К. В. Захарченко

АППАРАТНАЯ РЕАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКИ СТОЙКОГО ГЕНЕРАТОРА СЛУЧАЙНЫХ ЧИСЕЛ

Генератор случайных чисел (ГСЧ) является неотъемлемой частью практически любой криптографической системы. Являясь звеном, влияющим на надёжность всей системы, генератор обязан удовлетворять ряду требований. Ошибки в проектировании ГСЧ могут привести к уязвимости всей системы. Поэтому проектирование криптографически стойкого генератора случайных чисел является важной частью построения защищённой криптографической системы.

Введение

Случайность можно определить как непредсказуемость значений данных для злоумышленника. Мера случайности называется энтропией. В данной работе был спроектирован ГСЧ, получающий биты энтропии из нескольких источников. Однако, недостаточно полагаться только на внешние источники энтропии. Спроектированный генератор случайных чисел основан на генераторе псевдослучайных чисел (ГПСЧ), который является основным источником последовательности случайных чисел.

I. Механизм работы ГСЧ

В данном проекте ГПСЧ использует источники энтропии для инициализации своего состояния, а так же для периодического «перемешивания» своего внутреннего состояния случайными данными, полученными с источников. Для этого используется механизм пула. ГПСЧ обеспечивает надёжную работу генератора в не зависимости от источников действительно случайных данных, а так же позволяет гарантированно генерировать равномерно распределённые случайные данные. На рисунке 1 изображена структурная схема генератора случайных чисел.

Рис. 1 – Структурная схема генератора случайных чисел

Для того, чтобы ГПСЧ при включении генератора не начинал свою работу каждый раз с одного состояния, в схему ГСЧ введено устройство постоянной памяти, в которое происходит сохранение состояния ГПСЧ. Также подключены часы реального времени, которые способствуют ГПСЧ генерировать различные последовательности при каждом новом старте системы.

II. Тестирование и моделирование системы.

Для тестирования качества последовательности случайных чисел, предоставляемых генератором, были использованы тесты Diehard, а так же статистические тесты NIST, объединённые в одном программном пакете DieHarder.
Для моделирования и тестирования генератора случайных чисел была использована среда схемотехнического моделирования Proteus. Сгенерированная последовательность сохранялась в файл, после чего проходила проверку статистическими тестами.

III. Выводы

Была спроектирована система, отвечающая всем требованиям, предъявляемым к криптографическому ГСЧ. Таким образом, система, надёжно обеспечивающая генерацию случайной последовательности, должна сочетать в себе как источники действительно случайных данных, так и программные алгоритмы, обеспечивающие безотказную работу системы при нарушении работы источников, а так же «выравнивающие» распределение случайных данных. Важно продумать работу системы при различных критических ситуациях, таких как преждевременное отключение питания и при возможности различных видов атак на систему.

1. Нильс Фергюсон, Брюс Шнайер. Практическая криптография = Practical Cryptography: Designing and Implementing Secure Cryptographic Systems. – М.: Диалектика, 2004. – 432 с.
2. Дональд Кнут Искусство программирования, том 2. Получисленные алгоритмы = The Art of Computer Programming, vol.2. Seminumerical Algorithms. – 3-е изд. – Москва: «Вильямс», 2007. – 832 с.
3. Н. Смарт Криптография. – Москва: Техносфера, 2005. – 528 с.

Захарченко Константин Владимирович, студент группы 021902 БГУИР, cvzakharchenko@gmail.com.

Научный руководитель: Курулёв Александр Петрович, профессор, кандидат технических наук.

Научный руководитель: Свито Игорь Леонтьевич, доцент, кандидат технических наук.