

Национальный исследовательский университет ИТМО  
Факультет Программной Инженерии и Компьютерной Техники

Вариант №6  
Лабораторная работа №2.1  
«Атака на алгоритм шифрования RSA посредством  
метода Ферма»  
По дисциплине:  
«Информационная безопасность»

Работу выполнила:  
Студентка группы Р34102  
Никонова Наталья Игоревна  
Преподаватель:  
Рыбаков Степан Дмитриевич

Санкт-Петербург

2023

## Цель работы

Изучить атаку на алгоритм шифрования RSA посредством метода Ферма.

## Задание

- 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  $\Phi(N)$ ;
  - обратное значение экспоненты по модулю  $\Phi(N)$ ;
- дешифруйте зашифрованный текст, исходный текст должен быть фразой на русском языке

Вариант	Модуль, $N$	Экспонента, $e$	Блок зашифрованного текста, $C$
6	85609460573249	2448539	523815866990 26788001211021 34569932939126 85581094055910 23256663175806 62527703621248 7622521689363 32655715523491 81242663069415
			60438288306445 73937478628138 7793112362388

## Порядок выполнения

1. Вычисляем  $n = [\sqrt{N}] + 1$ . Получили [error] –  $N$  не является квадратом целого числа,  $n = 9252539$

A	
85609460573249	[error]
B	
2	
C	
1	
D	
9252539	

2.  $t1 = n + 1 = 9252540$ ,  $t1^2 = 85609496451600$

A	9252540
B	2
C	0
D	85609496451600

$$w1 = t1^2 - N = 35878351$$

A	85609496451600
B	-85609460573249
C	0
D	35878351

Проверка что  $w1$  – квадрат целого числа

BCalc	
A	35878351
B	2
C	0
D	5990
	[error]

Нет – берем  $t2 = 9252541$ ,  $t2^2 = 85609514956681$

A	9252541
B	2
C	0
D	85609514956681

$$w2 = t2^2 - N = 54383432$$

A	85609514956681
B	-85609460573249
C	0
D	54383432

Проверка, что  $w_2$  – квадрат целого числа

BCalc

A		
54383432		[error]
B		
2		
C		
0		
D		
7375		

Нет – берем  $t_3=9252542$ ,  $t_3^2=85609533461764$

A	
9252542	
B	
2	
C	
0	
D	
85609533461764	

$w_3=t_3^2-N=72888515$

A	
85609533461764	
B	
-85609460573249	
C	
0	
D	
72888515	

Проверка что  $w_3$  – квадрат целого числа

A		
72888515		[error]
B		
2		
C		
0		
D		
8538		

Нет. Берем  $t_4=t_3+1=9252543$ ,  $t_4^2=85609551966849$

A	
9252543	
B	
2	
C	
0	
D	
85609551966849	

$$w4 = t4^2 - N = 91393600$$

A
85609551966849
B
-85609460573249
C
0
D
91393600

Проверка что  $w4$  – квадрат целого числа

A		
91393600		
B		
2		
C		
0		
D		
9560		

Да. Заканчиваем шаг.

3.  $t4 = 9252543$ ,  $\text{sqrt}(w4) = 9560$
4.  $p = t4 + \text{sqrt}(w4) = 9262103$

A
9252543
B
9560
C
0
D
9262103
D = A + B

$$q = t4 - \text{sqrt}(w4) = 9242983$$

A
9252543
B
-9560
C
0
D
9242983
D = A + B

$$\text{Phi}(N) = (p-1)(q-1) = 85609442068164$$

A
9262102
B
9242982
C
0
D
85609442068164
D = A + B
D = A * B

$$d=e^{-1} \bmod \Phi(N)=62467989361523$$

A
2448539
B
-1
C
85609442068164
D
62467989361523

## 5. Дешифрация

A	
523815866990	
B	
62467989361523	
C	
85609460573249	
D	
4007979245	
<input type="button" value="D = A + B"/>	<input type="button" value="D = A^B mod C"/>

A
4007979245
B
62467989361523
C
85609460573249
D
один

A	
26788001211021	
B	
62467989361523	
C	
85609460573249	
D	
552657127	
<input type="button" value="D = A + B"/>	<input type="button" value="D = A^B mod C"/>

A		
552657127		
B		
62467989361523		
C		
85609460573249		
D		
раз		
<input type="button" value="D = A + B"/>	<input type="button" value="D = A^B mod C"/>	<input type="button" value="D = text( A )"/>

