**Лабораторная работа 2. ТЕСТИРОВАНИЕ ПРОСТЫХ ЧИСЕЛ И НАХОЖДЕНИЕ КВАДРАТИЧНЫХ ВЫЧЕТОВ**

**Цель работы**

Закрепить знания, полученные на лекциях курса “Основы криптографии с открытым ключом“ по разделам: “Квадратичные вычеты” и “Генерирование и тестирование простых чисел”.

**Используемое программное обеспечение**

Для работы используется программа “Maxima” и дополнительные командные строки для решения каждой из задач.

1.Выполнить упражнения по нахождению доли простых чисел заданной разрядности и генерированию простых чисел при вероятностном тестировании.

2.Найти квадратичные вычеты по простому модулю и произвести вычисление квадратных корней из них.

**Задание 1.**

Для начала работы перейти в каталог, содержащий описание лабораторных работ и убедиться в установке пакета программ “Maxima”.

Прочитать описание лабораторной работы 3.

1.Перейти к пакету “Maxima”.

2.Рассчитать вероятность попадания на простое число при случайном генерировании чисел разрядности *l*=100, 300, 500 и 1000 при помощи следующей команды:

*l:…..;*

*lg(x) := log(x)/log(10);*

*EstimateProb:2\*(9\*l-10)/(9\*l\*(l-1)\*lg(10));*

Ввод команд осуществлять построчно. Для выполнения команд использовать комбинацию клавиш Ctrl+Enter. Вместо переменных предпочтительнее подставлять конкретные числовые значения, получаемые в ходе работы.

3.Для проверки теста Ферма сгенерировать необходимое количество случайных 3-х разрядных чисел при помощи команды:

*U:100+random(900);*

и отобрать среди них не менее 3 нечетных чисел *m*, среди которых должно быть одно простое число

Сгенерировать не менее 5 случайных 2-х разрядных чисел *a* при помощи команды:

*U:10+random(90);*

*U;*

Произвести проверку чисел *m* на простоту, используя тест Ферма при помощи команды:

*power\_mod(a,m-1,m);*

Сделать выводы о правильности (или нет) произведенного тестирования. Какова может быть вероятность ошибки в данном случае?

4.Произвести тестирования числа Кармайкла*m=561* по методу Ферма. Для этого сгенерировать необходимое количество случайных 2-х разрядных чисел по п. 3 и далее выбрать из них не менее 5 чисел *a’* взаимно простых с *561*, используя команды:

*gcd(a’,561);*

Проверить число *561,* используя тест Ферма по п. 3.

Сделать вывод о возможности использования данного теста для таких чисел.

5.Произвести тестирование на простоту одного из чисел *m,* сгенерированных в п.3 и число Кармайкла 561, по методу Миллера–Рабина при помощи команды:

*m:533;*

*f:0;*

*a:m-1;*

*u:random(m-2);*

*x:0;*

*while mod(a,2)=0 do (*

*f:f+1,*

*a:a/2);*

*printf(false,"a:~d,",a) ;*

*printf(false,"f:~d,",f) ;*

*x:power\_mod(u,a,m);*

*for i:0 step  1 thru f do (*

*printf(true,"i:~d, x: ~d;",i,x),*

*x:mod(x^2,m));*

Если программа выводит или одна из следующих степеней u равна “-1”, то m проходит тест на простоту и надо повторить данный тест не менее 5 раз. Если хотя бы в одном случае m не прошло тест, то оно составное.

Сравнить эффективность данного теста с тестом Ферма.

6.Найти несколько квадратичных вычетов *u<m* по *mod(m),*где *m*одно из простых 3-х разрядных чисел, полученных в п. 5, используя вычисление символа Якоби ( который для простых *m*совпадает с символом Лежандра) , при помощи следующей команды:

*u:…..;m:…;*

*jacobi(u,m)*

**Задание 2**

1. Распределите числа в поле GF(p) на вычеты и невычеты.

р=17 для нечетных вариантов и р=13 для четных вариантов.

1. Проверьте, является ли число а=(№вар+20)mod31 вычетом по модулю 17, 19.
2. Решите уравнение 
   1. р=23, а= 6 для вариантов 1-5, а=8 для вар 6-10, а=12 для вар с 11-15, а=18 для вар с 16-20, а=13 для вар 21-25.
   2. р=29, а= №вар+3 для вариантов 1-13 №вар-10 для вар >13.
3. Решите уравнение 
   1. Для n=3\*7, для вариантов 1-6, a=16
   2. Для n=3\*11, для вариантов 7-12, a=25
   3. Для n=7\*11, для вариантов 13-19, a=81
   4. Для n=11\*19, для вариантов 19 и более, a=218.

Примечания:

1.При выполнении п.4 сначала нужно найти решения уравнения по простым модулям (сомножителям n) см. п. 3, затем, используя китайскую терему о остатках, получить решение системы. Нужно решить 4 системы из двух уравнений)

2. Второй способ решения уравнения , когда p=4k+1- алгоритм Чипполы. ( первый см.в учебнике и в лекционных материалах)

- подбираем b пока , то есть b2-1 невычет,

- искомый корень находим из уравнения 

Все действия при возведении в степень выполнять по modр.

**Отчет**

1.Титульный лист.

2.Исходные данные и результаты вычислений по всем 7 пунктам порядка выполнения работы.

3.Выводы о возможности (или нет) быстрого тестирования многоразрядных простых чисел, а также быстрого нахождения квадратичных вычетов по простому модулю и вычисления для них квадратных корней.

**Контрольные вопросы**

1.Какова доля простых чисел среди всех чисел заданной разрядности?

2.На какой теореме теории чисел основан тест Ферма?

Каковы его преимущества и недостатки перед другими тестами?

3.Каковы основные преимущества и недостатки теста Миллера-Рабина?

4.Что такое квадратичные вычеты и невычеты по заданному модулю и как они могут быть найдены?

5.В каких случаях нахождение квадратных корней по заданному модулю является простой (полиномиальной) задачей, а в каких - ее простое решение не известно?