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

Лабораторная работа №5

по дисциплине “Информационная безопасность”

на тему “Атака на алгоритм шифрования RSA методом бесключевого чтения ”

Вариант 3

Выполнила: Студентка гр. P3402

Калугина М. М.

Преподаватель: к.т.н, доцент

Маркина Т.А.

г. Санкт-Петербург

2021 г.

Цель работы

Изучить атаку на алгоритм шифрования RSA посредством повторного шифрования.

Задание

Определить значения r и s при условии, чтобы e1·r – e2·s = 1, используя расширенный алгоритм Евклида.
Используя полученные выше значения r и s, записать исходный текст.

Исходные данные

Вариант 3:
N = 445632735571
e_1 = 1120289
e_2 = 559633
C_1 = 348555354398 351363944134 96907337112 141119651255 317600466893 84967944527 340088880266 311235549494 41838603784 333172824695 89494655477 3256803669
C_2 = 366337925832 29318249989 120058862823 428190500861 322426909958 286841513079 150392378882 441874945028 297137742269 304115257300 123106598046 110955623263

Ход работы

Шаг 1. Решение уравнения

Решаем уравнение e1·r – e2·s = ±1: для этого помещаем в поле A, B, C значения $_1$, e_2 и N соответственно.

В результате, в поле C будет храниться значение s, а в поле D -- значение r.

Результат первого шага: s = 64611, r = 32276 (см. рис. 1).

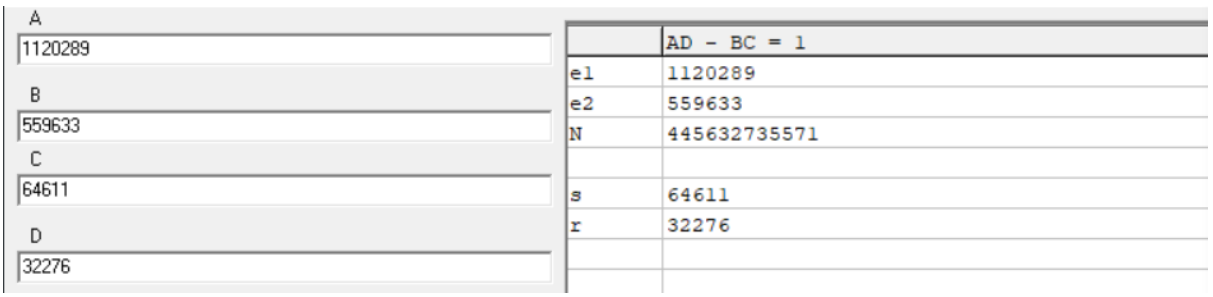

Рисунок 1. Шаг 1.

Шаг 2. Дешифрование зашифрованного текста.

Для дешифрации: каждый блок $$ c_1 $$ возводим в степень r, а каждый блок $$ c_2 $$ – в степень (–s) по модулю N.
После, значения перемножаются по модулю N и этот результат приводится к тексту. На рисунке 2 представлено дешифрование первого блока:

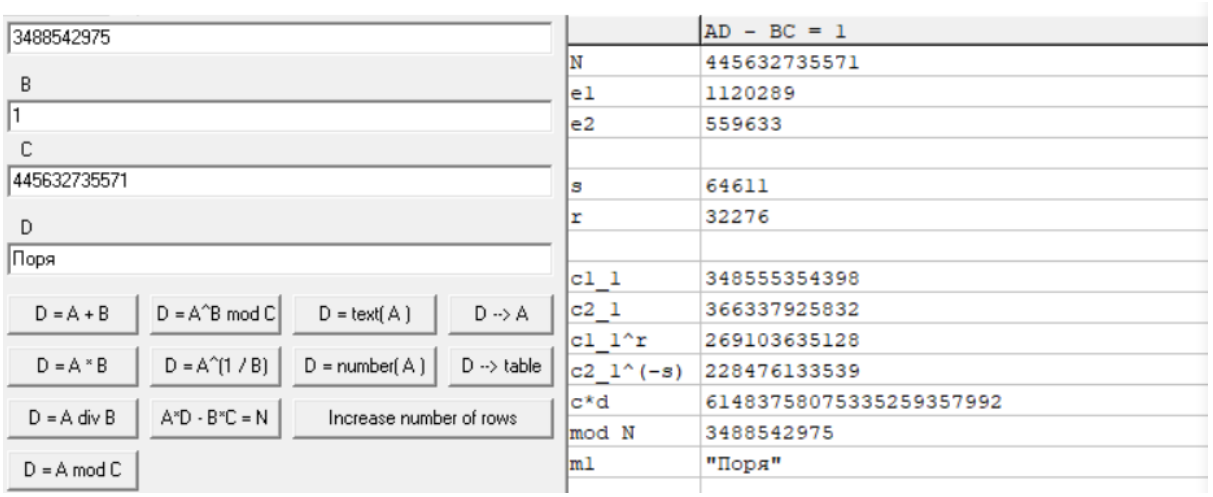

Рисунок 2. Дешифрация первого блока.

На рисунке 3 представлено дешифрование всего текста:

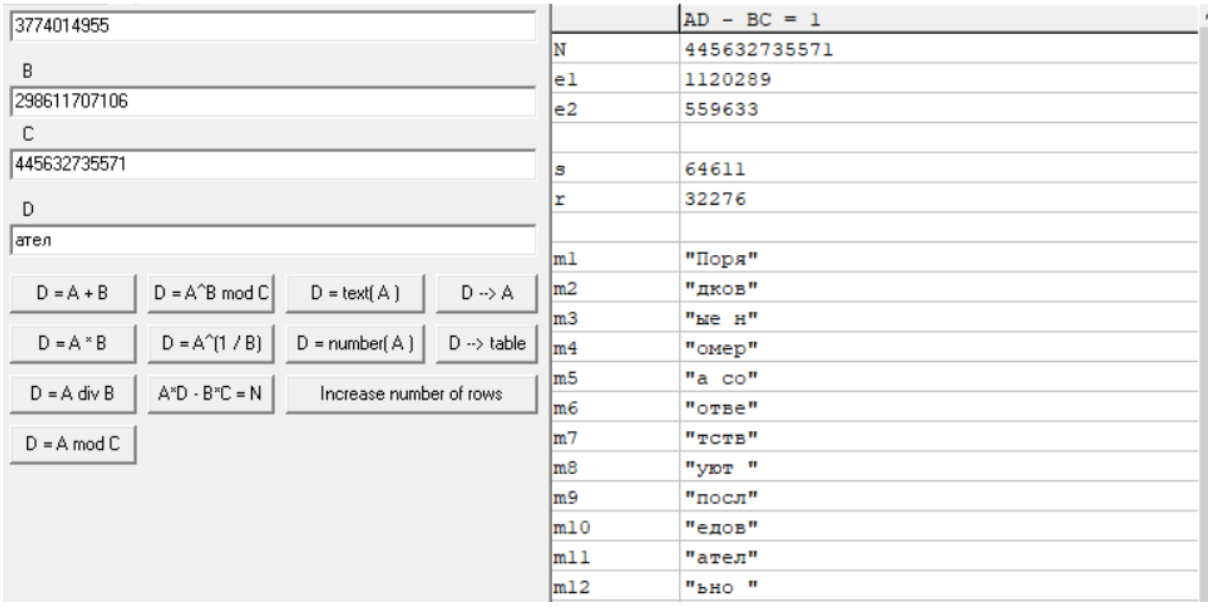

Рисунок 3. Дешифрование закодированного текста.

Результат

В результате была получена фраза: “Порядковые номера соответствуют последовательно ”

Вывод

В ходе данной лабораторной работы был изучен метод атаки на алгоритм шифрования RSA посредством метода бесключевого чтения.