федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»

Лабораторная работа №3

по дисциплине “Информационная безопасность”

на тему “Атака на алгоритм шифрования RSA посредством метода Ферма”

Вариант 3

Выполнила: Студентка гр. P3402

Калугина М. М.

Преподаватель: к.т.н, доцент

Маркина Т.А.

г. Санкт-Петербург

2021 г.

Цель

Изучение атаки на алгоритм шифрования RSA посредством метода Ферма.

Задание

Используя разложение модуля на простые числа методом Ферма и полученные исходные данные, определить следующие показатели:
– множители модуля (p и q);
– значение функции Эйлера для данного модуля $\varphi(N)$
– обратное значение экспоненты по модулю $\varphi(N)$
Расшифровать зашифрованный текст, исходный текст должен быть фразой на русском языке

Исходные данные

Вариант 3:
N = 93767386321457
e = 2091619
C = 62984326732858 22123186696272 24425203655789 45995309006047 8176196426076 12816278693250 27474201663022 86909026690842 20469575723850 29205116646939 21002901408912 79168478687790

Ход работы

Шаг 1.

На первом шаге необходимо определить множители p и q.

Для этого сначала необходимо посчитать значение n = $\sqrt{N} + 1$. С этого значения будет начинаться поиск таких p и q, произведение которых будет давать N. Чем ближе расположены p и q, тем меньше итераций потребуется для их поиска.

Алгоритм поиска p и q:

1. Присваиваем полученное значению переменной t_i.
2. Возводим t_i в квадрат
3. Рассчитываем значение $w_i = t_i^2 N$.
4. Проверяем, является ли значение w_i квадратом некоторого числа. Если число не является квадратом, увеличиваем значение n на единицу и возвращаемся к шагу 1.

5. Когда значение w_i найдено, переходим к расчету p и q: $p = t_i + sqrt(w_i)$, $= t_i + sqrt(w_i)$

На рисунке 1 представлен итеративный расчет значений p и q:

