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

Лабораторная работа №6

по дисциплине “Информационная безопасность”

на тему “Атака на алгоритм шифрования RSA, основанная на Китайской теореме об остатках”

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 китайской теореме об остатков.

Задание

Используя Китайскую теорему об остатках, получить исходный текст;

Исходные данные

Вариант 3:
e = 3
N_1 = 380077454101
N_2 = 380903460337
N_3 = 383306345689
C_1 = 120321295984 116941070964 156315192664 260149644765 357688967002 165841867143 349826484990 337993834720 117681826230 36279369135 124613350713 106958422772
C_2 = 261990433834 232071459327 305414687540 348455852917 206680974925 327578130329 5548686870 295985428633 157420509616 256913681356 271869775627 310864218021
C_3 = 322305651846 286065905390 188633713225 131649116365 253206684415 46677871611 65268441973 317133281785 52226297600 255637668770 201873507225 260192105953

Ход работы

Шаг 1.

Необходимо вычислить значения:

$$M_0 = N_1 * N_2 * N_3$$
$$m_1 = N_2 * N_3$$
$$m_2 = N_1 * N_3$$
$$m_3 = N_1 * N_2$$
$$n_1 = m_1^{-1} mod N_1$$
$$n_2 = m_2^{-1} mod N_2$$
$$n_3 = m_3^{-1} mod N_3$$

Результаты вычислений представлены на рисунке 1.

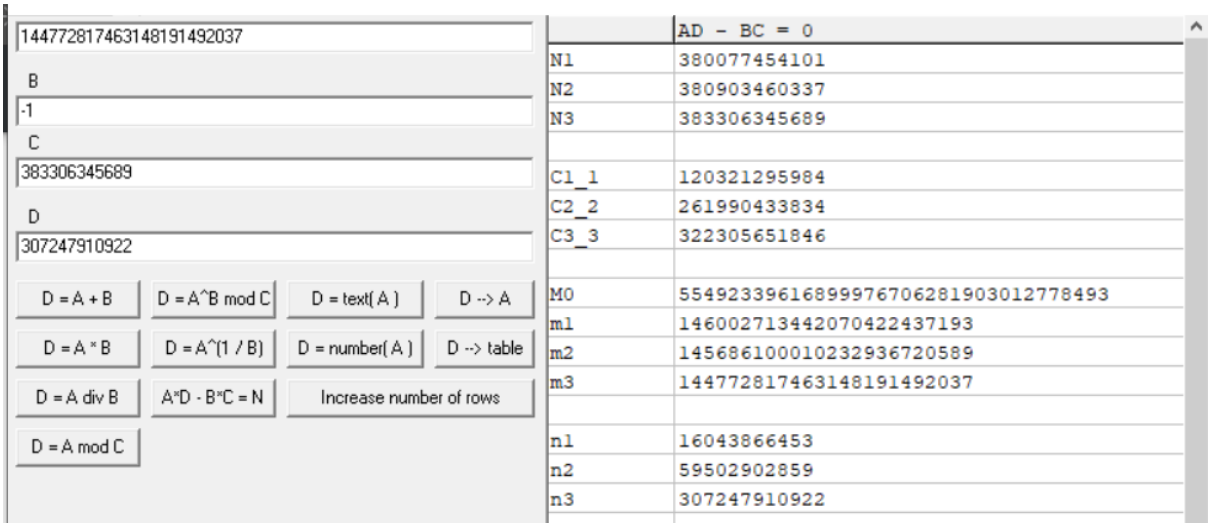

Рисунок 1. Шаг 1 - расчет констант

Шаг 2.

Для каждого блока итеративно необходимо рассчитать значение S и M

$$S = c_{1,i} * n_1 * m_1 + c_{2,i} * n_2 * m_2 + c_{3,i} * n_3 * m_3$$

$$M_i = (S mod M_0)^{(1/e)}$$

Значение M хранит зашифрованный текст.

