**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

***Изображение выглядит как черный, темнота

Автоматически созданное описание***

**Факультет Программной Инженерии и Компьютерной Техники**

**Дисциплина:**

**«*Информационная безопасность*»**

**(Криптографические системы с открытым ключом)**

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №4  
«Атака на алгоритм шифрования RSA, основанная   
на Китайской теореме об остатках»**

*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 Китайской теоремы об остатках.

# Задание

* Используя Китайскую теорему об остатках, получите исходный текст;
* Результаты и промежуточные вычисления значений для любых трех блоков шифрованного текста оформите в виде отчета.

Для всех вариантов экспонента

По варианту:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Вариант | Модуль, N | | | Блок зашифрованного текста | | |
|  |  |  |  |  |  |
| 9 | 441716293693 | 442258294987 | 444399387571 | 324500796659  324547036186  367901833181  38558700097  401956144715  260421328704  356041474179  113539876955  304515179769  302662240842  282367185538  432213853716 | 364411844182  137247785047  389030356498  293766643714  259139396276  429702138150  17968702271  84037113464  91988591941  425057692992  391906969363  244207991747 | 57065247639  130359065508  391859459727  128196485994  412050631244  367300386309  83703862830  218100297714  10243576841  232358719915  412546535924  398872645339 |

# Ход работы

1. Последовательно вычисляем параметры:
2. Вычисляем значение для блока зашифрованного текста
3. Вычисляем значение
4. Преобразуем результат в текст
5. Повторяем шаги 2–4 для каждой строки

|  |  |  |
| --- | --- | --- |
| № |  | Текст |
| 1 | 3488541683 | Полу |
| 2 | 4158714597 | чате |
| 3 | 3959169258 | ль к |
| 4 | 3773100256 | адра |
| 5 | 552595170 | пов |
| 6 | 4075745517 | торн |
| 7 | 3995132667 | о вы |
| 8 | 4159238635 | числ |
| 9 | 4293259808 | яет |
| 10 | 1129464608 | CRC |
| 11 | 3940607216 | кадр |
| 12 | 3760227630 | а… |

Расшифрованное сообщение: «Получатель кадра повторно вычисляет CRC кадра…»

# Скриншот работы программы

Изображение выглядит как текст, снимок экрана, число, Шрифт

Автоматически созданное описание

# Вывод

В ходе выполнения лабораторной работы я ознакомился с методом, основанным на китайской теореме об остатках, для атаки на RSA-шифрование.