УНИВЕРСИТЕТ ИТМО

Факультет программной инженерии и компьютерной техники

Направление подготовки 09.03.04 Программная инженерия

Дисциплина «Информационная безопасность»

**Лабораторная работа №1.1**

Атака на алгоритм шифрования RSA посредством метода Ферма

*Вариант 22*

Студент

*Патутин В. М.*

*P33101*

Преподаватель

*Маркина Т. А.*

Санкт-Петербург, 2022 г.

Цель работы

Изучить атаку на алгоритм шифрования RSA посредством метода Ферма.

Исходные данные:

*N =* 50824793010569

*e =* 4440901

*Блок текста C:*

14852129687156

2828083503727

40199165363197

50374743756265

38804027318759

48809751439118

17692593759762

11950610647201

31150513650241

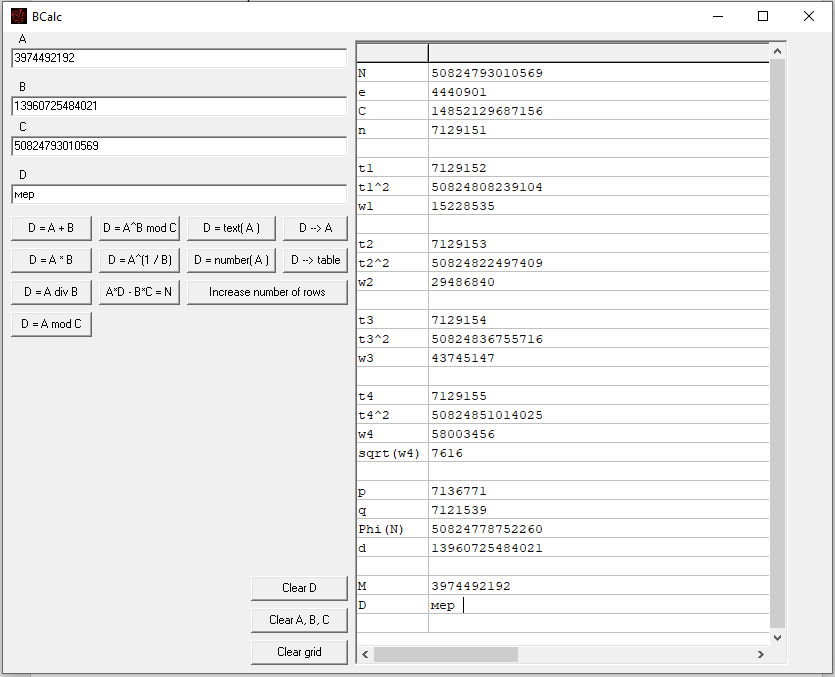
18538876359272

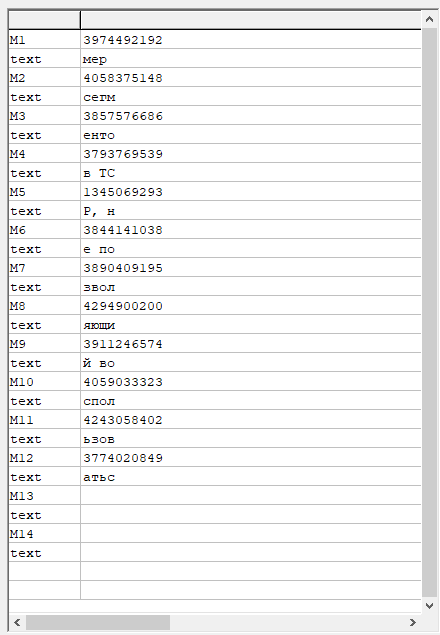
30210358214233

23631880532900

Выполнение работы

1. Вычисляем n = [sqrt(N)] + 1.
   1. Видим сообщение “[error]”, которое значит, что N - не квадрат целого числа.
2. Вычисляем t1 = n + 1 и далее d1 = t1^2 – N.
3. Проверяем, является ли d1 квадратом целого числа аналогично первому шагу.
   1. Снова видим сообщение “[error]”
4. Вычисляем t2 = t1 + 1 и d2 аналогично шагу 2.
5. Повторяем вычисления пока не дойдем до квадрата целого числа т.е. пока не перестанем видеть сообщение “[error]”
6. Дойдя до d6 не получаем сообщения об ошибке.
7. Вычисляем квадратный корень из d6.
8. Вычисляем p = t6 + sqrt(d6).
9. Вычисляем q = t6 – sqrt(d6).
10. Вычисляем Phi(N) = (p – 1)(q – 1).
11. Вычисляем d, как обратный к e: d = e^(-1) mod Phi(N).
12. Построчно выполняем дешифрацию текста. На каждую строку блока C вычисляем M= C^d mod N5.
13. Переводим каждое число в текстовый вид





Выводы

При выполнении лабораторной работы я изучил метод Ферма для атаки на алгоритм шифрования RSA