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 22*

Студент

*Патутин В. М.*

*P33101*

Преподаватель

*Маркина Т. А.*

Санкт-Петербург, 2022 г.

Цель работы

Изучить атаку на алгоритм шифрования RSA посредством повторного шифрования.

Исходные данные:

*N =* 914022837691

*e =* 517823

*Блок текста C:*

133088999278

758078110965

705889026842

98403371042

768948684522

78137927374

383272719045

341665550116

407871370619

382219973835

653544166840

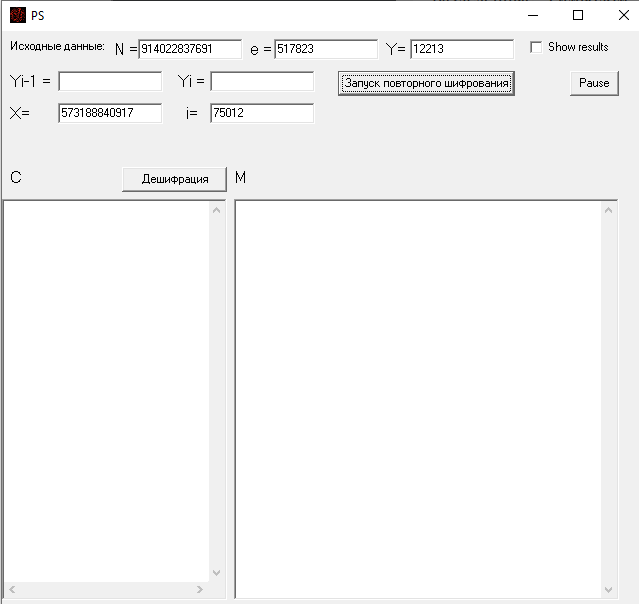
658599075370

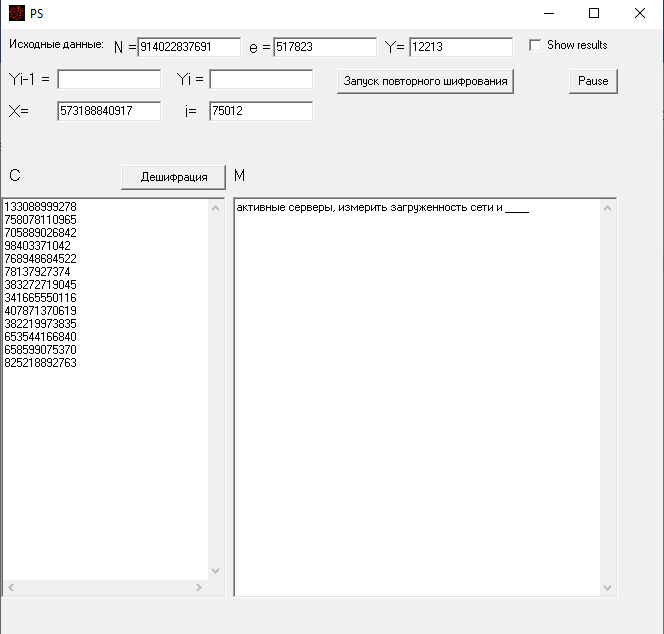
825218892763

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:

активные серверы, измерить загруженность сети и\_\_\_

Выводы

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