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 P34102

Никонова Наталья Игоревна

Преподаватель:

Рыбаков Степан Дмитриевич

Санкт-Петербург

2023

Цель работы

Изучить атаку на алгоритм шифрования RSA посредством метода Ферма.

Задание

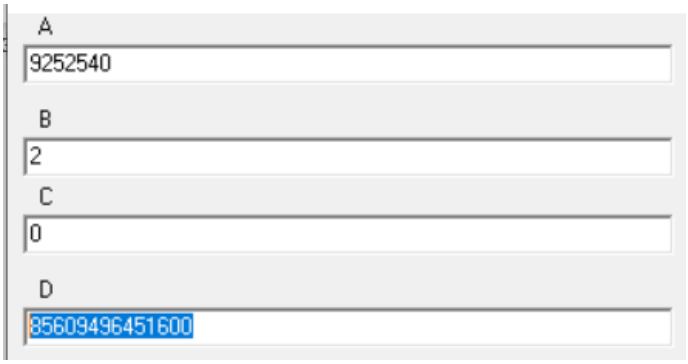
- используя разложение модуля на простые числа методом Ферма и полученные исходные данные, определите следующие показатели:
  - множители модуля (p и q);
  - значение функции Эйлера для данного модуля Phi(N);
  - обратное значение экспоненты по модулю Phi(N);
- дешифруйте зашифрованный текст, исходный 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

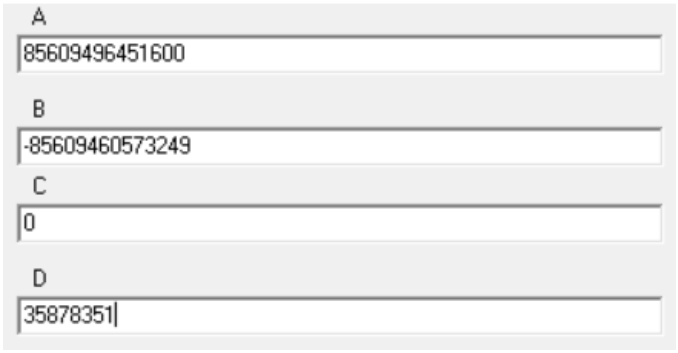
Порядок выполнения

1. Вычисляем n=[sqrt(N)]+1. Получили [error] – N не является квадратом целого числа, n=9252539

