       Министерство науки и высшего образования Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

“НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО”

Факультет Программной инженерии и компьютерной техники



Отчет

По лабораторной работе № 2

Атака на алгоритм шифрования RSA посредством повторного шифрования

По предмету:  Информационная безопасность

Вариант 1

Студент:

Андрейченко Леонид Вадимович

Группа P34301

Преподаватель:

Маркина Татьяна Анатольевна

Санкт-Петербург

2023

Цель работы

Изучить атаку на алгоритм шифрования RSA посредством повторного шифрования.

Выполнение

Исходные данные:

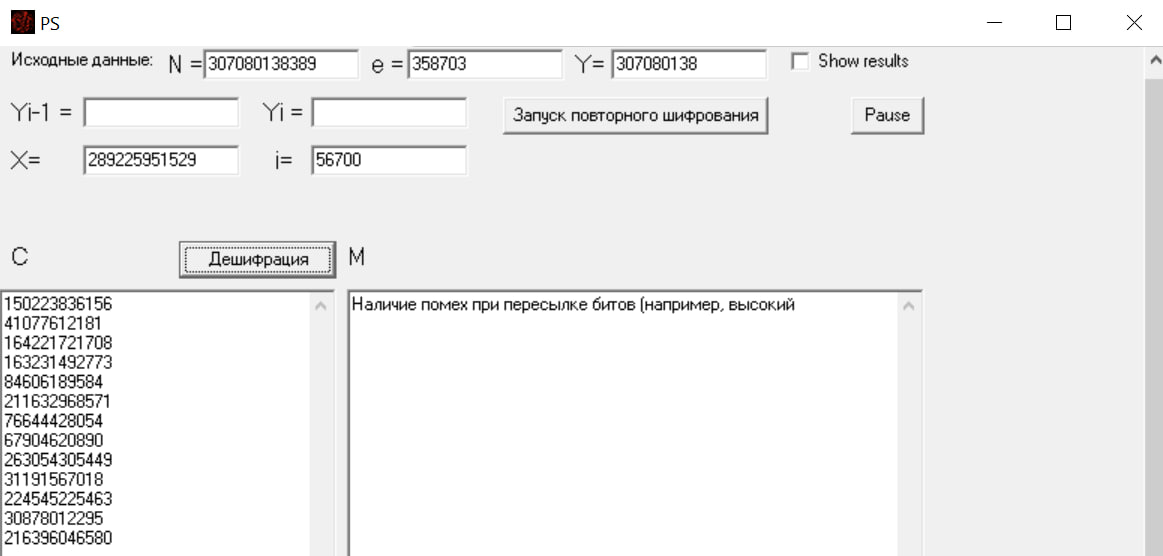
* Модуль N = 307080138389
* Экспонента e = 358703
* Блок зашифрованного текста С = 150223836156 ...

Используя метод перешифрования удалось вычислить порядок числа e = 56700

Используя значение порядка экспоненты, я получил исходный текст методом перешифрования.

Исходный текст: "Наличие помех при пересылке битов (например, высокий"

Листинг программы



Выводы

Я изучил атаку на алгоритм шифрования RSA посредством метода повторного шифрования. Анализ метода повторного шифрования хорошо показывает необходимость соблюдения требований на выбор p и q для обеспечения стойкости. Неудачный выбор криптосистемы привел к тому, что атака методом повторного шифрования дала результат почти сразу, тогда как нахождение d потребовало бы на порядок больших вычислений.