.916059157963

t2=8642986

s2=41728277

s\_sqrt2=6459.742796737344

t3=8642987

s3=59014250

s\_sqrt3=7682.073287856606

t4=8642988

s4=76300225

s\_sqrt4=8735.0

p=8651723.0

q=8634253.0

phi(N)=74701147981944

d=23647864249265

message = неправильной пересылки пакетов - повторные пере-

**Вывод**

Во время выполнения данной лабораторной работой изучил основной принцип работы алгоритма RSA. Узнал о возможности его взлома при неудачном подборе параметров. Научился производить взлом алгоритма RSA посредствам метода Ферма.