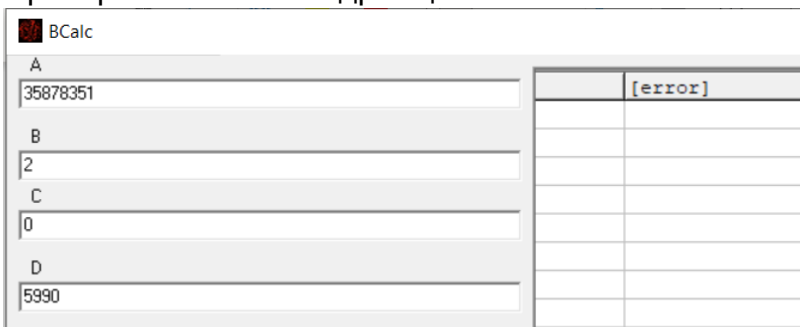
2. t1=n+1=9252540, t1^2=85609496451600



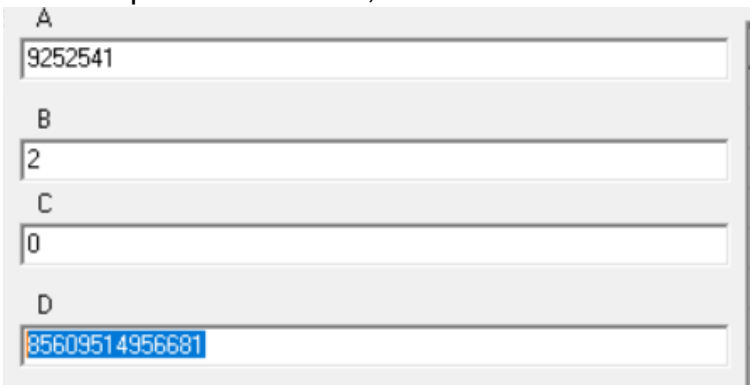
w1=t1^2-N=35878351



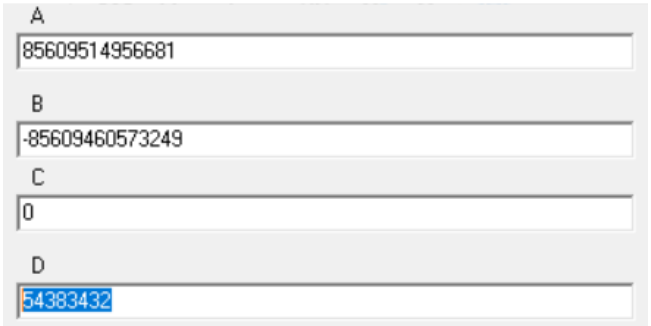
Проверка что w1 – квадрат целого числа



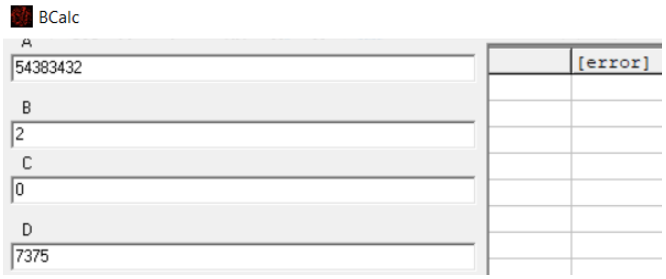
Нет – берем t2=9252541, t2^2=85609514956681



w2=t2^2-N=54383432

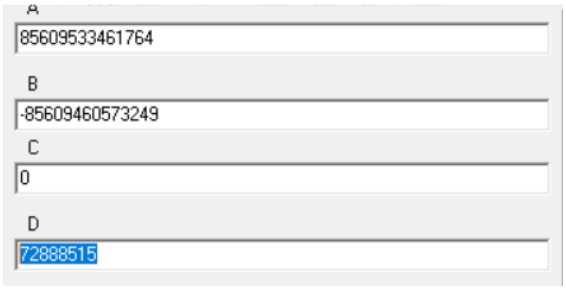


Проверка, что w2 – квадрат целого числа

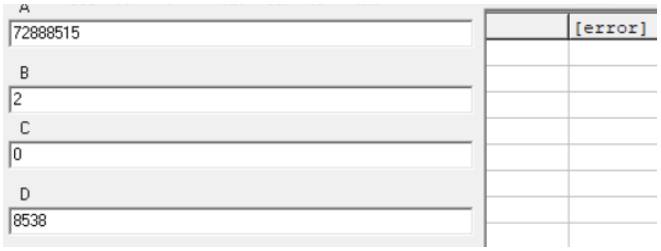


Нет – берем t3=9252542, t3^2=85609533461764

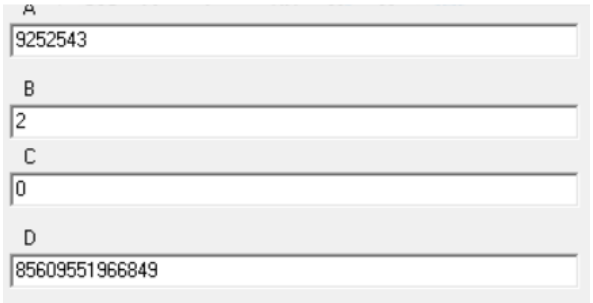
w3=t3^2-N=72888515



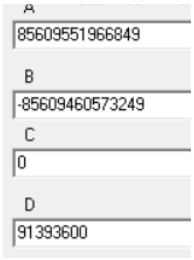
Проверка что w3 – квадрат целого числа



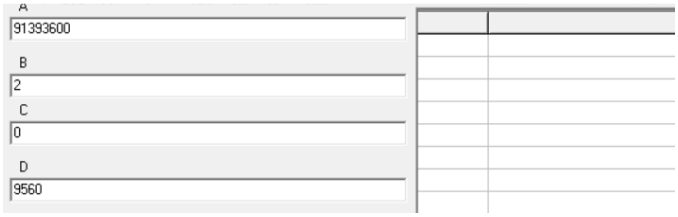
Нет. Берем t4=t3+1=9252543, t4^2=85609551966849



w4=t4^2-N=91393600

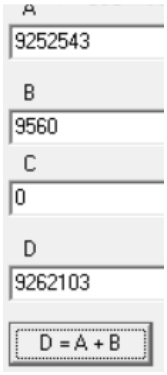


Проверка что w4 – квадрат целого числа

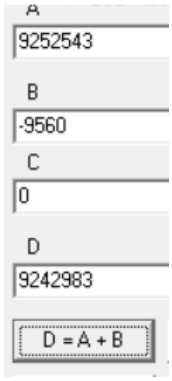


Да. Заканчиваем шаг.

