УНИВЕРСИТЕТ ИТМО

Факультет программной инженерии и компьютерной техники

Направление подготовки 09.03.04 Программная инженерия

Дисциплина «Информационная безопасность»

**Лабораторная работа №2.1**

Атака на алгоритм шифрования RSA посредством метода Ферма

*Вариант 20*

Студент

*Митрофанов Е. Ю.*

*P33101*

Преподаватель

*Маркина Т. А.*

Санкт-Петербург, 2022 г.

Цель работы

Изучить атаку на алгоритм шифрования RSA посредством метода Ферма.

Исходные данные

*N = 55925060669503*

*e = 4156793*

*Блок текста C:*

*53145801111837*

*24757475715890*

*19729078348176*

*49091835965654*

*29986321429979*

*35162644705488*

*45317135042859*

*49645513101014*

*1804825908594*

*35789821714579*

*3713734911002*

*23648998987066*

Выполнение работы

1. Вычисляем n = [sqrt(N)] + 1.
   1. Видим сообщение “[error]”, которое значит, что N - не квадрат целого числа.
2. Вычисляем t1 = n + 1 и далее d1 = t1^2 – N.
3. Проверяем, является ли d1 квадратом целого числа аналогично первому шагу.
   1. Снова видим сообщение “[error]”
4. Вычисляем t2 = t1 + 1 и d2 аналогично шагу 2.
5. Повторяем вычисления пока не дойдем до квадрата целого числа, т. е. пока не перестанем видеть сообщение “[error]”
6. Дойдя до d5 не получаем сообщения об ошибке.
7. Вычисляем квадратный корень из d5.
8. Вычисляем p = t5 + sqrt(d5).
9. Вычисляем q = t5 – sqrt(d5).
10. Вычисляем Phi(N) = (p – 1)(q – 1).
11. Вычисляем d, как обратный к e: d = e^(-1) mod Phi(N).
12. Построчно выполняем дешифрацию текста. На каждую строку блока C вычисляем M= C^d mod N5.
13. Переводим каждое число в текстовый вид

Изображение выглядит как стол

Автоматически созданное описание

Изображение выглядит как стол

Автоматически созданное описание

Полученный результат:

*зования протокола TCP: фрагментация на уровне IP*

Выводы

При выполнении лабораторной работы я изучил метод Ферма для атаки на алгоритм шифрования RSA