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

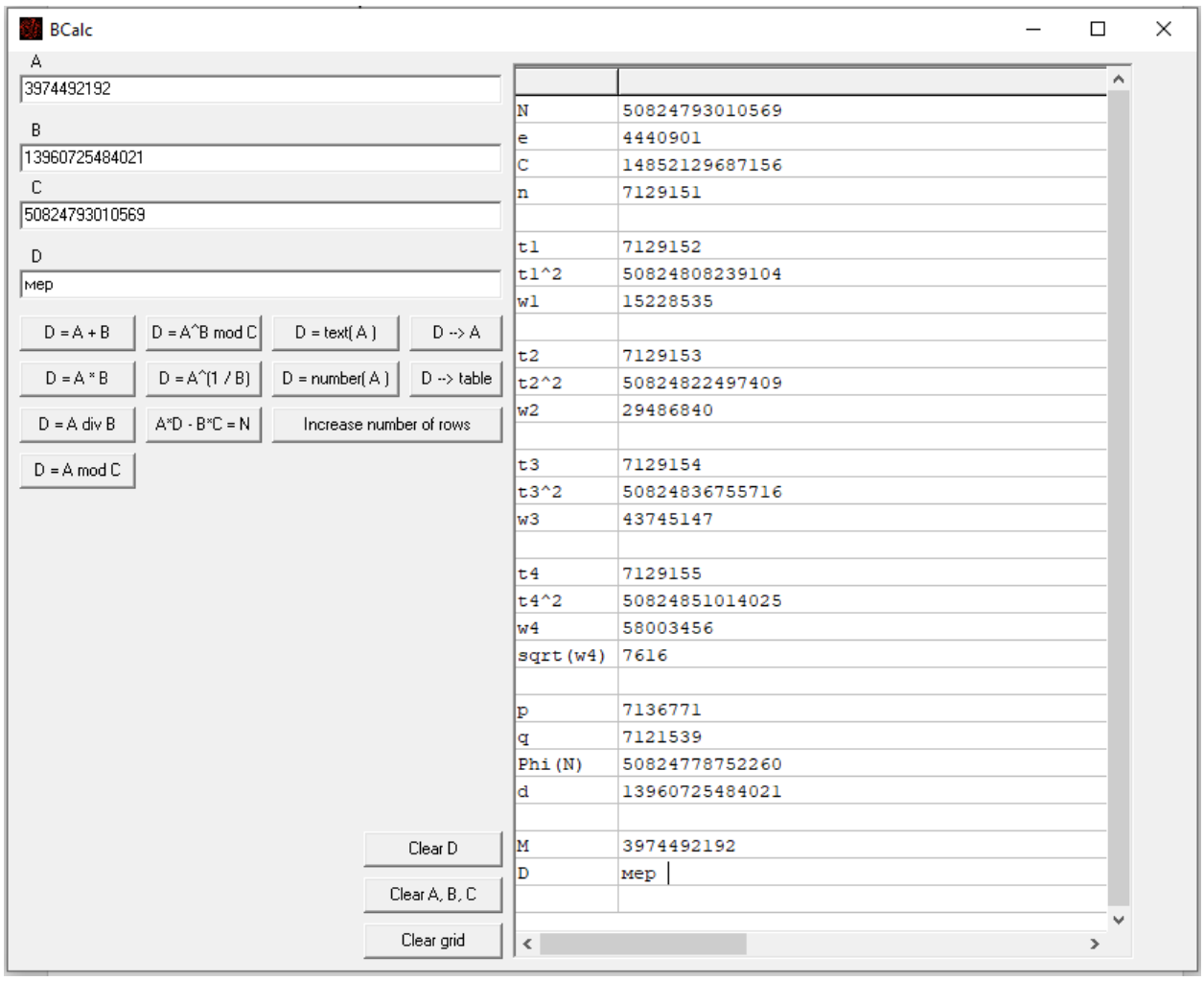
Изучить атаку на алгоритм шифрования RSA посредством метода Ферма.

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.
    a. 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.
    a. 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


BCalc
A
3974492192
B
13960725484021
C
50824793010569
D
мер
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
Clear D
Clear A, B, C
Clear grid
N 50824793010569
e 4440901
C 14852129687156
n 7129151
t1 7129152
t1^2 50824808239104
w1 15228535
t2 7129153
t2^2 50824822497409
w2 29486840
t3 7129154
t3^2 50824836755716
w3 43745147
t4 7129155
t4^2 50824851014025
w4 58003456
sqrt(w4) 7616
p 7136771
q 7121539
Phi(N) 50824778752260
d 13960725484021
M 3974492192
D мер

M1	3974492192
text	мер
M2	4058375148
text	сегм
M3	3857576686
text	ento
M4	3793769539
text	в ТС
M5	1345069293
text	Р, н
M6	3844141038
text	е по
M7	3890409195
text	звол
M8	4294900200
text	яющи
M9	3911246574
text	й во
M10	4059033323
text	спол
M11	4243058402
text	ьзов
M12	3774020849
text	атьс
M13	
text	
M14	
text	

Выводы

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