Федеральное государственное автономное образовательное учреждение высшего образования

Университет ИТМО

Дисциплина: Информационная безопасность (Криптография)

Лабораторная работа 2.2

Вариант 12

Работу выполнил студент группы P34111:
Кривоносов Егор Дмитриевич

Преподаватель:
Маркина Татьяна Анатольевна

2022 г.

г. Санкт-Петербург

Оглавление

Цель работы

Изучить атаку на алгоритм шифрования RSA посредством повторного шифрования.

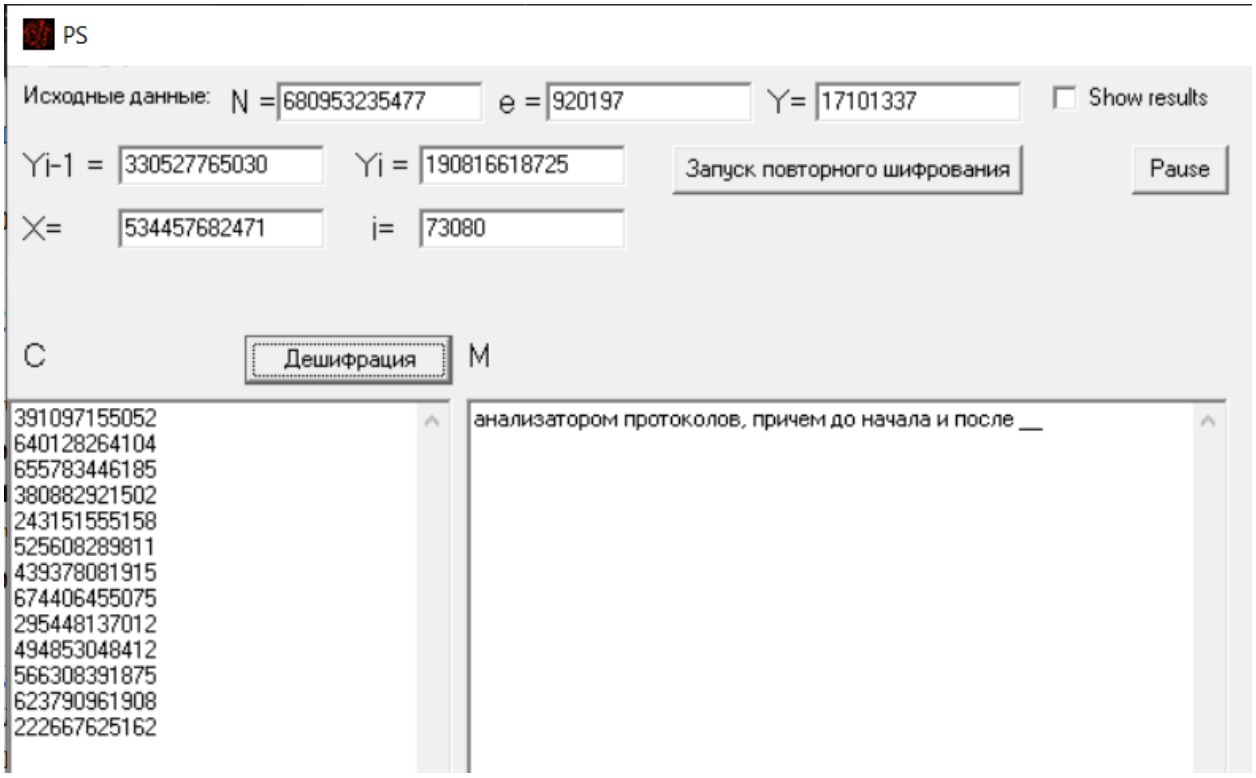
Задание

Вариант	Модуль, N	Экспонента, e	Блок зашифрованного текста, C
12	680953235477	920197	391097155052 640128264104 655783446185 380882921502 243151555158 525608289811 439378081915 674406455075 295448137012 494853048412 566308391875 623790961908 222667625162

Ход работы

1. Исходные данные заносятся в соответствующие поля ввода.
   Произвольное число Y = 17101337 (меньше чем заданное N)
2. После запуска повторного шифрования получены числа X = 534457682471 и i = 73080, где X - корень e степени от числа Y по модулю N, а i - порядок e.
3. В область C помещается блок зашифрованного текста и производится дешифрация

Скриншот работы программы PS.exe



Полученный результат: “анализатором протоколов, причем до начала и после __”

Вывод

В ходе выполнения данной лабораторной работы я ознакомился с методом повторного шифрования для атаки на алгоритм шифрования RSA.

$$y_1 = y$$

$$y_i = y_{y-1}^{\ e} \ mod \ N$$

$$y = x^e \ mod \ N$$