МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное автономное

образовательное учреждение высшего образования

«Национальный исследовательский университет ИТМО»

Факультет программной инженерии и компьютерной техники

ЛАБОРАТОРНАЯ РАБОТА №3

“Основы шифрования данных”

по дисциплине

“Информационная безопасность”

Вариант №12

Студент:

Миху Вадим Дмитриевич

Группа P34301

Преподаватель:

Рыбаков Степан Дмитриевич

г. Санкт-Петербург

2024

Цель работы:

Изучить атаку на алгоритм шифрования RSA посредством метода Ферма.

Вариант 5:

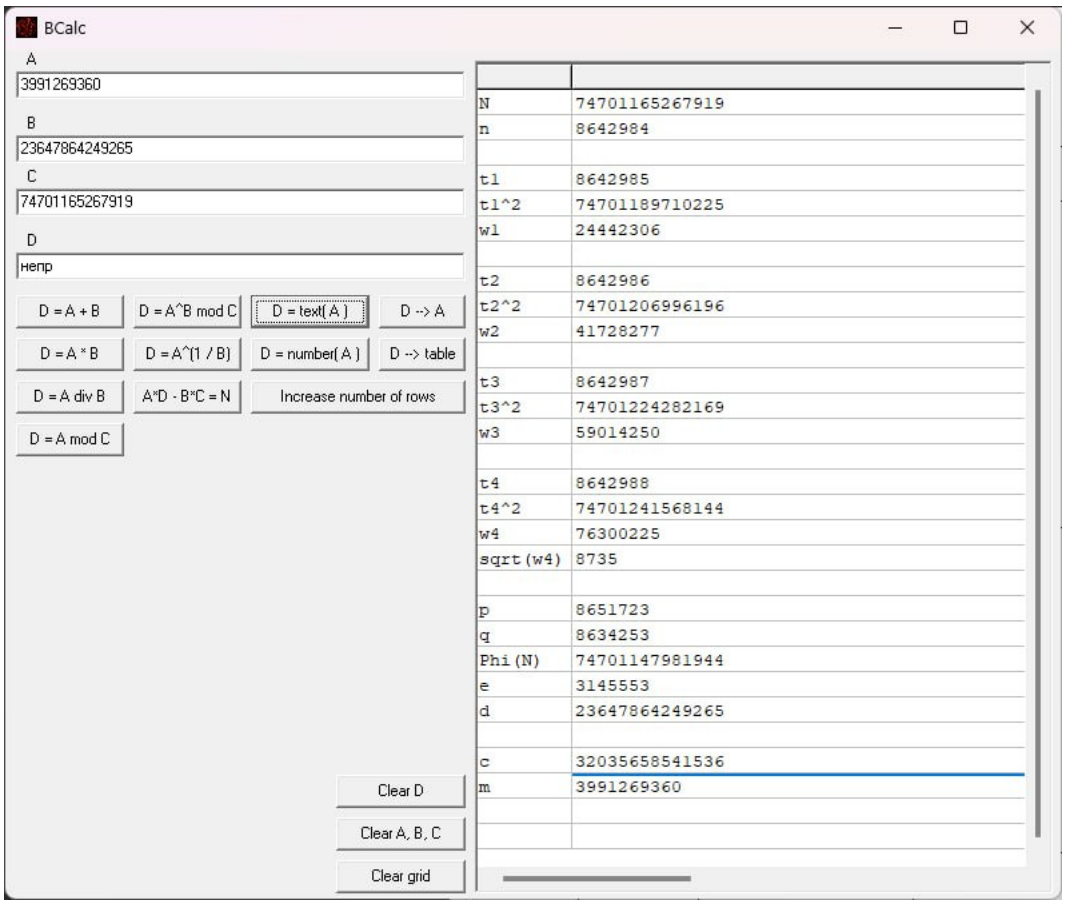
Вариант	Модуль, *N*	Экспонента, *e*	Блок зашифрованного текста, *C*
12	74701165267919	3145553	32035658541536 35242897170964 6268303368709 6877322610982 16329207109754 35007623593376 26715311593240 36220800128563 25019660581036 61639733671958 21186453949445 72477207535811

Выполнение:

Исходные данные: N = 74701165267919; e = 3145553; C = 32035658541536. Найти

1. Вычисляем $n = [\sqrt{N}] + 1$. В поле A помещаем N, в поле B – 2; нажимаем кнопку «$D = A\text{^}(1/B)$». В поле D заносится число 8642984, в первую строку таблицы – сообщение «[error]». Это свидетельствует, о том, что N не является квадратом целого числа.
2. $t_1 = n + 1$. Возводим число t1 в квадрат: A: = 8642985, B: = 2, C: = 0 (возведение в квадрат будет производиться не по правилам модульной арифметики), нажимаем «$D = A\text{^}B \ mod \ C$» => $D = t_1^2$ = 74701189710225. Вычисляем $w_1 = t_1^2 - N$. Для этого $A := t1^2, B: = -N$, затем нажимаем «$D = A + B$» => $D = w_1$ = 24442306. Проверяем, является ли w1 квадратом целого числа: $A: = w_1, B: = 2$, нажимаем «$D = A\text{^}(1/B)$» => в первой строке таблицы появляется сообщение «[error]», следовательно проделываем п. 2 заново с $t_2 = n + 2$ и так далее, пока не найдем, что некое wi является квадратом целого числа.
3. При вычислении квадратного корня w4 первая строка таблицы остается пустой, а D = $\sqrt{w_4} = 8735$, что свидетельствует об успехе факторизации. $t_4 = 76300225$.
4. Вычисляем $p = t_4 + \sqrt{w_4}$; $A: = t_4, B: = \sqrt{w_4}$, нажимаем «$D = A + B$» => $D = p$ = 8651723; $q = t_4 - \sqrt{w_4}$ = 8634253. Вычисляем $\varphi(N) = (p - 1)(q - 1)$, A:= 8651722, B:= 8634252, нажимаем «$D = A \cdot B$» => $D = \varphi(N)$ = 74701147981944. Вычисляем d, как обратный к e: $A: = e, B: = -1, C: = \varphi(N)$, нажимаем «$D = A\text{^}B \ mod \ C$» => D = d = 23647864249265.
5. Производим дешифрацию шифрблока C: A:= C; B:= d; C:= N. Нажимаем «D = A^B mod C». В поле D находится исходное сообщение M = 3991269360. Переводим M в текстовый вид. Для этого A:= M, нажимаем «D = text(A)» => D = = «непр».

Снимок экрана с окном программы «BCalc» приведен ниже.



Результаты дешифровки

Исходный текст	Расшифровка
32035658541536	непр
35242897170964	авил
6268303368709	ьной
6877322610982	пер
16329207109754	есыл
35007623593376	ки п
26715311593240	акет
36220800128563	ов –
25019660581036	пов
61639733671958	торн
21186453949445	ые п
72477207535811	ере-

Итоговое сообщение: “неправильной пересылки пакетов – повторные пере-”

Вывод:

В результате выполнения данной лабораторной работы я изучил атаку на алгоритм шифрования RSA посредством метода Ферма.