ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Литвиченко В. М.

Стройникова Е. Д. – ассистент кафедры информатики

В строго детерминированном мире процессорных кодов внесение в программу элемента случайности – не такая простая задача, как может показаться на первый взгляд. Наиболее часто встречающиеся приложения, в которых необходимо использование случайных чисел - это численное моделирование методом Монте-Карло и создание компьютерных игр.

Для изучения генерации псевдослучайных чисел был выбран линейный конгруэнтный метод, разработанный Д.Г. Лехнером в 1949 году. Этот метод позволяет получать цепочки псевдослучайных чисел с периодом m. Основная формула для получения псевдослучайного числа выглядит следующим образом:

$$X_{n+1} = (a X_n + c) \bmod m, \qquad n \geq 0$$
$$0 < m$$
$$0 \leq a < m$$
$$0 \leq c < m$$
$$0 \leq X_n < m$$

Причем период равный числу m достигается только при соблюдении условий, которые описаны в теореме А. Теорема А:

• Линейная конгруэнтная последовательность, определенная числами m, a, c и X_0 , имеет период длиной m тогда и только тогда, когда:

- 1. Числа c и m взаимно простые;
- 2. b = a – 1 кратно p для каждого простого p, являющегося делителем m;
- 3. b кратно 4, если m кратно 4.

На основании вышеуказанного метода был разработан программный модуль генерации псевдослучайных чисел берущихся из диапазона, который задаётся пользователем. Для его создания была использованна среда Microsoft Visual Studio 2010 и язык программирования C++.

Стоит отметить что основным достоинством этого метода является простота его реализации, поэтому во многих языках программирования он идет как базовый для получения псевдослучайного числа.

Генератор псевдослучайных чисел построенный на базисе этого метода дает нам относительно неплохую псевдослучайность числа, хотя назвать его криптостойким нельзя.

Если требуется генератор псевдослучайных чисел с большим периодом и с лучшей распределённостью, то скорее всего это будет генератор псевдослучайных чисел построенный на базе алгоритма Вихрь Мерсена с периодом 2^m. Один из лучших алгоритмов по получению псевдослучайных чисел, но увы не обладающий достаточной криптостойкостью для приложений где она критична.

В этом случае используются алгоритм Шульба, дающий достаточную криптостойкость псевдослучайного числа, которая получается за счет слишком долгого вычисления числа с обратной стороны.

В результате выполенной работы были получены следующие псевдослучайные числа, которые брались из диапазона от 0 до 8, общим количеством 100:

0 3 5 4 2 8 6 3 3 8 0 0 0 8 0 6 0 0 0 1 0 1 8 8 3 6 7 8 6 1 8 8 2 7 3 6 4 0 5 2 1 4 7 2 2 2 2 6 3 8 3 7 2 1 4 0 1 4 1 7 6 6 4 3 6 1 3 1 5 4 2 0 3 3 6 0 8 4 6 6 1 5 2 3 1 4 0 0 0 1 4 6 7 6 8 5 2 0 7 0.

В дальнейшем планируется реализация генератора псевдослучайного числа на основе алгоритма Вихрь Мерсена и дальнейшее сравнение этого алгоритма с предыдущим.

Список используемых источников:

1. Д. Э. Кнут “Искусство программирования” том 2.