ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

Факультет Программной Инженерии и Компьютерной Техники

Дисциплина:
«*Информационная безопасность*»
(Криптографические системы с открытым ключом)

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №2
«Атака на алгоритм шифрования RSA методом повторного шифрования»

Вариант 9

Выполнил:
Студент гр. P34151
Соловьев Артемий Александрович

Преподаватель:
Маркина Татьяна Анатольевна

Санкт-Петербург
2024г.

Цель работы

Изучить атаку на алгоритм шифрования RSA посредством повторного шифрования.

Задание

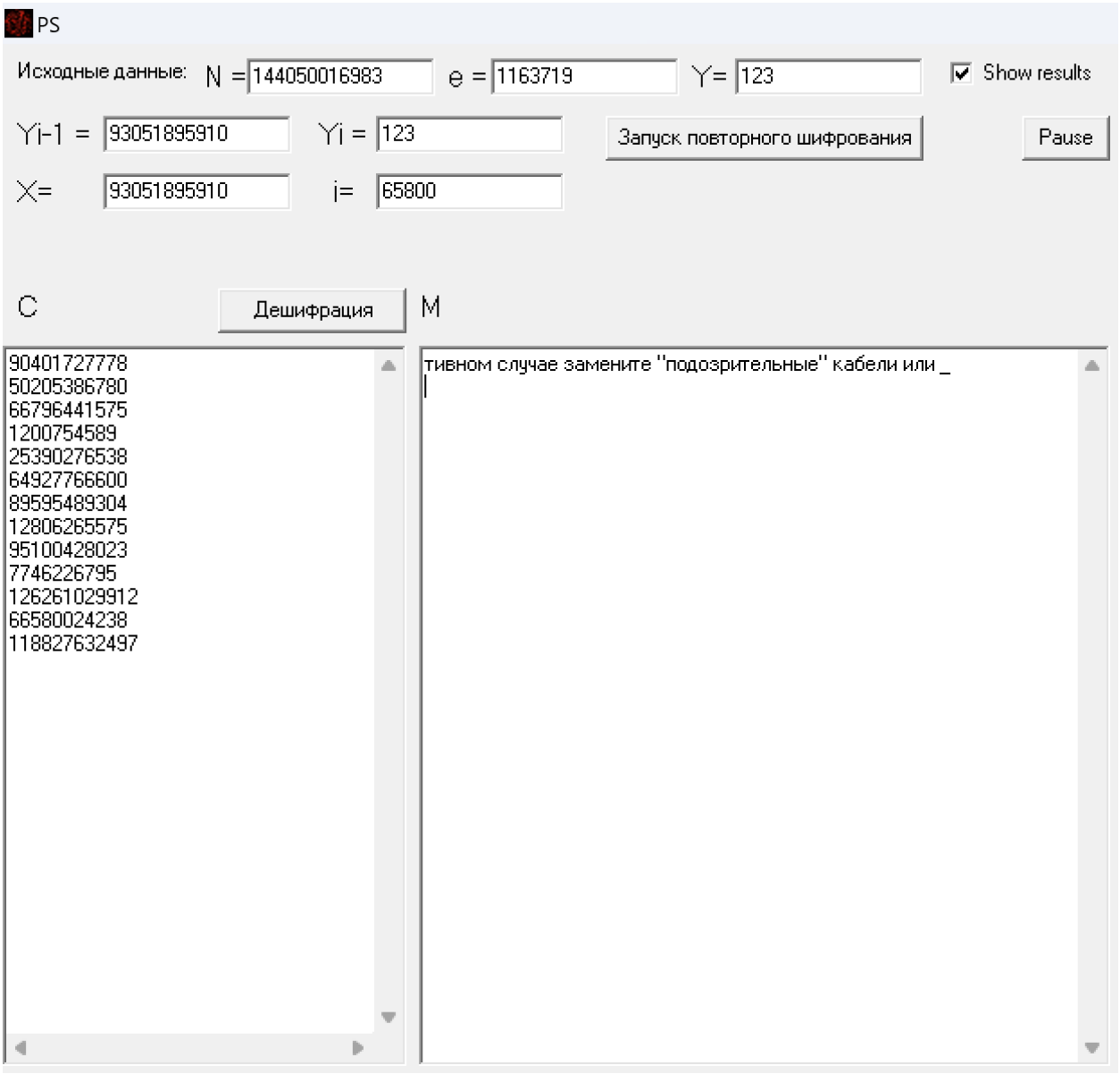
- по полученным исходным данным, используя метод перешифрования, определите порядок числа e в конечном поле ($Z_{\phi(N)}$
- используя значение порядка экспоненты, получите исходный текст методом перешифрования;
- результаты и промежуточные вычисления оформите в виде отчета.

По варианту:

Вариант	Модуль, N	Экспонента, e	Блок зашифрованного текста, C
9	144050016983	1163719	90401727778 50205386780 66796441575 1200754589 25390276538 64927766600 89595489304 12806265575 95100428023 7746226795 126261029912 66580024238 118827632497

Ход работы

1) Числа N и e заносятся в соответствующие поля ввода. В поле Y заносится произвольное число, в моем случае 123
2) После запуска повторного шифрования получены числа X=93051895910 и I = 65800
3) В поле C заносятся блоки зашифрованного текста
4) Расшифрованный текст «тивном случае замените «подозрительные» кабели или _»



Вывод

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