XXXII Неделя науки СПбГПУ. Материалы межвузовской научно-технической конференции. Ч.VI: С.41-43

СЕКЦИЯ «РАДИОЭЛЕКТРОННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»

УДК 621.319.019

А.В.Карабешкин (5 курс, каф. РЭСЗИ), Ю.В.Ветров, к.т.н., доц.

ИССЛЕДОВАНИЕ СТАТИСТИЧЕСКИХ СВОЙСТВ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ, ПРИМЕНЯЕМЫХ В СОВРЕМЕННЫХ КРИПТОАЛГОРИТМАХ

ABSTRACT: Developing an analysis of different methods generators construction of PR sequence used in modern crypt-algorithms. Particularly investigate generator of PR sequence in terms of algorithms LFSR and RC4.

Шифрование, как и дешифрация, осуществляется путем суммирования по модулю 2 исходных данных (в цифровом виде) и псевдослучайной последовательности, полученной с помощью ГПК (генератора псевдослучайного кода). Стойкость алгоритма к криптоанализу определяется секретностью ключа и свойствами генератора псевдослучайной последовательности символов.

Целью работы было исследование статистических свойств генераторов ПСП применяемых в современных криптоалгоритмах. Было исследовано два способа построения генераторов ПСП, причем оба из них находят применение в современной криптографии. Это генератор на основе регистра сдвига с обратными связями (LFSR) и генератор, реализованный в поточном криптоалгоритме RC4.

Шенноном было доказано, что подобная структура являет собой *абсолютно стойкий шифр*, когда: шифровочная последовательность является фрагментом истинно случайно последовательности, длины шифровочной и информационной последовательностей одинаковы и шифровочная последовательность используется один раз.

На практике такая схема оказывается слишком дорогой. Поэтому пытаются отойти от дорогих запросов абсолютной стойкости, однако, оставляя ее высокой. Главным отличием является использование генератора псевдослучайной последовательности, работающего в зависимости от сменной части шифра, а именно – ключа. Соответственно, основным критерием проверки данного генератора ПСП, является степень приближения его выходной ПСП к истинно случайной с равномерным законом распределения.

Одним из способов анализа получаемых с данного генератора псевдослучайных последовательностей является построение гистограмм. Были исследованы гистограммы для сравнения различных видов генераторов ПСП, а именно реализованный в среде Delphi датчик случайных чисел – random принимался за датчик истинно случайных (непредсказуемых) чисел.

Для гистограмм были построены доверительные интервалы, в которые с вероятностью 95% должны попасть результаты экспериментов. В нашем эксперименте в этот интервал попали все результаты.

Гистограммы дают лишь качественную, но не количественную оценку качества исследуемой ПСП. Поэтому для количественной оценки применим критерий хи-квадрат.

Для этого подсчитаем статистику. $y = \sum_{s=1}^{k} \frac{(Y_s - np_s)^2}{np_s}$ Очевидно, что с ростом количества испытаний величина **y** может изменяться. Проследим за изменениями этой статистики при различном количестве испытаний. Сразу же сделаем конкретные

вычислительные предпосылки. Выдвинем гипотезу о том, исследуемая ПСП имеет равномерный закон распределения. Тогда по критерию хи-квадрат подсчитаем границу принятия решения в пользу этой гипотезы в зависимости от величины статистики **y.** Граница составила – 78,4. (с вероятностью 90%). На рисунках 1,2 представлены зависимости статистики хи-квадрат от количества испытаний.

