Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Уфимский государственный нефтяной технический университет»

Кафедра вычислительной техники и инженерной кибернетики

Лабораторная работа №6

по дисциплине Информационная безопасность

Алгоритм шифрования RSA

Выполнил: студент гр. БПОи-16-01 К. И. Камалов

Проверил: кандидат технических наук, доцент Т.Х. Агишев

Уфа, 2019

## **ЗАДАНИЕ № 1**

**Атака на алгоритм шифрования RSA**

**посредством метода Ферма**

*Цель работы:* изучить атаку на алгоритм шифрования RSA посредством метода Ферма.

*Ход работы:*

– ознакомиться с теорией, («Взлом алгоритма RSA при неудачном выборе параметров криптосистемы»);

– используя разложение модуля на простые числа методом Ферма и полученные исходные данные, определить следующие показатели:

– множители модуля (*p* и *q*);

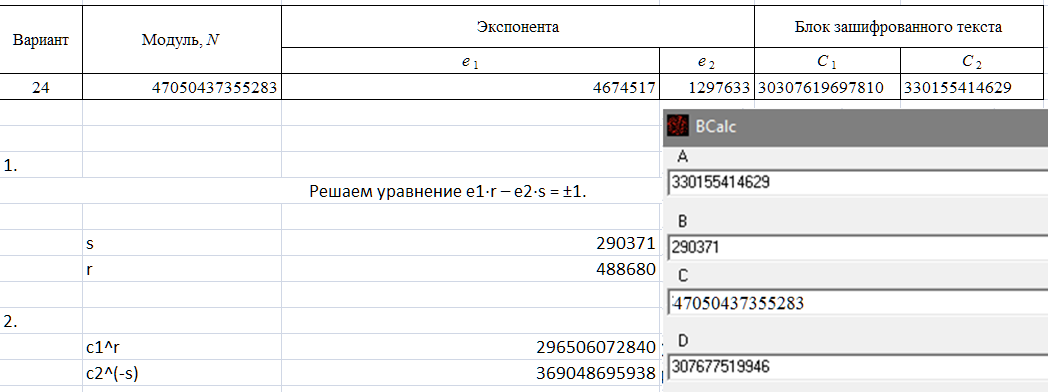
– значение функции Эйлера для данного модуля ;

– обратное значение экспоненты по модулю ;

– дешифровать зашифрованный текст, исходный текст должен быть фразой на русском языке;

– результаты и промежуточные вычисления оформить в виде отчета.

|  |  |  |  |
| --- | --- | --- | --- |
| 24 | 47050437355283 | 4674517 | 30307619697810  38075405389785  37116384337234  20795372941054  22354675528431  20104615399105  403582911849  16733578384925  37765786204941  16059974394842  10942482418438  39745386116422 |



## **ЗАДАНИЕ № 2**

**Атака на алгоритм шифрования RSA**

**методом повторного шифрования**

*Цель работы:* изучить атаку на алгоритм шифрования RSA посредством повторного шифрования.

*Ход работы:*

– ознакомиться с теорией, («Атака повторным шифрованием»);

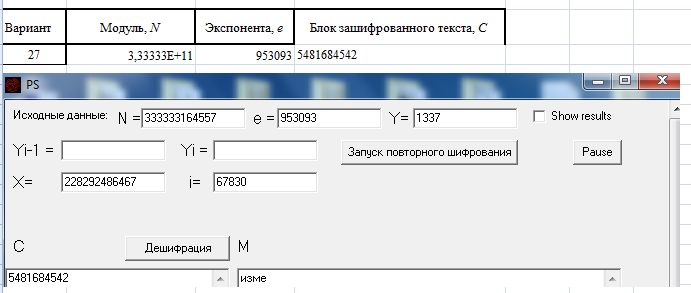
– по полученным исходным данным, используя метод перешифрования, определить порядок числа *e* в конечном поле ;

– используя значение порядка экспоненты, получить исходный текст методом перешифрования;

– результаты и промежуточные вычисления оформить в виде отчета.

**Атака повторным шифрованием**

Строим последовательность: . Итак, , а так как , то существует такое натуральное число m, что . Но тогда , отсюда следует, что , значит, *y*m-1 – решение сравнения .



## **ЗАДАНИЕ № 3**

**Атака на алгоритм шифрования RSA**

**методом бесключевого чтения**

*Цель работы*: изучить атаку на алгоритм шифрования RSA посредством метода бесключевого чтения.

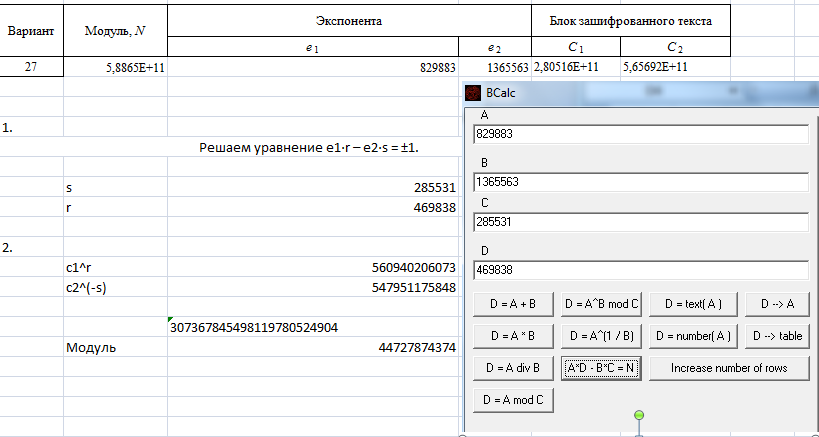
*Ход работы*:

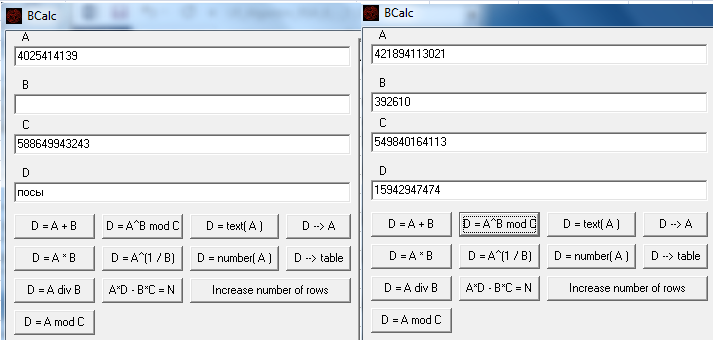
– ознакомиться с теорией, («Бесключевое чтение»);

– по полученным данным определить значения *r* и *s* при условии, чтобы *e*1∙*r – e*2∙*s* =1. Для этого необходимо использовать расширенный алгоритм Евклида;

– используя полученные выше значения *r* и *s*, записать исходный текст;

– результаты и промежуточные вычисления значений для любых трех блоков шифрованного текста оформить в виде отчета





**Бесключевое чтение**

Пусть два пользователя выбрали одинаковый модуль *N* и разные экспоненты *e*1 и *e*2. Если один пользователь посылает им некое цирку­лярное сообщение *x*, то криптоаналитик противника может получить в свое распоряжение два шифрованных текста  и  В таком случае криптоаналитик может получить исходное сообщение, используя расширенный алгоритм Евклида, находим  такие, что . Отсюда получаем: 