**МИНОБРНАУКИ РОССИИ**

**Санкт-Петербургский государственный**

**электротехнический университет**

**«ЛЭТИ» им. В.И. Ульянова (Ленина)**

**Кафедра Информатики**

отчет

**по лабораторной работе №4**

**по дисциплине «Защита информации в компьютерных сетях»**

Тема: Исследование криптографической системы RSA

|  |  |  |
| --- | --- | --- |
| Студент гр. 6373 |  | Солодов М.П. |
| Преподаватель |  | Копыльцов |

Санкт-Петербург

2018

**Цель работы:** Ознакомиться с классической криптосистемой с открытым ключом RSA и вариантами ее использования.

**Протокол.**

Задача 1. Общий ключ для двух пользователей. Выберите некоторое простое число p и число g – примитивный корень по модулю p. Примитивным корнем g по модулю p называется число, все степени которого g1,g2,…gn-1 различны. Придумайте некоторые произвольные числа k1 и k2 (ключи). Выполните на компьютере последовательность действий, обеспечивающих выработку общего ключа k для двух пользователей. Вручную проверьте правильность вычислений.

Решение. Пусть Тогда найдем .

Известно, что порождающий элемент (примитивный корень) числа , где , если показатель числа по модулю равен . При этом любой показатель числа по модулю делит . Значит, достаточно проверить, что для любого числа делителя выполняется: .

1) – не порождающий элемент.

2) – не порождающий элемент.

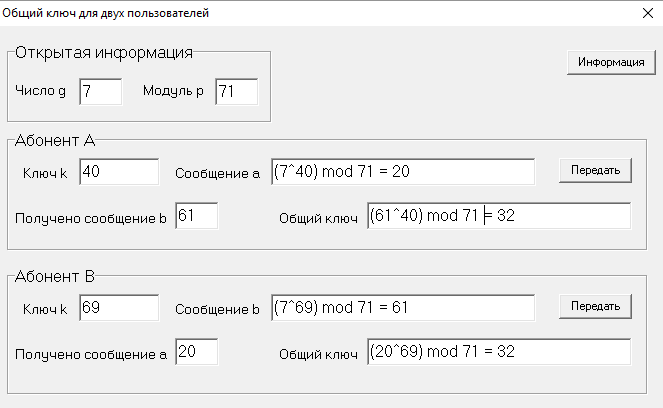
3) – аналогично.

4) 7 – порождающий элемент.

Итак,

Пусть .

Результат работы программы:

**

Проверим результаты вручную.

1.

2.

3.

4.

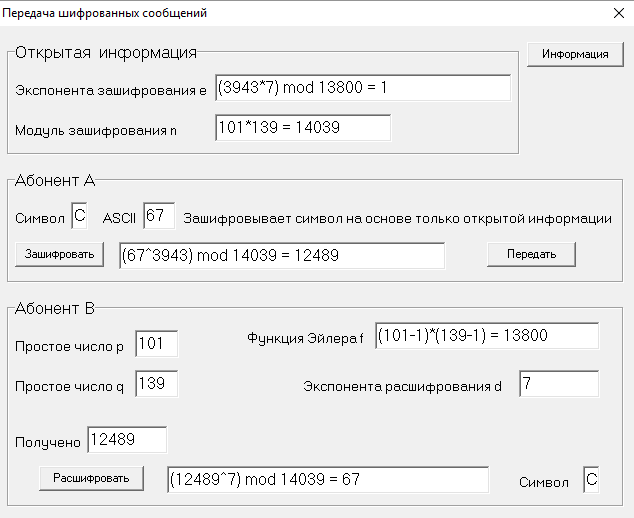
Задача 2. Передача шифрованных сообщений. Возьмите два простых числа p и q, найдите их произведение и функцию Эйлера выберите из условия . Введите эти данные в компьютер и посмотрите, какой закрытый ключ будет вычислен. Для абонента А, имеющего только открытую информацию введите некоторый символ и автоматически получите его ASCII-код. Нажмите кнопку «Зашифровать» и запишите полученное сообщение. Передайте это сообщение абоненту В, нажмите кнопку «Расшифровать» и убедитесь, что расшифрование выполнено правильно. При ошибках (Ваших) в выборе простых чисел и вычислении зашифрование будет невозможным. В этом случае проанализируйте свои ошибки.

Решение. Пусть

Функция Эйлера:

Найдем Пусть – экспонента расшифрования.

Результат работы программы:



Задача 3. Сообщение от клиентов банку. Представив себя банкиром B, выберите простые числа ; затем представив себя клиентами , выберите несколько пар простых чисел и , вычислите и за банкира и за клиентов значения функций Эйлера и все открытые ключи. Введите полученные данные в компьютер. Выберите номер клиента и некоторый символ и введите их в компьютер, автоматически получив ASCII-код. Зашифруйте его и передайте банку, получите протокол с этапами зашифрования и расшифрования. Проанализируйте этот протокол и запишите, какие действия выполняются согласно этому протоколу. Если результат положительный, то Вам будет предложено использовать сформированные Вами данные для посимвольной передачи неизвестного Вам сообщения от выбранного Вами клиента банку. Запишите полученное после расшифровки сообщение. Представив себя клиентом, выдающим банку себя за другого, воспользуйтесь открытой информацией и попытайтесь передать сообщение банку. Проанализируйте результат.

Решение. Составим таблицу простых чисел для Банкира и Клиентов, а также вычислим функцию Эйлера для каждого из них.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Вычислим экспоненту расшифрования

Занесем данные в таблицу.

Протокол шифрования:

Символ , код символа клиент номер

– шифрование клиентом сообщения своим секретным ключом .

– шифрование полученного на первом этапе сообщения открытой экспонентой дешифрования Банка по модулю Банка.

Протокол дешифрования:

– расшифровка полученного Банком сообщения собственным секретным ключом .

– расшифровка полученного на предыдущем этапе сообщения с помощью публичного ключа расшифрования и модуля клиента №2 соответственно.

Сообщение доставлено и расшифровано верно.