ЛАБОРАТОРНАЯ РАБОТА № 5

ГЕНЕРАЦИЯ ПРОСТЫХ ЧИСЕЛ, ИСПОЛЬЗУЕМЫХ В АСИММЕТРИЧНЫХ СИСТЕМАХ ШИФРОВАНИЯ

Цель работы: изучение методов генерации простых чисел, используемых в системах шифрования с открытым ключом.

Описание лабораторной работы. Для выполнения лабораторной работы необходимо запустить программу **L_PROST.exe**. На экране дисплея появляется окно с текстовым редактором (для отображения информации об осуществленных программой действиях), в верхней строке окна расположено главное меню, чуть ниже основного меню — панель инструментов (для управления быстрыми командными кнопками и другими «горячими» элементами управления), а в самом низу окна, под тестовым редактором, находится строка состояния, в которой указывается подсказка и выводится дополнительная информация. Клавиши панели инструментов для удобства снабжены всплывающими подсказками.

Для того чтобы попасть в основное меню, необходимо нажать клавишу F10. Передвижение по главному меню осуществляется клавишами перемещения курсора. Чтобы вызвать пункт меню, нужно нажать клавишу ENTER, ESC — выход из основного меню.

Для удобства в программе предусмотрена работа с мышью. В этом случае указатель подводится к нужному пункту главного меню или к нужной кнопке на панели инструментов и нажимается левая клавиша мыши, для отказа достаточно нажать клавишу ESC.

Кроме основных функций главного меню (Генерация простого *P*, Поиск в интервале, Проверка на простоту и т.д.) панель инструментов содержит клавишу, при нажатии которой выводится информация о программе.

Генерация простого P. Возможность генерации простого числа; количество разрядов генерируемого числа задается пользователем (от 1 до 5).

Поиск в интервале. Возможность поиска простых чисел в заданном интервале. Пользователем задается начало интервала — значение x, длина интервала — значение L. Поиск будет осуществляться в интервале $(x, x + L)$.

При проверке на простоту каждого числа интервала сначала выполняется тест пробных делений на первые по порядку простые числа, а затем проверка по тесту Ферма. Для задания способов проверки на простоту необходимо левой клавишей мыши отметить флажок

рядом с названием нужного метода, а затем указать все необходимые данные для начала поиска.

В методе пробных делений исходными данными является количество первых простых чисел для деления, а в тесте Ферма надо указать количество оснований и их значения.

По окончании расчета на экран выводятся найденные простые числа и их количество. Полную картину результатов работы можно просмотреть в пункте меню Вывод результатов.

Проверка на простоту. Возможность проверки на простоту любого числа. Необходимо ввести число и параметры расчета аналогично поиску в интервале.

Вывод результатов. Возможность просмотра всех результатов последней обработки. При входе в программу, когда никаких расчетов еще не производилось, предоставляется возможность просмотра исходного файла первых простых чисел, используемых для теста пробных делений.

Дополнительные сведения о программе

1. При запуске утилит генерации простого числа, поиска в интервале и проверки на простоту у пользователя запрашивается подтверждение на правильность выбранного метода для работы.
2. Во время работы длительных по исполнению процедур запускается прогресс процесса и гасится окно текстового редактора. По полоске прогресса можно наблюдать и оценивать примерную скорость работы алгоритма и время окончания текущего процесса.
3. Будьте внимательны при установке параметров работы, так как в процессе вычисления по ходу работы эти параметры изменить уже не удастся.
4. Описание «горячих» клавиш:
   Ctrl+F1 — генерация простого P;
   Ctrl+F2 — поиск в интервале;
   Ctrl+F3 — проверка на простоту;
   Ctrl+F4 — вывод результатов;
   Ctrl+X — выход из программы.
5. В лабораторной работе из-за большого времени счета рекомендуется использовать числа не более пяти разрядов и длину интервала выбирать не более 500, количество оснований для теста Ферма — не более 5.
6. Для правильного функционирования программы в рабочей директории (вместе с файлом **l_prost.exe**) обязательно должны находиться файлы **prost.txt** и **work.txt**. Не рекомендуется вносить какие-либо изменения в эти текстовые файлы, иначе последствия могут быть непредсказуемые.

Задание

1. Проверить на простоту два произвольных целых числа разрядностью не менее 5.
2. Распределение простых чисел.
   2.1. Задан интервал вида $[x, x + L]$. Вычислить количество $\Pi(x, L)$ простых чисел в интервале и сравнить с величиной $L/\ln(x)$. При каких условиях $\Pi(x, L)/L$ близко к $1/\ln(x)$ при заданных $x = 2000$, $L = 500$, количество простых чисел для деления 5—15, количество оснований 1—2?
   2.2. Найти в интервале (1000, 1000 + 300) все простые числа. Пусть $L(i)$ — разность между двумя соседними простыми числами. Построить гистограмму для $L(i)$. Вычислить выборочное среднее $L_{\text{сред.}}$. Сравнить с величиной $\ln(x)$, где x — середина интервала. Задано: количество простых чисел для деления 5—20, количество оснований 1—3.
   2.3. Для заданного набора чисел $\{k\}$ оценить относительную погрешность формулы для k-го простого числа:
   $p(k) = k/\ln(k)$, $k = \{10, 15, 20, 30, 35\}$.
3. Методы генерации простых чисел.
   3.1. В интервале (500, 500 + 200) построить график относительного количества натуральных чисел, проходящих «решето Эратосфена», т.е. не делящихся на первые k простых.
   Расчет производится для всех $k <= 10$.
   3.2. Для интервала (1500, 1500 + 300):
   а) рассчитать точное количество P_0 простых чисел в интервале, т.е. при проверке задать только тест на делимость. Количество первых простых чисел для деления определяется из расчета максимальное число для деления равно квадратному корню из максимального значения интервала;
   б) составить тест с небольшим количеством пробных делений и одним основанием в тесте Ферма. Вычислить количество P_1 вероятно простых чисел, удовлетворяющих этому тесту;
   в) составить тест с бóльшим, чем в предыдущем случае, количеством пробных делений и двумя или тремя основания-

ми в тесте Ферма. Вычислить количество P_2 вероятно простых чисел, удовлетворяющих этому тесту.
Проанализировать полученные данные.

3.3. Известно, что в заданном интервале имеются числа Кармайкла. Найти их.
Варианты интервалов: (1050, 1050 + 100);
(1700, 1700 + 100);
(2400, 2400 + 100).

4. Привести в отчете ответы на контрольные вопросы в соответствии с номером варианта (табл. 2.1).

Таблица 2.1

Номер варианта	Контрольные вопросы
1, 5, 7, 3, 9, 18, 28	Почему в качестве первого основания в тестах типа теста Ферма для проверки на простоту очень больших чисел целесообразно использовать число 2?
2, 4, 6, 8, 20, 22, 24, 26, 30	Какова вероятность $P(x)$ того, что наугад взятое нечетное очень большое число, не превосходящее x, окажется простым?
11, 13, 15, 10, 17, 19, 27	Вычислить: 1812 (mod 13), 127 (mod 7)
12, 14, 16, 21, 23, 25, 29	Сформулируйте суть теста на простоту с использованием пробных делений