       Министерство науки и высшего образования Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

“НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО”

Факультет Программной инженерии и компьютерной техники



Отчет

По лабораторной работе

№ 1. Атака на алгоритм шифрования RSA посредством метода Ферма

По предмету:  Информационная безопасность

Вариант 1

Студент:

Андрейченко Леонид Вадимович

Группа P34301

Преподаватель:

Маркина Татьяна Анатольевна

Санкт-Петербург

2023

Цель работы

Изучить атаку на алгоритм шифрования RSA посредством метода Ферма.

Выполнение

Исходные данные

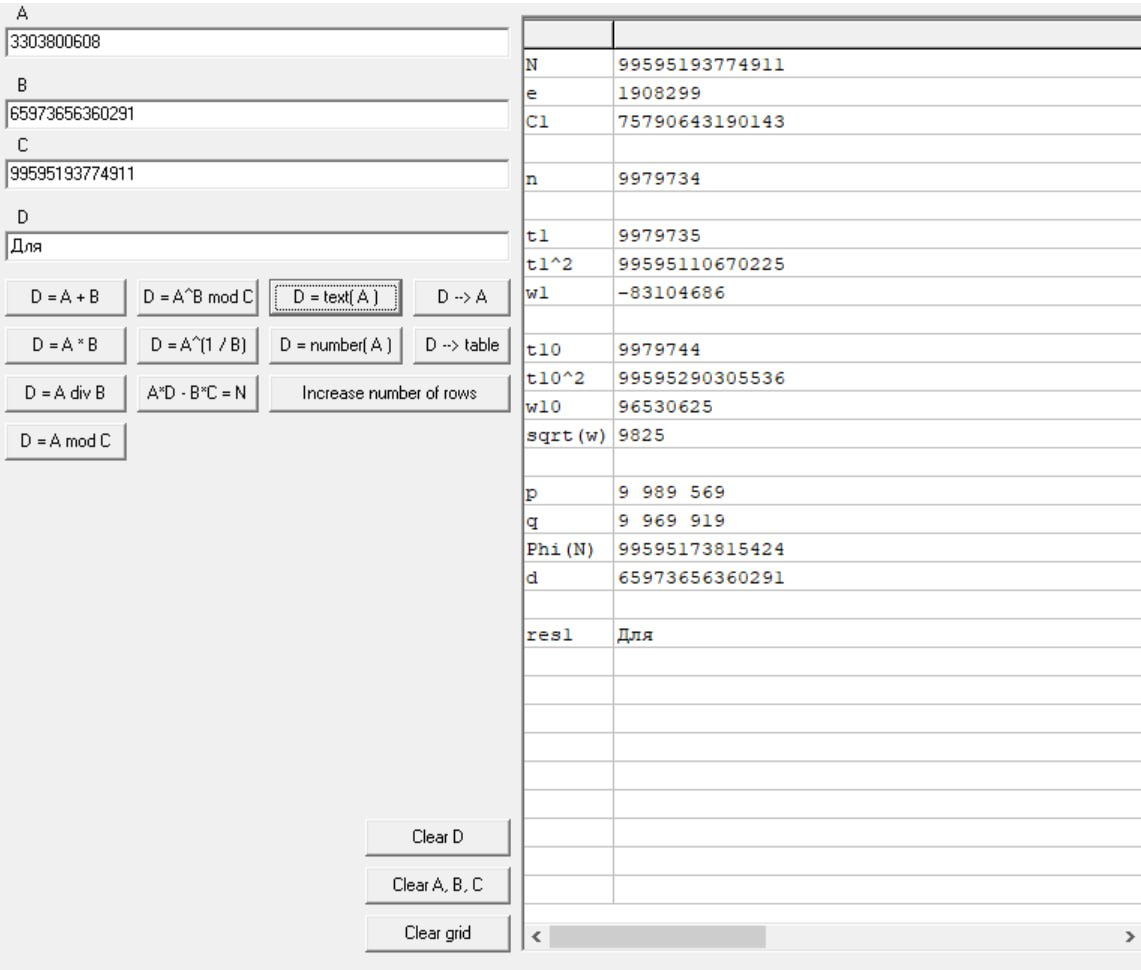
* N = 99595193774911
* e = 1908299
* C = 75790643190143 36869061035180 38422576553598 68899435645717 16193161920958 98487458352335 34167725433806 96613844267045 26583768908805 73052827576371 94695336463618 69092596694070

1. В начале вычислим n = [sqrt(N)] + 1 = sqrt(99595193774911) + 1 = 9979734
2. Начинаем поиск верных значений для w
   1. t1 = n + 1 = 9979735
   2. t1^2 = 99595110670225
   3. w1 = t1^2 – N = 99595110670225 - 99595193774911 = -83104686 – не является корнем целого числа, значит продолжаем поиск
   4. ....................................................................................................................................................
   5. t10 = n + 10 = 9979744
   6. t^2 = 99595290305536
   7. w10 = 99595290305536 - 99595193774911 = 96 530 625, sqrt = 9825. Останавливаем поиск
3. p = t10 + sqrt(w10) = 9979744 + 9825 = 9 989 569
4. q = t10 - sqrt(w10) = 9979744 - 9825 = 9 969 919
5. Phi(N) = (p – 1)(q – 1) = 99595173815424
6. d = 1 / e mod Phi(N) = 1 / 1908299 mod 99595173815424 = 65973656360291
7. Начинаем расшифровку послания
   1. answer1 = C1 ^ d mod N = 75790643190143 ^ 65973656360291 mod 99595193774911 = 3303800608

Продолжая расшифровку для следующих блоков зашифрованного письма получаем расшифрованное послание:

Для работы алгоритма маршрутизации от источника\_

Листинг работы



Выводы

Я изучил атаку на алгоритм шифрования RSA посредством метода Ферма, а именно факторизовали N и нашли исходные параметры p и q. Успешность атаки объясняется неудачным выбором исходных параметров – у них была недостаточная разрядность.