На рисунке 2 представлено итеративное декодирование закодированной фразы.

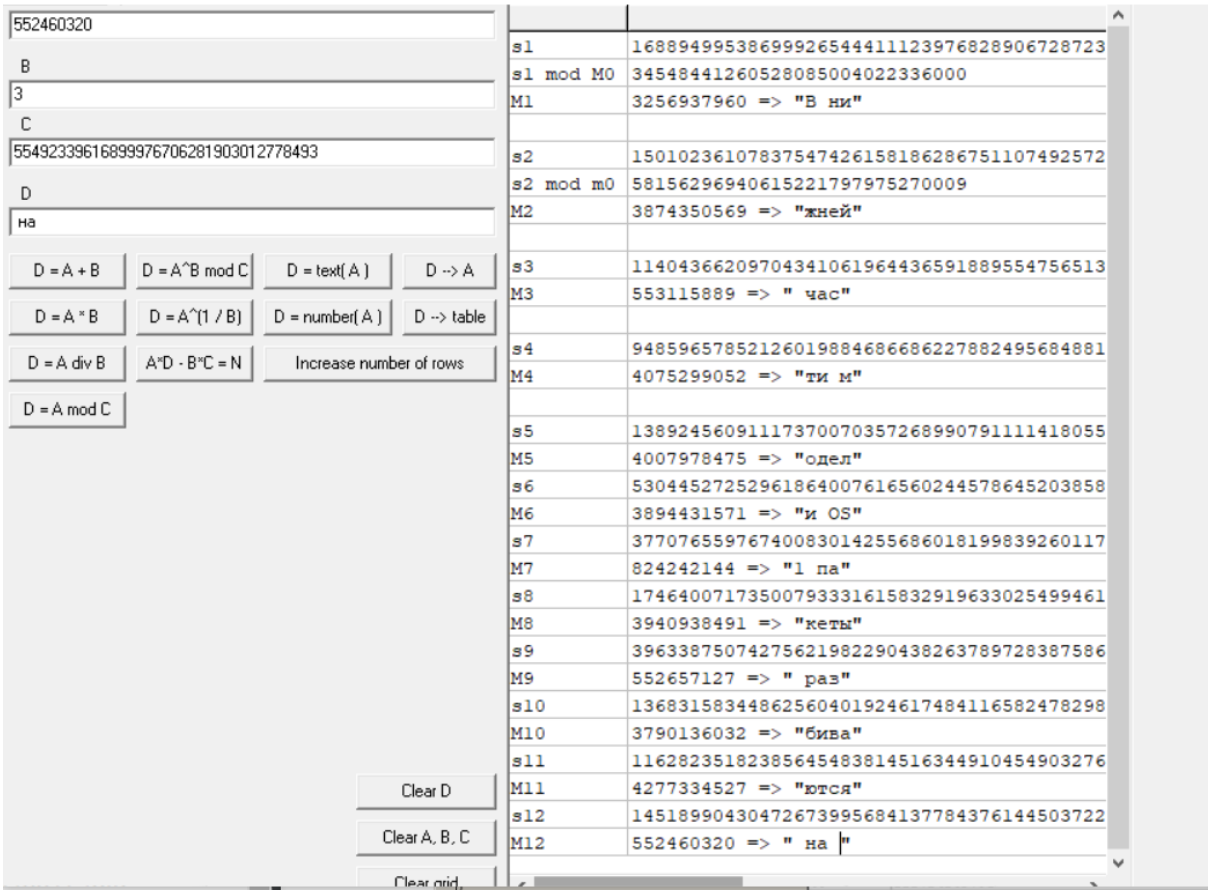

Рисунок 2. Декодирование закодированной фразы

Результат

Была получена фраза “В нижней части модели OSI пакеты разбиваются на ”

Вывод

В ходе выполнения лабораторной работы была изучена атака на алгоритм шифрования RSA посредством китайской теореме об остатков.