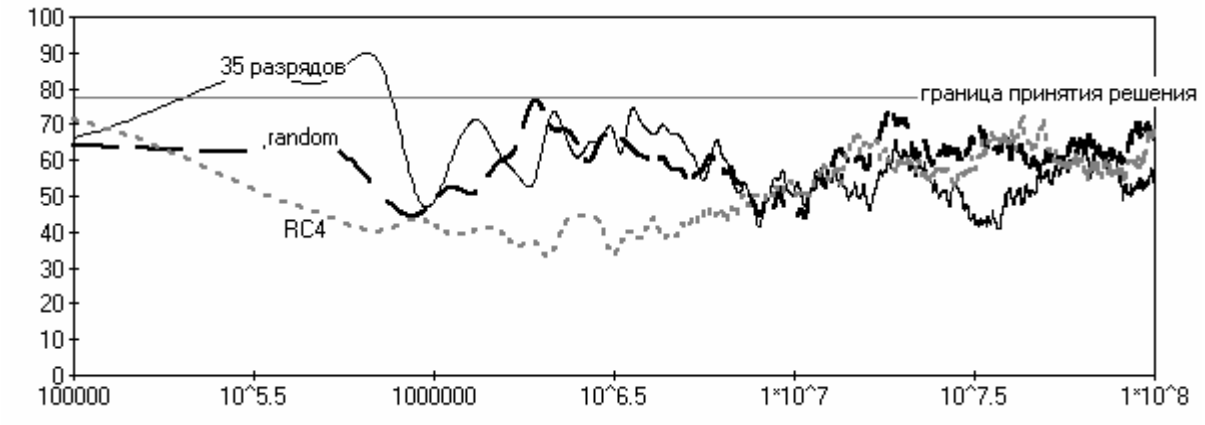

Рис.1. Зависимость y от количества испытаний для различных генераторов

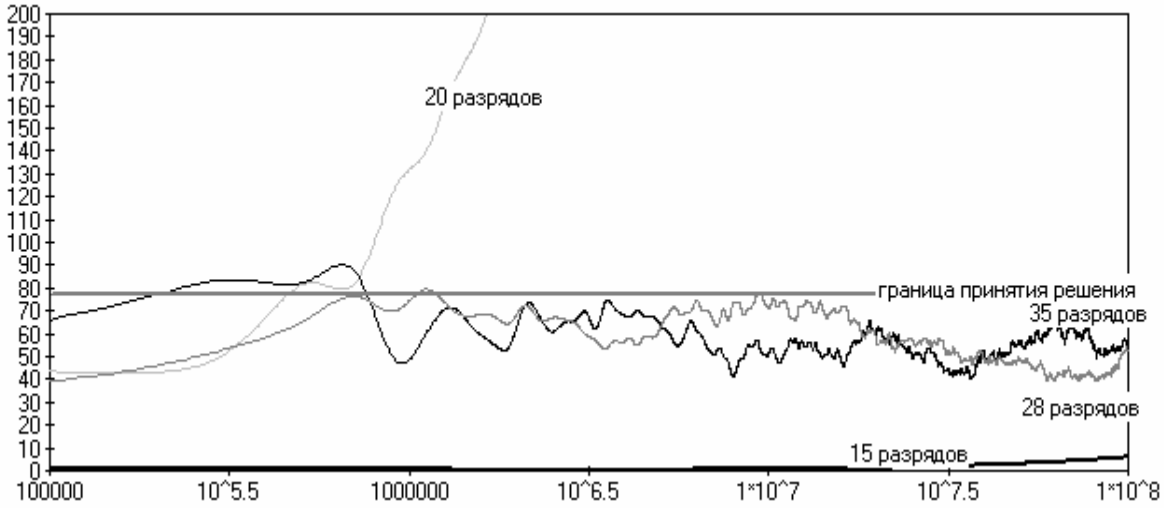

Рис.2. Зависимость y от количества испытаний для регистров различной разрядности

Таким образом, мы подтвердили наши результаты, полученные с помощью исследования гистограмм.

Генератор ПСП на основе алгоритма RC4 показывает очень убедительные результаты с точки зрения приближения к истинно случайной ПСП с равномерным законом распределения. Более того, алгоритм RC4 является криптостойким в силу своей нелинейности и большой длины ключа (до 2048 бит). Генераторы ПСП на основе LFSR показывают неплохие результаты с точки зрения приближения к истинно случайной ПСП с равномерным законом распределения. Однако, здесь ситуация меняется с изменением разрядности LFSR. Таким образом, необходимо подбирать для данного генератора регистры в соответствии с необходимым объемом ПСП, которую мы хотим с этого генератора получить. Чем больше длина требуемой ПСП, тем больше должна быть разрядность регистра. Однако с точки зрения криптостойкости, LFSR оказываются неприменимыми в чистом виде в современных криптоалгоритмах, в силу своей линейности и жесткой схеме

отводов обратной связи. Однако при объединении нескольких LFSR и внедрение дополнительной нелинейности (как, например, управление тактовой частотой регистра), их уже можно применять в защищенных системах цифровой связи. Например, используемый в стандарте GSM поточный шифр A5 имеет именно такую структуру (3 LFSR, разрядности 19,22,23 имеющие один общий выход).

ЛИТЕРАТУРА:

1. Ященко В.В. «Введение в криптографию». Изд. «Питер», 2001.
2. Нечаев В.И. «Элементы Криптографии. Основы теории защиты информации». Москва, изд. «Высшая Школа», 1999 год.