ИССЛЕДОВАНИЕ МЕТОДОВ АВТОМАТИЧЕСКОЙ ГЕНЕРАЦИИ КРИПТОСТОЙКИХ СЛУЧАЙНЫХ ЧИСЕЛ

Е. И. Сорокин, Д. Н. Лясин

Волжский политехнический институт (филиал) ВолгГТУ

В связи с развитием информационных технологий особенную актуальность приобретают вопросы защиты информации от взлома. Современная информатика широко использует псевдослучайные числа в самых разных приложениях — от метода Монте-Карло и имитационного моделирования до криптографии. При этом от качества используемых ГСЧ напрямую зависит качество получаемых результатов.

Если генератор выдает числа, смещенные в какую-то часть интервала (одни числа выпадают чаще других), то результат решения задачи, решаемой статистическим методом, может оказаться неверным. Поэтому проблема использования хорошего генератора действительно случайных и действительно равномерно распределенных чисел стоит очень остро.

Цель работы: повышение эффективности автоматической генерации криптостойких случайных чисел.

Большинство простых арифметических генераторов хотя и обладают большой скоростью, но страдают от многих серьёзных недостатков: слишком короткий период/периоды, последовательные значения не являются независимыми, неравномерное одномерное распределение, обратимость.

Примером энтропии аппаратных ГСЧ могут служить: шум звуковой карты; частота тактов процессора; дампы памяти; аппаратурный генератор шума (ГШ), в качестве которого используют шумящее тепловое устройство, например, транзистор.

Анализ существующих программных продуктов показал, что генераторы криптостойких случайных чисел, использующие источники энтропии обладают серьёзным недостатками - медленный сбор энтропии, некоторые алгоритмы являются недостаточно криптостойкими, что делает их негодными для использования.

В результате проделанной работы разработанный алгоритм обладает необходимой криптостойкостью и сбор энтропии был заметно ускорен, при этом алгоритм проходит тесты стандарта FIPS 140-2, проверку на равномерность распределения и статическую независимость. Что позволяют алгоритму генерировать последовательности криптостойких чисел намного быстрее и эффективнее.

Список литературы:

1. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире (Secrets and Lies) // Методы. Алгоритмы. Программы. - 2006.