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

Факультет программной инженерии и компьютерной техники

Дисциплина «Информационная безопасность»

**Лабораторная работа №2.1**

**«Атака на алгоритм шифрования RSA посредством метода Ферма»**

Вариант: 4

**Учебно-методическое пособие:** Криптографические системы с секретным и открытым

ключом: учебное пособие. / А.А. Ожиганов; УНИВЕРСИТЕТ ИТМО. — Санкт-Петербург, 2015

**Автор**: Калинин Даниил Дмитриевич

**Группа**: P34141

**Преподаватель**: Маркина Татьяна Анатольевна

г. Санкт-Петербург

2024

# Содержание

[**Содержание 2**](#_1j29sb1plksc)

[**Цель работы 2**](#_ic6vz9o4aev6)

[**Порядок выполнения работы 2**](#_7c966s7zbuo)

[**Вариант 2**](#_tk58wqserqjy)

[**Выполнение работы 3**](#_i73wvolbwe0b)

[Код 3](#_opx7en3yhfv9)

[Результаты работы программы 6](#_h1i0yqxqtni2)

[**Вывод 7**](#_uft2d2ek0ay3)

# Цель работы

Изучить атаку на алгоритм шифрования RSA посредством метода Ферма.

# Порядок выполнения работы

* Ознакомьтесь с теорией, изложенной в [3]. («Взлом алгоритма RSA при неудачном выборе параметров криптосистемы»);
* Получите вариант задания у преподавателя;
* Используя разложение модуля на простые числа методом Ферма и полученные исходные данные, определите следующие показатели:
  + множители модуля (*p* и *q*);
  + значение функции Эйлера для данного модуля *φ(N)*;
  + обратное значение экспоненты по модулю *φ(N)*;
* Дешифруйте зашифрованный текст, исходный текст должен быть фразой на русском языке;
* Результаты и промежуточные вычисления оформите в виде отчета.

# Вариант

| **Вариант** | **Модуль, *N*** | **Экспонента, *е*** | **Блок зашифрованного текста, *C*** |
| --- | --- | --- | --- |
| 4 | 89318473363897 | 2227661 | 3403106899606  26746900101177  67769260919924  77873792354218  15782947730235  15100267747684  28877721728826  62898555111378  4989704651236  55293402838380  4108112294245  8492269964172 |

# 

# 

# 

# 

# 

# 

# Выполнение работы

## Код

import math

def fermats\_method(N, e):

*"""Вычисляет закрытый ключ и параметры шифрования методом Ферма"""*

print("-- Метод Ферма --")

n = math.trunc(math.sqrt(N)) + 1

print(f'n = [sqrt(N)] + 1')

i = 1

while True:

t = n + i

w = pow(t, 2) - N

print(f't\_{i} = n + i = {n} + {i} = {t}')

print(f'w\_{i} = t\_{i}^2 - N = {pow(t, 2)} - {N} = {w}')

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

*# w - не квадрат целого числа*

print(f'w\_{i} - не квадрат целого числа')

i += 1

else:

*# w - квардрат целого числа*

print(f'w\_{i} - квадрат целого числа')

break

p = t + int(math.sqrt(w))

q = t - int(math.sqrt(w))

euler\_function = (p - 1) \* (q - 1)

d = pow(e, -1, euler\_function)

print()

print(f'p = t + sqrt(w) = {t} + {int(math.sqrt(w))} = {p}')

print(f'q = t - sqrt(w) = {t} - {int(math.sqrt(w))} = {q}')

print(f'euler\_function = (p - 1)(q - 1) = {euler\_function}')

print(f'd = e^(-1) mod euler\_function = {d}')

return p, q, euler\_function, d

def decode\_part(N, d, part):

*"""Декодирует часть сообщения в текст"""*

int\_decoded\_part = pow(part, d, N)

return int\_decoded\_part.to\_bytes(4, byteorder='big').decode('cp1251')

def decode(N, d, C):

*"""Декодирует полученное сообщение в текст"""*

print("-- Дешифрование сообщения --")

*# Раздаляем закодированное сообщение на части и подготавливаем их*

raw\_parts = C.split("\n")

parts = []

for i in range(len(raw\_parts)):

if raw\_parts[i].strip() != "":

parts.append(int(raw\_parts[i].strip()))

*# Декодируем каждую часть*

original\_message = ""

for part in parts:

decoded\_part = decode\_part(N, d, part)

original\_message += decoded\_part

print(f'Декодирована часть {part} -----> {decoded\_part}')

return original\_message

if \_\_name\_\_ == '\_\_main\_\_':

*# Описание варианта*

N = 89318473363897

e = 2227661

C = """

3403106899606

26746900101177

67769260919924

77873792354218

15782947730235

15100267747684

28877721728826

62898555111378

4989704651236

55293402838380

4108112294245

8492269964172

"""

print("-- Исходные данные --")

print(f'N = {N}')

print(f'e = {e}')

print(f'C = \"{C}\"')

print("\n")

*# Вычисляем закрытый ключ и требуемые параметры*

p, q, euler\_function, d = fermats\_method(N, e)

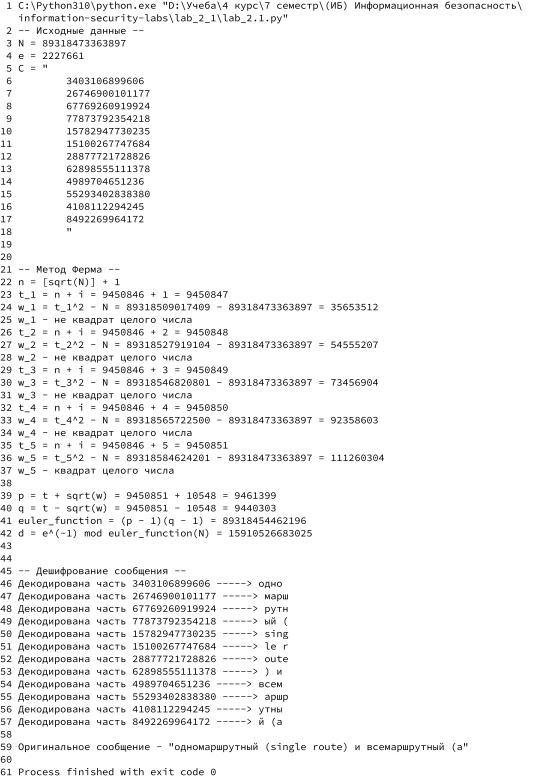
print("\n")

*# Декодируем сообщение*

original\_message = decode(N, d, C)

print(f'\nОригинальное сообщение - \"{original\_message}\"')

## Результаты работы программы



# Вывод

В ходе лабораторной работы была совершена атака на алгоритм шифрования RSA посредством метода Ферма, в следствии чего было декодировано исходное сообщение. В процессе выполнения был изучен алгоритм шифрования RSA, а также вариант атаки на данный алгоритм шифрования с использованием метода Ферма.