Отчет по лабораторной работе
“Атака на алгоритм шифрования RSA методом повторного шифрования”
по дисциплине
“Информационная безопасность”

Вариант 4

Выполнил:
студент группы P34131
Бусыгин Дмитрий Алексеевич
Преподаватель:
Маркина Татьяна Анатольевна

Санкт-Петербург
2024

Цель работы

Изучить атаку на алгоритм шифрования RSA посредством повторного шифрования..

Вариант

№	Модуль, N	Экспонента, e	Блок зашифрованного текста, C
4	489740760623	892627	237434928568 89382477865 257542914775 153947910848 219678068406 166466311168 49516725114 55375254449 370796045103 322927050068 196366079994 39243100230 299525662956

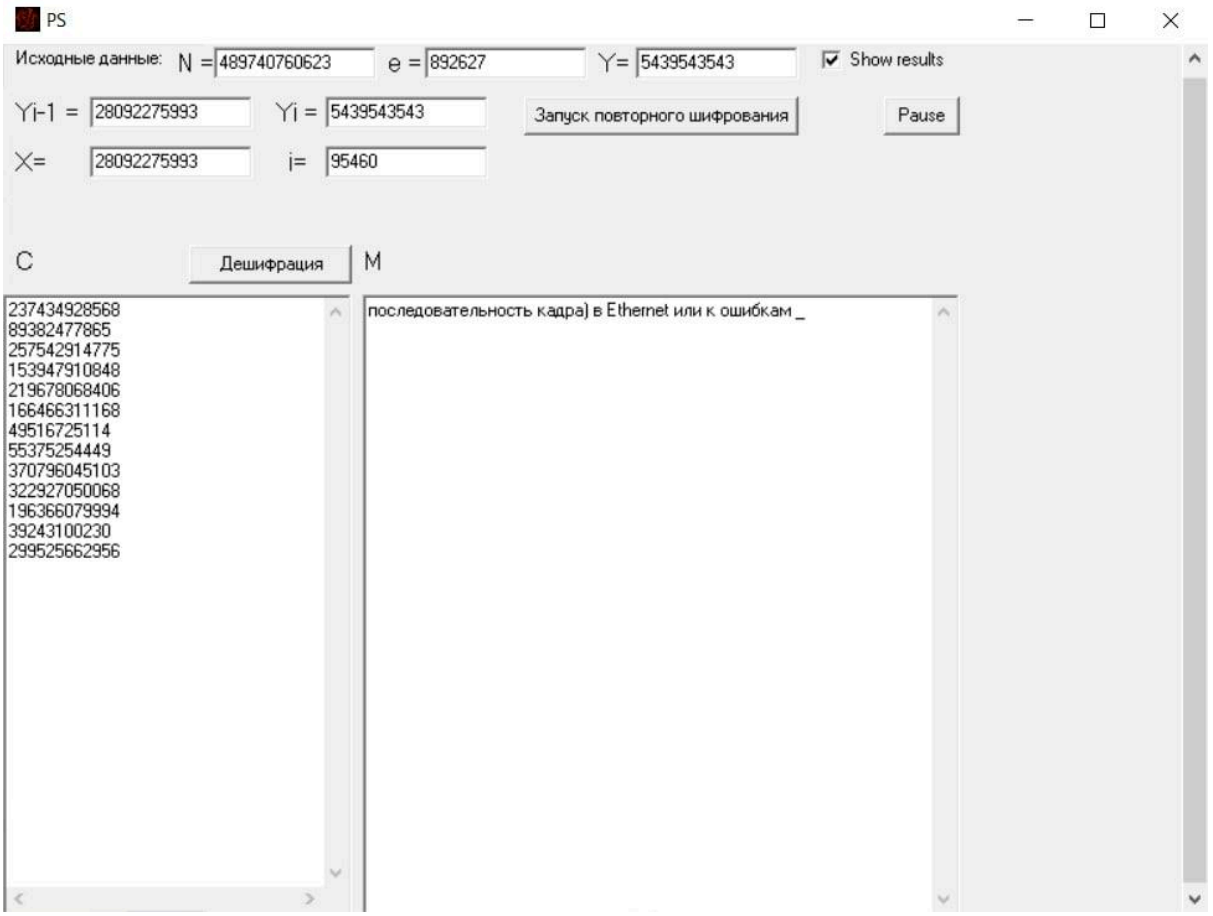
Выполнение в программе PS.exe

1. Определяем порядок экспоненты. Для этого необходимо ввести значение модуля в поле N = 489740760623, экспоненты в поле e = 892627, в поле Y записывается произвольное число, меньше чем N, возьмем 5439543543. После этого запустим повторное шифрование и дождемся, пока в поле X появится значение, равное корню e степени от числа Y по модулю N, а в поле i – порядок e в конечном поле $Z_{\varphi(N)}$. В предоставленном варианте он составляет 95460.
2. Дешифруем зашифрованный текст. Помещаем блоки зашифрованного текста, разделенные символом конца строки, значение модуля в поле N, экспоненты в поле e и порядка экспоненты в поле i. Затем нажать на кнопку Дешифрация и дождаться появления исходного текста в области редактирования M.

Полученное сообщение: ***последовательность кадра) в Ethernet или к ошибкам_***

Результат работы программы PS.exe

Исходные данные и расчет


PS
Исходные данные: N = 489740760623
e = 892627
Y= 5439543543
Show results
Yi-1 = 28092275993
Yi = 5439543543
Запуск повторного шифрования
Pause
X= 28092275993
i= 95460
C
Дешифрация
M
237434928568
89382477865
257542914775
153947910848
219678068406
166466311168
49516725114
55375254449
370796045103
322927050068
196366079994
39243100230
299525662956
последовательность кадра) в Ethernet или к ошибкам _