       Министерство науки и высшего образования Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

“НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО”

Факультет Программной инженерии и компьютерной техники



Отчет

По лабораторной работе № 3

Атака на алгоритм шифрования RSA методом бесключевого чтения

По предмету:  Информационная безопасность

Вариант 1

Студент:

Андрейченко Леонид Вадимович

Группа P34301

Преподаватель:

Маркина Татьяна Анатольевна

Санкт-Петербург

2023

Цель работы

Изучить атаку на алгоритм шифрования RSA посредством метода бесключевого чтения.

Выполнение

Исходные данные:

* Модуль N = 420882327013
* Экспонента e1 = 1372369
* Экспонента e2 = 961447
* Блок зашифрованного текста С1 = 373413138774 ...
* Блок зашифрованного текста С2 = 105783140624 ...

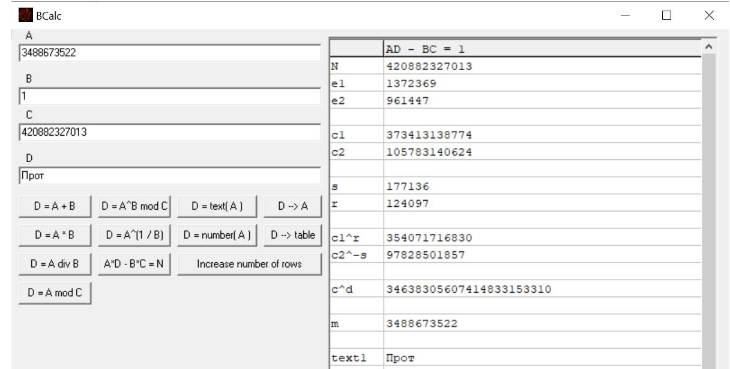
Решаем уравнение e1\*r – e2\*s = ±1, результаты r = 124097 s = 177136

Производим дешифрацию m1 = c1^r mod(N) = 354071716830, m2 = c2^-s mod(N) = 97828501857

Итоговое блок сообщения m = m1\*m2 mod(N) =3488673522, переводя в текст: "Прот"

Исходный текст: "Протоколы определяют синтаксис-семантику данных."

Листинг программы



Выводы

Атака основывается на слабостях или ошибках в генерации случайных чисел или выборе открытой экспоненты (e). Если атакующий обнаруживает, что экспонента e является маленьким и он может найти обратное число по модулю n и использовать его для расшифровки сообщений без доступа к приватному ключу.