A	
34569932939126	
B	
62467989361523	
C	
85609460573249	
D	
551690474	
<input type="button" value="D = A + B"/>	<input type="button" value="D = A^B mod C"/>

A		
551690474		
B		
62467989361523		
C		
85609460573249		
D		
в к		
<input type="button" value="D = A + B"/>	<input type="button" value="D = A^B mod C"/>	<input type="button" value="D = text( A )"/>

A	
85581094055910	
B	
62467989361523	
C	
85609460573249	
D	
3773228270	
<input type="button" value="D = A + B"/>	<input type="button" value="D = A^B mod C"/>

A		
3773228270		
B		
62467989361523		
C		
85609460573249		
D		
аждо		
<input type="button" value="D = A + B"/>	<input type="button" value="D = A^B mod C"/>	<input type="button" value="D = text( A )"/>

A	A
23256663175806	3961580270
B	B
62467989361523	62467989361523
C	C
85609460573249	85609460573249
D	D
3961580270	м ко
<input type="button" value="D = A + B"/>	<input type="button" value="D = A^B mod C"/>
<input type="button" value="D = A + B"/>	<input type="button" value="D = A^B mod C"/>
<input type="button" value="D = text( A )"/>	

A	A
62527703621248	3959224037
B	B
62467989361523	62467989361523
C	C
85609460573249	85609460573249
D	D
3959224037	льце
<input type="button" value="D = A + B"/>	<input type="button" value="D = A^B mod C"/>
<input type="button" value="D = A + B"/>	<input type="button" value="D = A^B mod C"/>
<input type="button" value="D = text( A )"/>	

A	A
7622521689363	740354798
B	B
62467989361523	62467989361523
C	C
85609460573249	85609460573249
D	D
740354798	, ко
<input type="button" value="D = A + B"/>	<input type="button" value="D = A^B mod C"/>
<input type="button" value="D = A + B"/>	<input type="button" value="D = A^B mod C"/>
<input type="button" value="D = text( A )"/>	

A	A
32655715523491	3823427616
B	B
62467989361523	62467989361523
C	C
85609460573249	85609460573249
D	D
3823427616	гда
<input type="button" value="D = A + B"/>	<input type="button" value="D = A^B mod C"/>
<input type="button" value="D = A + B"/>	<input type="button" value="D = A^B mod C"/>
<input type="button" value="D = text( A )"/>	

A	A
81242663069415	3941526524
B	B
62467989361523	62467989361523
C	C
85609460573249	85609460573249
D	D
3941526524	коль
<input type="button" value="D = A + B"/>	<input type="button" value="D = A^B mod C"/>
<input type="button" value="D = A + B"/>	<input type="button" value="D = A^B mod C"/>
<input type="button" value="D = text( A )"/>	

A	A
60438288306445	4141883633
B	B
62467989361523	62467989361523
C	C
85609460573249	85609460573249
D	D
4141883633	ца с
<input type="button" value="D = A + B"/>	<input checked="" type="button" value="D = A^B mod C"/>
<input type="button" value="D = A + B"/>	<input type="button" value="D = A^B mod C"/>
<input type="button" value="D = A + B"/>	<input type="button" value="D = text( A )"/>

  

A	A
73937478628138	3808421856
B	B
62467989361523	62467989361523
C	C
85609460573249	85609460573249
D	D
3808421856	вяза
<input type="button" value="D = A + B"/>	<input checked="" type="button" value="D = A^B mod C"/>
<input type="button" value="D = A + B"/>	<input type="button" value="D = A^B mod C"/>
<input type="button" value="D = A + B"/>	<input type="button" value="D = text( A )"/>

  

A	A
7793112362388	3992658015
B	B
62467989361523	62467989361523
C	C
85609460573249	85609460573249
D	D
3992658015	ны _
<input type="button" value="D = A + B"/>	<input checked="" type="button" value="D = A^B mod C"/>
<input type="button" value="D = A + B"/>	<input type="button" value="D = A^B mod C"/>
<input type="button" value="D = A + B"/>	<input type="button" value="D = text( A )"/>

дешифрованный текст = «один раз в каждом кольце, когда кольца связаны \_»

## Выводы

В ходе выполнения лабораторной работы я познакомилась с методом Ферма для атаки на алгоритм шифрования RSA и выполнила его руками.