УНИВЕРСИТЕТ ИТМО

Факультет программной инженерии и компьютерной техники

Направление подготовки 09.03.04 Программная инженерия

Дисциплина «Информационная безопасность»

**Лабораторная работа №2.2**

Атака на алгоритм шифрования RSA методом повторного шифрования

*Вариант 13*

Студент

*Крюков А. Ю*

*P33101*

Преподаватель

*Маркина Т. А.*

Санкт-Петербург, 2022 г.

Цель работы

Изучить атаку на алгоритм шифрования RSA посредством повторного шифрования.

Исходные данные:

*N =* 915012974539

*e =* 1001953

*Блок текста C:*

763770087861  
 432343847598

764682728575

206635140312

627210520886

794063631890

309297959146

68118108284

116045398315

912085643674

257483784869

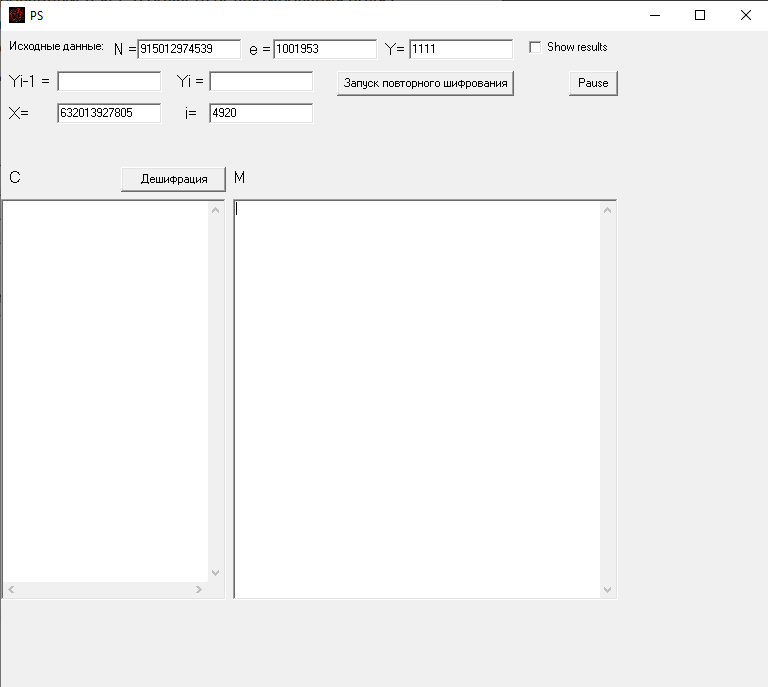
167814127445

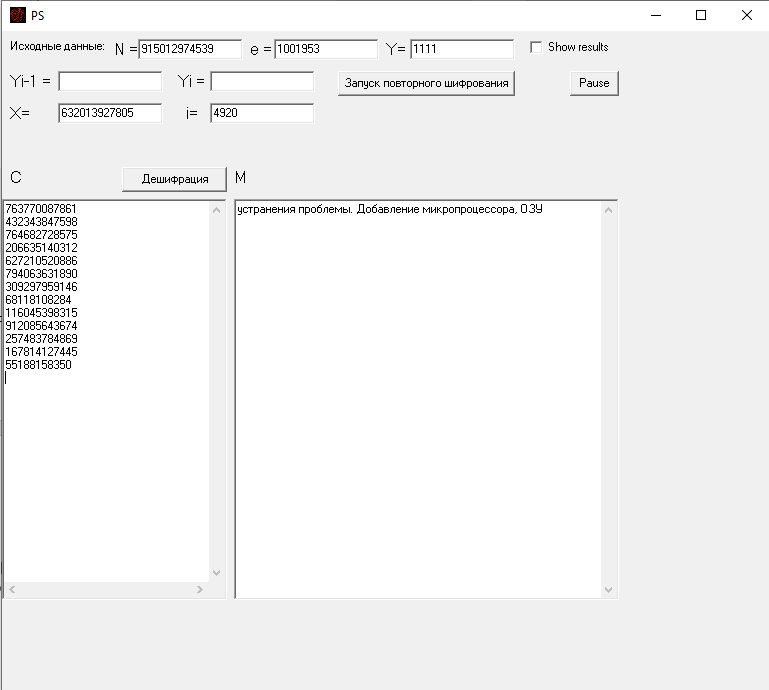
55188158350

Алгоритм выполнения

1. Определяем порядок экспоненты при помощи программы PS. Для этого значение модуля помещаем в поле N, экспоненты в поле e, в поле Y записывается произвольное число . В поле X появится значение, равное корню е степени от числа Y по модулю N, а в поле i – порядок e.
2. Дешифруем зашифрованный текст. В область редактирования поля C поместить блоки зашифрованного текста, значение модуля в поле N, экспоненты в поле e и порядка экспоненты в поле i. Получаем исходный текст в области редактирования M.

Выполнение работы





Исходный текст:

устранения проблемы. Добавление микропроцессора, ОЗУ

Выводы

В данной лабораторной работе я изучил атаку на алгоритм шифрования RSA посредством повторного шифрования.