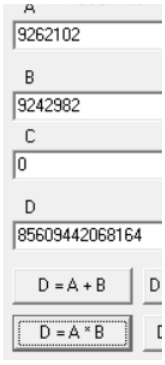
3. t4=9252543, sqrt(w4)=9560
4. p=t4+sqrt(w4)= 9262103



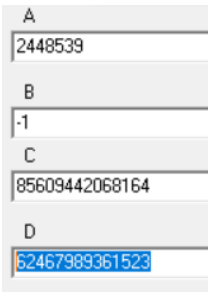
q=t4-sqrt(w4)= 9242983



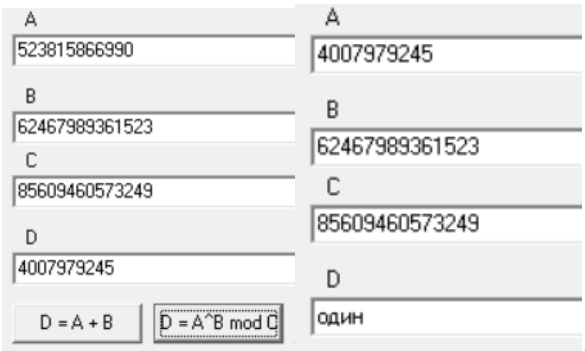
Phi(N)=(p-1)(q-1)= 85609442068164

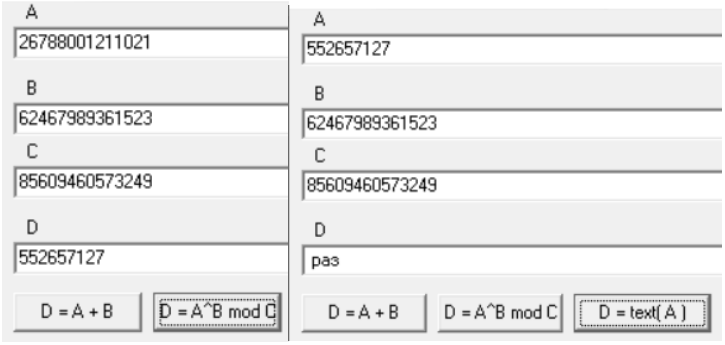


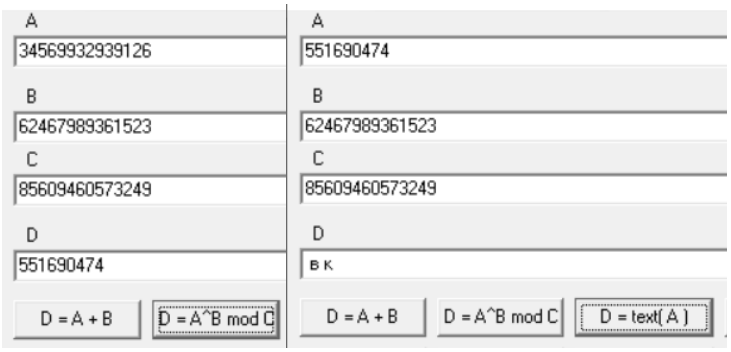
d=e^-1 mod Phi(N)= 62467989361523

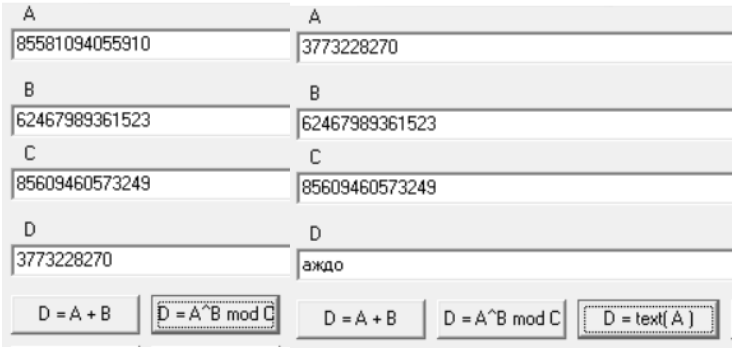


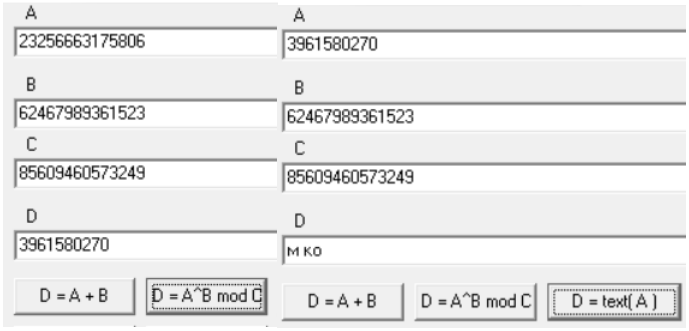
5. Дешифрация

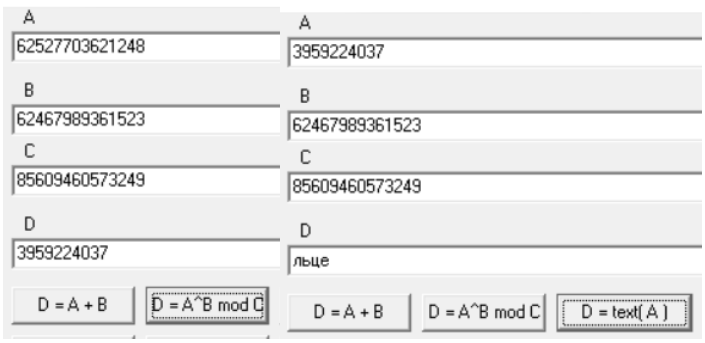


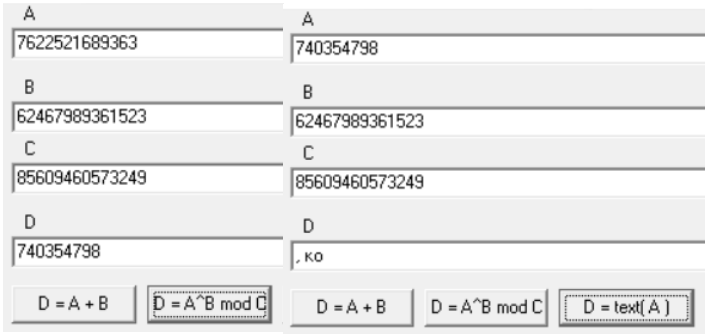


