**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 методом бесключевого чтения»**

*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 метода бесключевого чтения.

# Задание

* По полученным данным определить и при условии чтобы . Для этого необходимо использовать расширенный алгоритм Евклида
* Используя полученные выше значения и , записать исходный текст
* Результаты и промежуточные вычисления значений для любых трех блоков шифрованного текста оформить в виде отчета.

По варианту:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Вариант | Модуль, N | Экспоненты | | Блок зашифрованного текста | |
|  |  |  |  |  |  |
| 9 | 319418480417 | 602087 | 523639 | 52405618926  216147098445  216743861265  66972942908  191820297330  190353918873  110095200781  90183965366  296876615222  154988611456  166443759664  9906682687 | 82810335170  187684665216  48173641649  96024498047  247351492178  97241452868  255901558905  27364319220  227156630511  66990230889  183816391944  104719299259 |

# Ход работы

1. Решаем уравнение .  
   для этого в поле А помещаем значение в поле В помещаем значение .   
   После нажатия кнопки «A\*D - B\*C =N», ,
2. Производим дешифрацию: возводим в степень , а в степень по модулю .  
   ,
3. После находим , перемножив и .
4. Берем модуль от полученного значения N.   
   Получаем: 4075692116
5. Преобразуем в текст «то Т»
6. Повторяем алгоритм для остальных значений C

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| C1 | C2 |  | N | Дешифрованный текст |
| 216147098445 | 187684665216 | 789376507474379036874 | 1129328111 | CP-п |
| 216743861265 | 48173641649 | 46186359834117322773800 | 4042192613 | роце |
| 66972942908 | 96024498047 | 6593996776502725087836 | 4059111665 | сс с |
| 191820297330 | 247351492178 | 68344861019975852174962 | 3857769189 | ерве |
| 190353918873 | 97241452868 | 18705431686782645825328 | 4 041 220 335 | ра п |
| 110095200781 | 255901558905 | 84672521521213128220004 | 4007981794 | одтв |
| 90183965366 | 27364319220 | 12806336897216364665592 | 3857770212 | ержд |
| 296876615222 | 227156630511 | 3867232217645264903544 | 3773166112 | ает |
| 154988611456 | 66990230889 | 47657043272695217537540 | 686891247 | (с п |
| 166443759664 | 183816391944 | 4176899185647681268278 | 4008505081 | омощ |
| 9906682687 | 104719299259 | 2424145410141789995618 | 4244512800 | ью |

# Вывод

В ходе выполнения лабораторной работы я ознакомился с методом бесключевого чтения для атаки на RSA-шифрование.