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

Факультет программной инженерии и компьютерной техники

Дисциплина «Информационная безопасность»

**Лабораторная работа №2.3**

**«Атака на алгоритм шифрования RSA методом бесключевого чтения»**

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 3**](#_tk58wqserqjy)

[**Выполнение работы 4**](#_i73wvolbwe0b)

[Код 4](#_opx7en3yhfv9)

[Результаты работы программы 6](#_h1i0yqxqtni2)

[**Вывод 7**](#_uft2d2ek0ay3)

# Цель работы

Изучить атаку на алгоритм шифрования RSA посредством метода бесключевого чтения.

# Порядок выполнения работы

* Ознакомьтесь с теорией в [3], в подразделе («Бесключевое чтение»);
* Получите вариант задания у преподавателя;
* По полученным данным определите значения r и s при условии, чтобы . Для этого необходимо использовать расширенный алгоритм Евклида;
* Используя полученные выше значения r и s, запишите исходный текст;
* Результаты и промежуточные вычисления значений для любых трех блоков шифрованного текста оформите в виде отчета.

# 

# 

# Вариант

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Вариант** | **Модуль, *N*** | **Экспоненты** | | **Блок зашифрованного текста** | |
| ***e1*** | ***e2*** | **C1** | **C2** |
| 4 | 535598392051 | 455341 | 396971 | 444982997352  277831853272  133187882628  331361392426  273206302188  470299046774  168157171491  258737286129  312335302650  489235057221  427689116872  418723605534  135022585485 | 358696089912  360292494113  91390259562  534590606880  193203217609  166702058071  68207231399  487524624411  325841328769  533726724224  369967614519  247201359991  478832067683 |

# 

# 

# 

# 

# 

# 

# Выполнение работы

## Код

def extended\_euclidean\_algorithm(e1, e2):

if e2 == 0:

print(f'Расш. алг. Евклида (e1 = {e1}, e2 = {e2}) --> r = {1}, s = {0}')

return 1, 0

else:

print(f'Расш. алг. Евклида (e1 = {e1}, e2 = {e2})')

r, s = extended\_euclidean\_algorithm(e2, e1 % e2)

print(f'Расш. алг. Евклида (e1 = {e1}, e2 = {e2}) --> r = {s}, s = {r - s \* (e1 // e2)}')

return s, r - s \* (e1 // e2)

def decode(N, C1, C2, r, s):

*"""Декодирует полученные сообщение в текст"""*

print("-- Дешифрование сообщения --")

*# Раздаляем закодированное сообщение на части и подготавливаем их*

raw\_parts\_C1 = C1.split("\n")

parts\_C1 = []

for i in range(len(raw\_parts\_C1)):

if raw\_parts\_C1[i].strip() != "":

parts\_C1.append(int(raw\_parts\_C1[i].strip()))

raw\_parts\_C2 = C2.split("\n")

parts\_C2 = []

for i in range(len(raw\_parts\_C2)):

if raw\_parts\_C2[i].strip() != "":

parts\_C2.append(int(raw\_parts\_C2[i].strip()))

if (len(parts\_C1) != len(parts\_C2)):

print("Дешифрование прервано - Ввод C1 и C2 с разным количеством частей")

exit(1)

*# Декодируем каждую часть*

original\_message = ""

for i in range(len(parts\_C1)):

y1 = parts\_C1[i]

y2 = parts\_C2[i]

int\_decoded\_part = pow(y1, r, N)\*pow(y2, s, N) % N

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

original\_message += decoded\_part

print(f'Декодирована часть C1 = {y1} и C2 = {y2} -----> {int\_decoded\_part} -----> {decoded\_part}')

return original\_message

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

*# Описание варианта*

N = 535598392051

e1 = 455341

e2 = 396971

C1 = """

444982997352

277831853272

133187882628

331361392426

273206302188

470299046774

168157171491

258737286129

312335302650

489235057221

427689116872

418723605534

135022585485

"""

C2 = """

358696089912

360292494113

91390259562

534590606880

193203217609

166702058071

68207231399

487524624411

325841328769

533726724224

369967614519

247201359991

478832067683

"""

print("-- Исходные данные --")

print(f'N = {N}')

print(f'e1 = {e1}')

print(f'e2 = {e2}')

print(f'C1 = \"{C1}\"')

print(f'C2 = \"{C2}\"')

print()

*# Решаем уравнение r\*e1 + s\*e2 = 1*

print("-- Расширенный алгоритм Евклида --")

r, s = extended\_euclidean\_algorithm(e1, e2)

print(f'r = {r}')

print(f's = {s}')

print(f'r\*e1 + s\*e2 = {r}\*{e1} + {s}\*{e2} = {r\*e1 + s\*e2}')

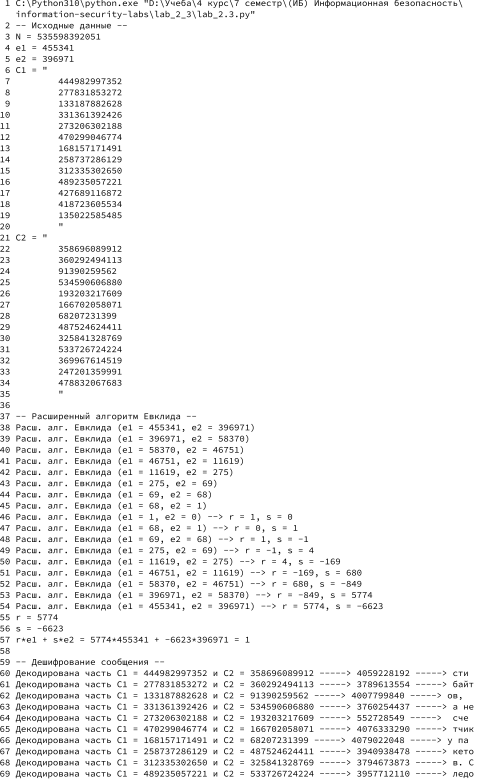
print()

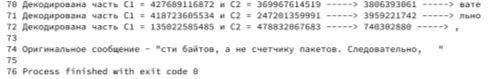
*# Декодируем сообщение*

original\_message = decode(N, C1, C2, r, s)

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

## Результаты работы программы





# Вывод

В ходе лабораторной работы была совершена атака на алгоритм шифрования RSA методом бесключевого чтения, в следствии чего было декодировано исходное сообщение. В процессе выполнения была изучена атака на алгоритм шифрования RSA посредством метода бесключевого чтения, а также был изучен расширенный алгоритм Евклида.