РАЗРАБОТКА ТРЕБОВАНИЙ К КРИПТОГРАФИЧЕСКИ СТОЙКОМУ ГЕНЕРАТОРУ ПСЕВДОСЛУЧАЙНОЙ ГАММЫ

Рысованый А.Н.
Национальний технический университет «Харьковский политехнический институт», г. Харьков

Основная проблема классической криптографии заключалась в трудности генерирования непредсказуемых двоичных последовательностей большой длины с применением короткого случайного ключа. Для ее решения широко используются генераторы двоичных псевдослучайных последовательностей.

В работе рассмотрены требования к криптографически стойкому генератору псевдослучайной последовательности. Получаемые программно из ключа, случайные или псевдослучайные ряды чисел иногда называются гаммой, по названию буквы греческого алфавита, которой в математических записях обозначаются случайные величины.

Первым требованием к криптографически стойкому генератору псевдослучайной последовательности или гаммы – период генерирования гаммы должен быть достаточно большим для шифрования сообщений различной длины. Сама гамма должна быть трудно предсказуемой. Это значит, что если известны тип генератора и часть гаммы, то невозможно предсказать следующую часть гаммы с вероятностью выше первоначальной.

Самая важная характеристика генератора псевдослучайных чисел – информационная длина периода. Эта длина фактически определяет возможное число ключей системы и зависит от алгоритма получения псевдослучайных чисел. Требуемую длину периода определяет степень секретности данных.

Вторым требованием можно считать непредсказуемость гаммы. Но пока еще нет универсальных и практически проверяемых критериев. Неизвестна и общая теория криптоанализа, которая могла бы быть применена для такого доказательства, за исключением все возрастающего количества конкретных способов анализа, выработанных для различных практических целей. Интуитивно случайность воспринимается как непредсказуемость. Чтобы гамма считалось случайной, как минимум, необходимо, чтобы ее период был очень большим, а различные комбинации бит определенной длины равномерно распределялись по всей ее длине. Итак, второе требование к ряду заключается в подтверждаемом статистическом подобии его свойств настоящей случайной выборке. Чем длиннее требуемая длина ряда, тем жестче к нему требования.

И, наконец, последнее третье требование связано с возможностью практической реализации генератора в виде программы или электронного устройства, быстродействием, необходимым для применения в современных коммуникациях, а также удобством его практического использования.