

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

**Факультет программной инженерии и компьютерной техники**

**ЛАБОРАТОРНАЯ РАБОТА № 2.1**

**ПО ДИСЦИПЛИНЕ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

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

Выполнил: Давыдов Иван Денисович

Группа: Р3400

Вариант 5

Санкт-Петербург

2020/2021

## Цель работы

Изучить атаку на алгоритм шифрования RSA посредством метода Ферма.

## Задание

Вариант	Модуль, N	Экспонента, e	Блок зашифрованного текста, C
5	87046121832829	2342047	38288567928461 32933111631628 3796990272007 14526017018271 6637183116942 46455894660145 17024410119252 49991104309343 20967672129390 3377231740209 37201047739579 56818318686813

## Выполнение

Для выполнения лабораторной работы использовалась программа BCalc.exe.


Найдем  $n = [\text{sqrt}(N)]$ :

The screenshot shows the BCalc application window. On the left, there are four input fields labeled A, B, C, and D. Field A contains the value 87046121832829. Field B contains the value 2. Field C is empty. Field D contains the value 9329852. On the right, there is a table with two columns. The first column contains the labels 'N' and 'n'. The second column contains the values '[error]' and '9329852' respectively.

N	[error]
n	9329852

N не является квадратом целого числа, т.к. вверху таблицы высветилось сообщение об ошибке.


Проверим  $w = (n + k)^2 - N$ ,  $k = 1$ :

 BCalc

A	35168780		[error]
B	2	N	87046121832829
C	0	n	9329852
D	5931	t1	9329853
		t1^2	87046157001609
		w1	35168780

w не является квадратом целого числа

Проверим  $w = (n + k)^2 - N$ ,  $k = 2$ :

 BCalc

A	53828487		[error]
B	2	N	87046121832829
C	0	n	9329852
D	7337	t1	9329853
		t1^2	87046157001609
		w1	35168780
		t2	9329854
		t2^2	87046175661316
		w2	53828487

w не является квадратом целого числа

Проверим  $w = (n + k)^2 - N$ ,  $k = 3$ :

**BCalc**

A	72488196
B	2
C	0
D	8514

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	87046121832829
n	9329852
t1	9329853
t1^2	87046157001609
w1	35168780
t2	9329854
t2^2	87046175661316
w2	53828487
t3	9329855
t3^2	87046194321025
w3	72488196

$w$  является квадратом целого числа

Вычислим  $p = t3 - \sqrt{w}$  и  $q = t3 + \sqrt{w}$ :

**BCalc**

A	9329855
B	-8514
C	0
D	9321341

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	87046121832829
n	9329852
t1	9329853
t1^2	87046157001609
w1	35168780
t2	9329854
t2^2	87046175661316
w2	53828487
t3	9329855
t3^2	87046194321025
w3	72488196
w3^1/2	8514
p	9338369
q	9321341


Найдем  $\Phi(n)$  и параметр  $d$ :

 BCalc

A	
2342047	
B	
-1	
C	
87046103173120	
D	
72185156245343	
<div> <div>D = A + B</div> <div>D = A^B mod C</div> <div>D = text( A )</div> <div>D --&gt; A</div> </div>	
<div> <div>D = A * B</div> <div>D = A^(1 / B)</div> <div>D = number( A )</div> <div>D --&gt; table</div> </div>	
<div> <div>D = A div B</div> <div>A*D - B*C = N</div> <div>Increase number of rows</div> </div>	
<div> <div>D = A mod C</div> </div>	

N	87046121832829
n	9329852
t1	9329853
t1^2	87046157001609
w1	35168780
t2	9329854
t2^2	87046175661316
w2	53828487
t3	9329855
t3^2	87046194321025
w3	72488196
w3^1/2	8514
p	9338369
q	9321341
Phi	87046103173120
d	72185156245343

Далее, расшифруем сообщение:

 BCalc

A
1919907188
B
72185156245343
C
87046121832829
D
rou

Криптограмма	Сообщение	Текст
38288567928461	1919907188	rout
32933111631628	1702045998	es).
3796990272007	550429933	Одн
14526017018271	3995987168	о-ма
6637183116942	4042846451	ршру
46455894660145	4075682793	тный
17024410119252	552591594	пак
49991104309343	3857850607	ет п
20967672129390	4009747179	оявл
3377231740209	4293260017	яетс
37201047739579	4280349422	я то
56818318686813	3959220974	лько

Итоговое сообщение: «(routes). Одно-маршрутный пакет появляется только»

## Вывод

В ходе выполнения данной лабораторной работы была успешно произведена атака на алгоритм RSA методом Ферма.