ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

Факультет программной инженерии и компьютерной техники

ЛАБОРАТОРНАЯ РАБОТА № 2.2

ПО ДИСЦИПЛИНЕ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Атака на алгоритм шифрования RSA методом повторного шифрования

Выполнил: Давыдов Иван Денисович

Группа: P3400

Вариант 5

Санкт-Петербург

2020/2021

Цель

Изучить атаку на алгоритм шифрования RSA посредством повторного шифрования.

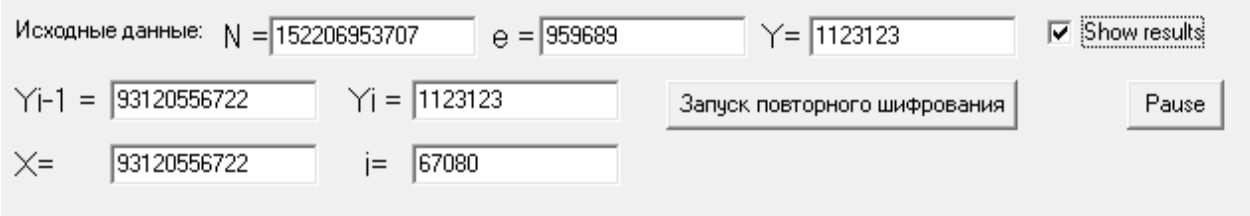
Задание

Вариант	Модуль, N	Экспонента, e	Блок зашифрованного текста, C
5	152206953707	959689	106157029398 26037756325 64970468176 111381095515 102219112033 10446585653 125818085975 140293474360 118182182667 102323948722 81537011095 534009223 79513867811

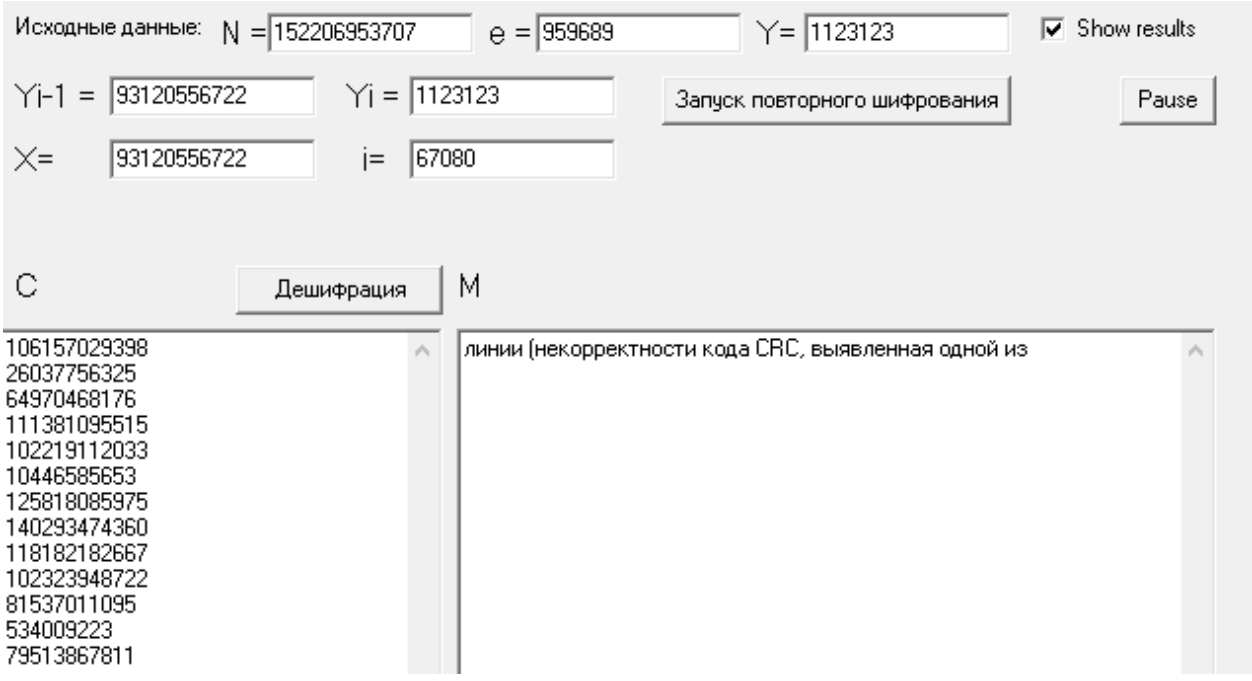
Выполнение

Для выполнения работы использовалась программа PS.exe.

Определим порядок экспоненты:



Дешифруем сообщение:



Итоговый текст:

линии (некорректности кода CRC, выявленная одной из

Выводы

В ходе выполнения лабораторный работы была успешно проведена атака методом повторного шифрования на алгоритм RSA.