

федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»

Лабораторная работа №3

по дисциплине “Информационная безопасность”

**на тему “Атака на алгоритм шифрования RSA
посредством метода Ферма”**

Вариант 3

Выполнила: Студентка гр. Р3402

Калугина М. М.

Преподаватель: к.т.н, доцент

Маркина Т.А.

г. Санкт-Петербург

2021 г.

Цель

Изучение атаки на алгоритм шифрования RSA посредством метода Ферма.

Задание

Используя разложение модуля на простые числа методом Ферма и полученные исходные данные, определить следующие показатели:

- множители модуля (р и q);
- значение функции Эйлера для данного модуля $\varphi(N)$
- обратное значение экспоненты по модулю $\varphi(N)$

Расшифровать зашифрованный текст, исходный текст должен быть фразой на русском языке

Исходные данные

Вариант 3:

$N = 93767386321457$

$e = 2091619$

$C = 62984326732858 \quad 22123186696272 \quad 24425203655789 \quad 45995309006047$
 $8176196426076 \quad 12816278693250 \quad 27474201663022 \quad 86909026690842 \quad 20469575723850$
 $29205116646939 \quad 21002901408912 \quad 79168478687790$

Ход работы

Шаг 1.

На первом шаге необходимо определить множители р и q.

Для этого сначала необходимо посчитать значение $n = \sqrt{N} + 1$. С этого значения будет начинаться поиск таких р и q, произведение которых будет давать N. Чем ближе расположены р и q, тем меньше итераций потребуется для их поиска.

Алгоритм поиска р и q:

1. Присваиваем полученное значению переменной t_i .
2. Возводим t_i в квадрат
3. Рассчитываем значение $w_i = t_i^2 N$.
4. Проверяем, является ли значение w_i квадратом некоторого числа. Если число не является квадратом, увеличиваем значение n на единицу и возвращаемся к шагу 1.

5. Когда значение w_i найдено, переходим к расчету p и q : $p = t_i + \text{sqrt}(w_i)$,
 $= t_i + \text{sqrt}(w_i)$

На рисунке 1 представлен итеративный расчет значений p и q :

The interface shows the following data:

A	3908170219
B	26651504610523
C	93767386321457
D	иссл

Buttons available:

- $D = A + B$
- $D = A^B \bmod C$
- $D = \text{text}(A)$
- $D \rightarrow A$
- $D = A * B$
- $D = A^{(1/B)}$
- $D = \text{number}(A)$
- $D \rightarrow \text{table}$
- $D = A \div B$
- $A^D \cdot B^C = N$
- Increase number of rows
- $D = A \bmod C$

Table of results:

N	93767386321457
e	2091619
C	62984326732858 22123186696272 2442520365578
n	9683357
t1	9683358
t1^2	93767422156164
w1	35834707
D1	5987
t2	9683359
t2^2	93767441522881
w2	55201424
D2	7430
t3	9683360
t3^2	93767460889600
w3	74568143
D3	8636
t4	9683361
t4^2	93767480256321
w4	93934864
D4	9692
p	9693053
q	9673669
Phi (N)	93767366954736
d	26651504610523

Buttons at the bottom:

- Clear D
- Clear A, B, C
- Clear grid

Рисунок 1. Расчет значений p и q

Шаг 2

Расчет значений ϕ обратного значения экспоненты по модулю $\phi(N)$

Расчет ϕ производится по формуле: $\phi(N) = (p - 1)(q - 1)$.

Пусть d - значение обратное к e по модулю $\phi(N)$. Тогда результат d будет вычисляться по формуле: $d = e^{-1} \bmod \phi(N)$

Численные значения d и $\phi(N)$ представлены в двух последних строчках рисунка 1.

Шаг 3. Дешифрование.

Для каждого блока C_i производятся следующие вычисления:

$$M_i = C_i^d \bmod N$$

В блоках M_i хранится дешифрованная информация.
На рисунке 2 представлено итеративное декодирование зашифрованной фразы:

A	
975200095	
B	
26651504610523	
C	
93767386321457	
D	
: _	
D = A + B	
D = A^B mod C	
D = text(A)	
D --> A	
D = A * B	
D = A^(1 / B)	
D = number(A)	
D --> table	
D = A div B	
A*D - B*C = N	
Increase number of rows	
D = A mod C	

N	93767386321457
e	2091619
C	62984326732858 22123186696272 2442520365578
p	9693053
q	9673669
Phi (N)	93767366954736
d	26651504610523
m1	3908170219 => 'иссл'
m2	3856985826 => 'едов'
m3	3774014955 => 'ател'
m4	3857260785 => 'ей с'
m5	552394992 => ' мар'
m6	4176540658 => 'шрут'
m7	3907510518 => 'изац'
m8	3907381536 => 'ией '
m9	4008845544 => 'от и'
m10	4059229943 => 'сточ'
m11	3991464672 => 'ника'
m12	975200095 => ': _'

Рисунок 2. Дешифрование.

Результат

Итоговая фраза звучит так “исследователей с маршрутизацией от источника: _”

Вывод

В ходе выполнения лабораторной работы был изучен метод шифрования RSA, были получены навыки дешифрования алгоритма шифрования RSA посредством метода Ферма и была проведена дешифрация фразы путем решения уравнения $t^2 - w^2 = n$ для определения значений p и q , после чего дешифрование сводится к последовательному расчету пары значений: $\phi(N)$ и d и дальнейшему дешифрованию закодированных блоков.