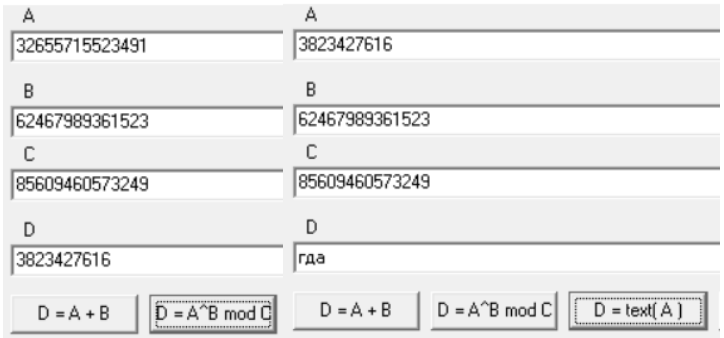


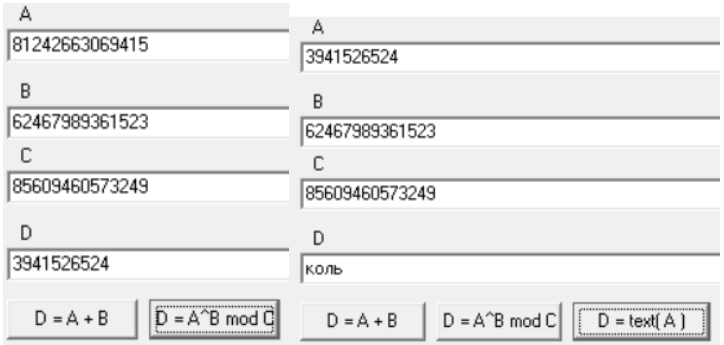


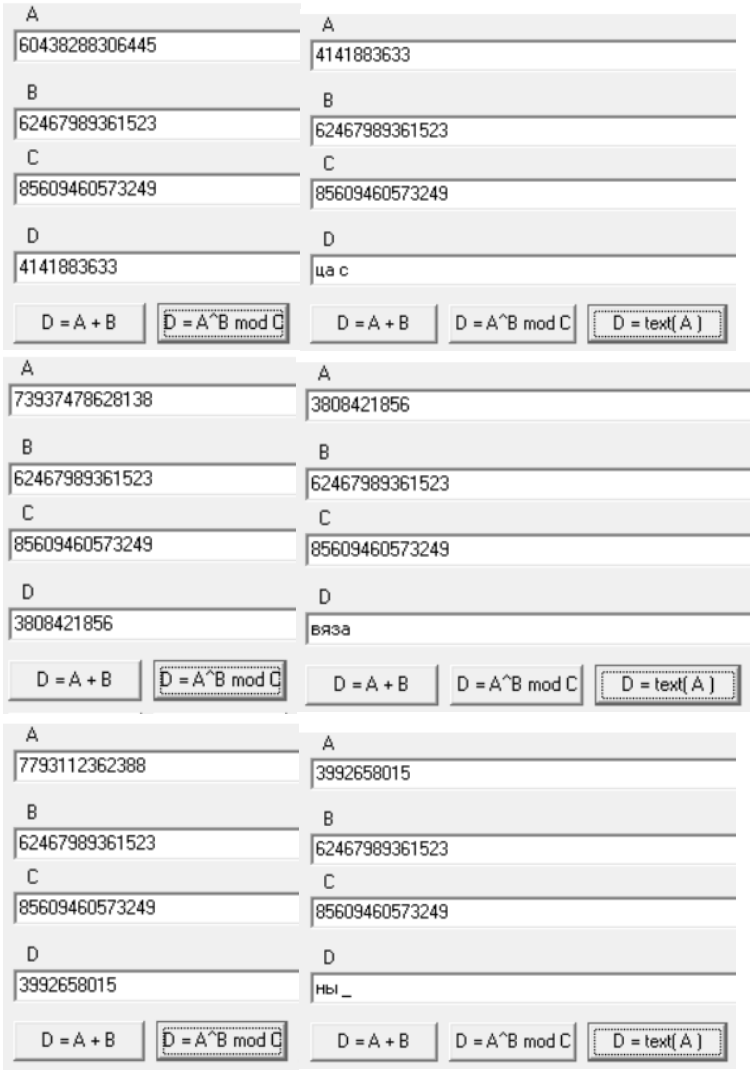

A
23256663175806
B
62467989361523
C
85609460573249
D
3961580270
D = A + B
D = A^B mod C
A
3961580270
B
62467989361523
C
85609460573249
D
м ко
D = A + B
D = A^B mod C
D = text(A)


A
62527703621248
B
62467989361523
C
85609460573249
D
3959224037
D = A + B
D = A^B mod C
A
3959224037
B
62467989361523
C
85609460573249
D
льце
D = A + B
D = A^B mod C
D = text(A)


A
7622521689363
B
62467989361523
C
85609460573249
D
740354798
D = A + B
D = A^B mod C
A
740354798
B
62467989361523
C
85609460573249
D
, ко
D = A + B
D = A^B mod C
D = text(A)


A
32655715523491
B
62467989361523
C
85609460573249
D
3823427616
D = A + B
D = A^B mod C
A
3823427616
B
62467989361523
C
85609460573249
D
гда
D = A + B
D = A^B mod C
D = text(A)


A
81242663069415
B
62467989361523
C
85609460573249
D
3941526524
D = A + B
D = A^B mod C
A
3941526524
B
62467989361523
C
85609460573249
D
коль
D = A + B
D = A^B mod C
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.