Теория псевдослучайных генераторов. Практическая работа

Практическая работа состоит из двух заданий. В каждом задании необходимо на языке программирования реализовать несколько алгоритмов. Результатом выполнения каждого из заданий должна быть исполняемая программа, не требующая установки специального программного обеспечения для запуска. Программа должна иметь возможность запуска с параметрами без выполнения пользователем дополнительных действий – ответов на вопросы программы, нажатий кнопок, переключения флажков, выбора пути выгрузки и т.п.

Итогом практической работы является отчет. Отчет должен состоять из двух разделов, - по разделу на задание. Каждый раздел должен содержать описание задачи, описание алгоритма(-ов), описание условий запуска/работы программы, исходный текст программы.

Задание 1. Генератор псевдослучайных чисел.

Создайте программу для генерации псевдослучайных величин следующими алгоритмами:

a. Линейный конгруэнтный метод;
b. Аддитивный метод;
c. Пятипараметрический метод;
d. Регистр сдвига с обратной связью (РСЛОС);
e. Нелинейная комбинация РСЛОС;
f. Вихрь Мерсенна;
g. RC4;
h. ГПСЧ на основе RSA;
i. Алгоритм Блюма-Блюма-Шуба;

Название программы: **prng.exe**

На входе

Для управления приложением предлагается следующий формат параметров командной строки:

/g:<код_метода> - параметр указывает на метод генерации ПСЧ, при этом код_метода может быть одним из следующих:

- lc – линейный конгруэнтный метод;
- add – аддитивный метод;
- 5p – пятипараметрический метод;
- lfsr – регистр сдвига с обратной связью (РСЛОС);
- nfsr – нелинейная комбинация РСЛОС;
- mt – вихрь Мерсенна;
- rc4 – RC4;
- rsa – ГПСЧ на основе RSA;
- bbs – алгоритм Блюма-Блюма-Шуба;

Элементы вектора параметров разделяются запятой. Порядок элементов вектора для каждого из методов описан в таблице 1.

Таблица 1. Порядок элементов вектора параметров

Метод	Описание параметров
lc	Модуль, множитель, приращение, начальное значение
add	Модуль, младший индекс, старший индекс, последовательность начальных значений
5p	p, q1, q2, q3, w (см. лекции п. 3.5.2), начальное значение
lfsr	Двоичное представление вектора коэффициентов, начальное значение регистра
nfsr	В алгоритме использовать три РСЛОС R1, R2, R3, скомбинированных функцией R1^R2+R2^R3+R3. Параметры – двоичное представление векторов коэффициентов для R1, R2, R3, w, x1, x2, x3. w – длина слова, x1, x2, x3 – десятичное представление начальных состояний регистров R1, R2, R3.
mt	Модуль, начальное значение x
rc4	256 начальных значений
rsa	Модуль n, число e, w, начальное значение x. e удовлетворяет условиям: 1 < e < (p-1)(q-1), НОД(e, (p-1)(q-1)) = 1, где p*q=n. x из интервала [1,n] w – длина слова.
bbs	Начальное значение x (взаимно простое с n). При генерации использовать параметры: p = 127, q = 131, n = p*q = 16637

/n:<длина> - количество генерируемых чисел. Если параметр не указан, - генерируется 10000 чисел.

/f:<полное_имя_файла> - полное имя файла, в который будут выводиться данные. Если параметр не указан, данные должны записываться в файл с именем rnd.dat.

/h – информация о допустимых параметрах командной строки программы.

Пример

Для того чтобы сгенерировать последовательность ПСЧ длиной 16000 линейным конгруэнтным методом и записать результат в файл rnd_lc.dat, программу нужно запустить следующим образом:

D:/>prng.exe /g:lc /f:rnd_cl.dat /n:16000

На выходе

Текстовый файл кодировки UTF-8 со случайными числами в десятичной системе исчисления. Тестовая последовательность должна содержать 10000 десятичных чисел из интервала [0,1023], разделенных запятой (без пробелов и других символов). Начальные значения из параметров также должны быть включены в результирующий файл.

Во время работы программа должна отображать информацию о состоянии процесса генерации на консоль.

Требования к реализации

Программа должна быть реализована на языке программирования C++, C# или python. Архитектура программа строится по модульному принципу.

Задание 2. Преобразование ПСЧ к заданному распределению.

Создать программу для преобразования последовательности ПСЧ в другую последовательность ПСЧ с заданным распределением:

a. Стандартное равномерное с заданным интервалом;
b. Треугольное распределение;
c. Общее экспоненциальное распределение;
d. Нормальное распределение;
e. Гамма распределение (для параметра *c*=*k*);
f. Логнормальное распределение;
g. Логистическое распределение;
h. Биномиальное распределение.

Название программы: **rnc.exe**

На входе

Текстовый файл с десятичными числами (разделитель – любой), интервал преобразуемых значений, параметры распределения.

Для управления приложением предлагается следующий формат параметров командной строки:

/f:<имя_файла> - имя файла с входной последовательностью.

/d:<распределение> - код распределения для преобразования последовательности. Рекомендуется использовать следующие коды распределений:

- st – стандартное равномерное с заданным интервалом;
- tr – треугольное распределение;
- ex – общее экспоненциальное распределение;
- nr – нормальное распределение;
- gm – гамма распределение;
- ln – логнормальное распределение;
- ls – логистическое распределение;
- bi – биномиальное распределение.

/p1:<параметр1> - 1-й параметр, необходимый, для генерации ПСЧ заданного распределения.

/p2:<параметр2> - 2-й параметр, необходимый, для генерации ПСЧ заданного распределения.

/p3:<параметр3> - 3-й параметр, необходимый, для генерации ПСЧ гамма-распределением.

На выходе

Текстовый файл distr-xx.dat с преобразованными числами, где <xx> – код распределения.

Список источников

1. Руководство пользователя к пакету NIST STS. Доступно: NIST STS Guide.
2. Средство для статистического анализа случайных последовательностей. Доступно: NIST STS Software.

Приложение 1. Титульный лист отчета

Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

ТЕОРИЯ ПСЕВДОСЛУЧАЙНЫХ ГЕНЕРАТОРОВ

ОТЧЕТ ПО ПРАКТИЧЕСКОМУ КУРСУ

студента X курса XXX группы

факультета компьютерных наук и информационных технологий

Иванова Ивана Ивановича

фамилия, имя, отчество

Научный руководитель

Ст. преподаватель _____ И.И. Слеповичев

подпись, дата

Саратов 2015

Приложение 2. Описание задания в отчете.

Задание 1. Генерация псевдослучайных чисел.

Описание задания: создать программу, генерирующую псевдослучайные числа из заданного диапазона. Входные параметры алгоритмы передаются программе через строку параметров (через файл с параметрами). Выходные значения записываются в файл, указанный в параметре запуска программы.

Алгоритм 1. Линейный конгруэнтный метод.

Описание алгоритма.

Параметры запуска программы.

Исходный текст программы.