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

Лабораторная работа №4

по дисциплине “Информационная безопасность”

на тему “Атака на алгоритм шифрования RSA методом повторного шифрования”

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

Используя метод перешифрования, определить порядок числа e в конечном поле $Z_{\phi(N)}$

Используя значение порядка экспоненты, получить исходный текст методом перешифрования;

Исходные данные

Вариант 3:
N = 385181864647
e = 938573
C = 331245775481 282425324609 65377570000 89972965825 264803627317 320989226085 324723654667 294634302620 142237555971 221994269576 209958712589 221718426295 163788492835

Ход работы

Шаг 1. Определение порядка экспоненты.

Внесем значения N и e в программу.
Внесем в поле Y произвольное число, меньшее N, в качестве значения Y было выбрано число 123456.
Запускаем повторное шифрование и дожидаемся, пока в поле X появится значение, равное корню e степени от числа Y по модулю N, а в поле i – порядок e в конечном поле $Z_{\varphi(N)}$. В результате получаем число X = 137411149345 (см. рис. 1)

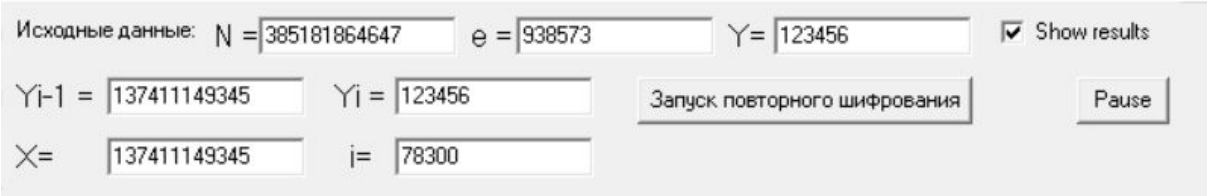

Рисунок 1. Шаг 1.

Шаг 2. Дешифрование зашифрованного текста.

В область редактирования поля C необходимо поместить блоки зашифрованного текста, разделенные символом конца строки, значение модуля в поле N, экспоненты в поле e и порядка экспоненты в поле i. Затем нажать на кнопку “Дешифрация” и дождаться появления исходного текста в области редактирования M.

Результат работы дешифрации представлен на рисунке 2.

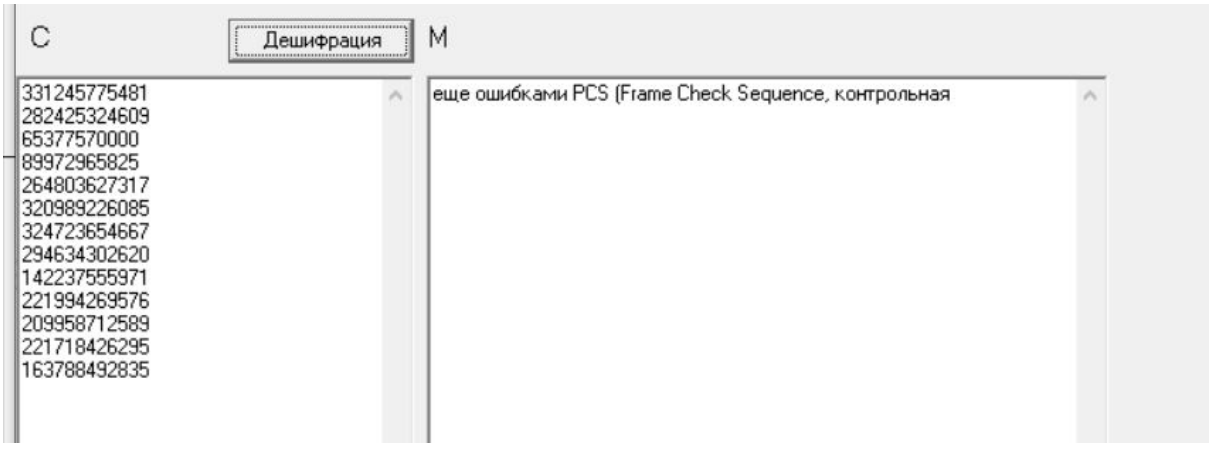

Рисунок 2. Дешифрация закодированного текста.

Результат

В результате была получена фраза: “еще ошибками PCS (Frame Check Sequence, контрольная”

Вывод

В ходе данной лабораторной работы был изучен метод атаки на алгоритм шифрования RSA путем использования повторного шифрования.