УДК 004.422.324

ГЕНЕРАТОРЫ СЛУЧАЙНЫХ ЧИСЕЛ

Д.Д. МОРОЗОВ
(Представлено: канд. физ.-мат. наук., доц. О.В. ГОЛУБЕВА)

Статья вводит понятия генератора случайных чисел и генератора псевдослучайных чисел. Здесь приведены их принципиальные различия и требования, которым они должны удовлетворять. Приведены примеры их использования, в том числе комбинированного.

Ключевые слова: *генератор псевдослучайных чисел, генератор случайных чисел.*

Генератор псевдослучайных чисел (ГСПЧ) – алгоритм, порождающий последовательность чисел, элементы которого почти независимы друг от друга и подчиняются заданному распределению (обычно равномерному). При этом от качества используемых ГСПЧ напрямую зависит качество получаемых результатов.

Наравне с существующей необходимостью генерировать легко воспроизводимые последовательности случайных чисел, также существует необходимость генерировать совершенно непредсказуемые или попросту абсолютно случайные числа. Такие генераторы называются **генераторами случайных чисел** (ГСЧ – англ. *random number generator, RNG*). Так как такие генераторы чаще всего применяются для генерации уникальных симметричных и асимметричных ключей для шифрования, они чаще всего строятся из комбинации криптостойкого ГПСЧ и внешнего источника энтропии (и именно такую комбинацию теперь и принято понимать под ГСЧ).

Простой ГСЧ с источником энтропии получится, если в качестве источника энтропии использовать текущее время, то для получения целого числа от 0 до N достаточно вычислить остаток от деления текущего времени в миллисекундах на число N+1. Недостатком этого ГСЧ является то, что в течение одной миллисекунды он выдает одно и то же число.

Источниками настоящих случайных чисел могут быть: физические шумы, такие, как детекторы событий ионизирующей радиации; дробовой шум в резисторе или космическое излучение. Устройства базирующиеся на таких источниках случайных чисел не находят большого применения в приложениях сетевой безопасности потому что имеют рад недостатков:

– время и трудозатраты при установке и настройке по сравнению с программными ГПСЧ;
– дороговизна;
– генерация случайных чисел происходит медленнее, чем при программной реализации ГПСЧ;
– невозможность воспроизведения ранее сгенерированной последовательности случайных чисел.

В то же время случайные числа, получаемые из физического источника, могут использоваться в качестве порождающего элемента для программных ГПСЧ. Такие комбинированные генераторы применяются в криптографии, лотереях, игровых автоматах.

Поэтому, качественные требования, предъявляемые к ГПСЧ:

– достаточно длинный период, гарантирующий отсутствие зацикливания последовательности в пределах решаемой задачи. длина периода должна быть математически доказана;
– эффективность – быстрота работы алгоритма и малые затраты памяти;
– воспроизводимость – возможность заново воспроизвести ранее сгенерированную последовательность чисел любое количество раз;
– портируемость – одинаковое функционирование на различном оборудовании и операционных системах.

Недостатком ГСПЧ является то, что никакой детерминированный алгоритм не может генерировать полностью случайные числа, он может только аппроксимировать некоторые их свойства. Любой ГПСЧ с ограниченными ресурсами рано или поздно зацикливается – начинает повторять одну и ту же последовательность чисел.

Длина циклов ГПСЧ зависит от самого генератора. Если порождаемая последовательность ГПСЧ сходится к слишком коротким циклам, то такой ГПСЧ становится предсказуемым и непригодным для практических приложений.

Большинство простых арифметических генераторов хотя и обладают большой скоростью, но страдают от многих серьезных недостатков:

– слишком короткий период/периоды.
– последовательные значения не являются независимыми.

– некоторые биты «менее случайны», чем другие.
– неравномерное одномерное распределение.
– обратимость.

В частности, алгоритм RANDU, десятилетиями использовавшийся на мейнфреймах, оказался очень плохим, что вызвало сомнения в достоверности результатов многих исследований, использовавших этот алгоритм.

Почти все крупные производители микрочипов поставляют аппаратные ГСЧ с различными источниками энтропии, используя различные методы для их очистки от неизбежной предсказуемости. Однако на данный момент скорость сбора случайных чисел всеми существующими микрочипами (несколько тысяч бит в секунду) не соответствует быстродействию современных процессоров.

В современных исследованиях осуществляются попытки использования измерения физических свойств объектов (например, температуры) или даже квантовых флуктуаций вакуума в качестве источника энтропии для ГСЧ.

В персональных компьютерах авторы программных ГСЧ используют гораздо более быстрые источники энтропии, такие, как шум звуковой карты или счетчик тактов процессора. Сбор энтропии являлся наиболее уязвимым местом ГСЧ. Эта проблема до сих пор полностью не разрешена во многих устройствах (например, смарт-картах), которые таким образом остаются уязвимыми. Многие ГСЧ используют традиционные испытанные, хотя и медленные, методы сбора энтропии вроде измерения реакции пользователя (движение мыши и т. п.), как, например, в PGP и Yarrow, или взаимодействия между потоками, как, например, в Java SecureRandom.

Криптографические приложения используют для генерации случайных чисел детерминированные алгоритмы, следовательно, генерируют последовательность чисел, которая теоретически не может быть статистически случайной. В то же время, если выбрать хороший алгоритм, полученная численная последовательность – **псевдослучайных чисел** – будет проходить большинство тестов на случайность. Одной из характеристик такой последовательности является большой период повторения.

ЛИТЕРАТУРА

1. Материал из Википедии – свободной энциклопедии. ГСПЧ [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/Генератор_псевдослучайных_чисел. – Дата доступа: 23.09.2019.
2. Материал из Википедии – свободной энциклопедии. ГПЧ [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/%D0%90%D0%BF%D0%BF%D0%B0%D1%80%D0%B0%D1%82%D0%BD%D1%8B%D0%B9_%D0%B3%D0%B5%D0%BD%D0%B5%D1%80%D0%B0%D1%82%D0%BE%D1%80_%D1%81%D0%BB%D1%83%D1%87%D0%B0%D0%B9%D0%BD%D1%8B%D1%85_%D1%87%D0%B8%D1%81%D0%B5%D0%BB. – Дата доступа: 23.09.2019.