       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 № 4

Атака на алгоритм шифрования RSA, основанная на Китайской теореме об остатках

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 Китайской теоремы об остатках.

Выполнение

Исходные данные:

* Модуль N1 = 359690807803
* Модуль N2 = 361062169537
* Модуль N3 = 363514381513
* Экспонента e = 3
* Блок зашифрованного текста С1 = 177412278620 ...
* Блок зашифрованного текста С2 = 227891126441 ...
* Блок зашифрованного текста С3 = 230974691188 ...

M0 = N1\*N2\*N3 = 47209882973814679636420365630460243;

m1 = N2\*N3 = 131251291246984504569481;

m2 = N1\*N3 = 130752781534418899345939;

m3 = N1\*N2 = 129870743427867268497211;

n1 = m1^ (–1) mod N1 = 299250018305;

n2 = m2^ (–1) mod N2 = 4817391352;

n3 = m3^ (–1) mod N3 = 56233175801;

Sum = c1\*n1\*m1 + c2\*n2\*m2 + c3\*n3\*m3 = 8798577572183112135137768687985034298289358016

S mod M0 = 42460097516027074294677432648

M = (S mod M0)^(1/e) = 3488673522

text = "Прот"

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

Листинг программы