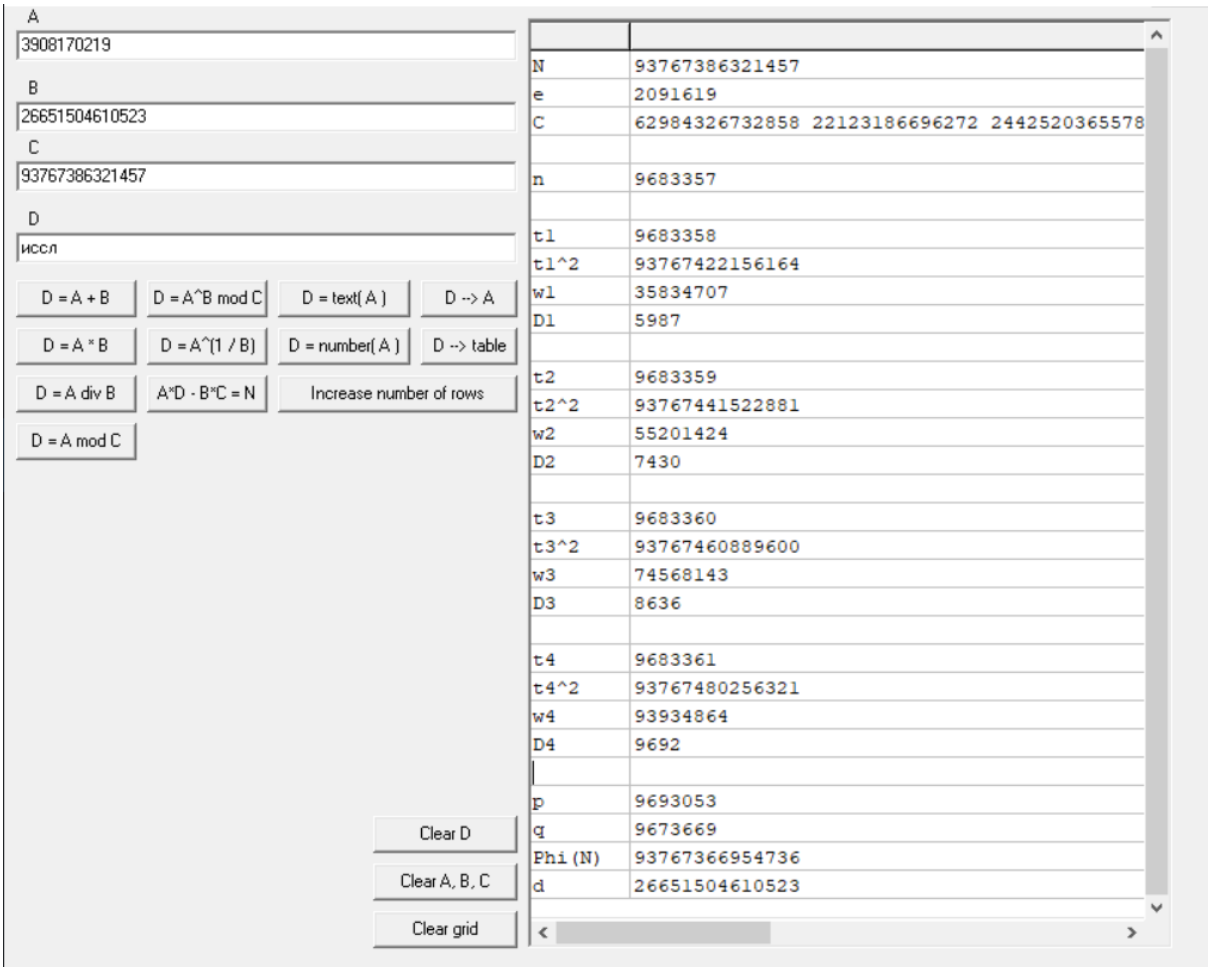

Рисунок 1. Расчет значений p и q

Шаг 2

Расчет значений φи обратного значения экспоненты по модулю $\varphi(N)$

Расчет φпроизводится по формуле: $\phi(N) = (p-1)(q-1)$.

Пусть d - значение обратное к e по модулю $\varphi(N)$. Тогда результат d будет вычисляться по формуле: $d = e^{-1} mod \phi(N)$

Численные значения d и $\varphi(N)$ представлены в двух последних строчках рисунка 1.

Шаг 3. Дешифрование.

Для каждого блока C_i производятся следующие вычисления:

$$M_i = C_i^d mod N$$

В блоках M_i хранится дешифрованная информация.
На рисунке 2 представлено итеративное декодирование зашифрованной фразы:

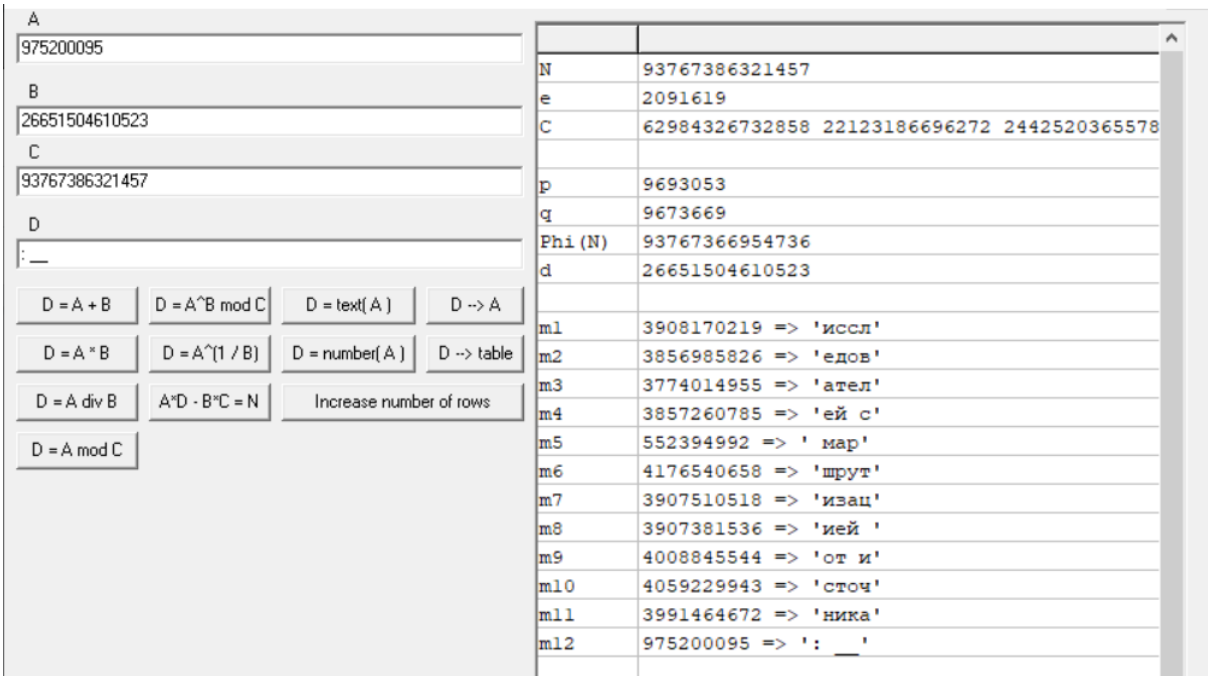

Рисунок 2. Дешифрование.

Результат

Итоговая фраза звучит так “исследователей с маршрутизацией от источника: __”

Вывод

В ходе выполнения лабораторной работы был изучен метод шифрования RSA, были получены навыки дешифрования алгоритма шифрования RSA посредством метода Ферма и была проведена дешифрация фразы путем решения уравнения $t^2 - w^2 = n$ для определения значений p и q, после чего дешифрование сводится к последовательному расчету пары значений: $\varphi(N)$ и d и дальнейшему дешифрованию закодированных блоков.