Анализ распределения псевдослучайной последовательности, генерируемой алгоритмом шифрования A5/1

Солуянов Дмитрий Алексеевич,
студент кафедры «Информационная безопасность»,
МГТУ МИРЭА, Россия, г. Москва

Ключевые слова: псевдослучайная последовательность, тесты НИСТ, шифр, A5/1

Внутреннее состояние шифра A5/1 состоит из трех линейных регистров сдвига с обратной связью R1, R2, R3, длиной 19, 22 и 23 бита соответственно(всего 64 бита). Сдвиг в регистрах R1, R2, R3 происходит только при выполнении определенного условия. Каждый регистр содержит "бит управления тактированием". В R1 это 8-й бит, а в R2 и R3 — 10-й. На каждом шаге сдвигаются только те регистры, у которых значение бита синхронизации равно большинству значений синхронизирующих битов всех трех регистров.

Перед работой алгоритма выполняется инициализация регистров, затем производится вычисление 228 бит выходной последовательности. 114 бит используется для шифрования данных исходящего потока, остальные 114 бит для шифрования данных входного потока. Само шифрование представляет собой XOR (побитовое сложение по модулю 2) между данными и произведенной алгоритмом A5/1 псевдослучайной последовательностью.

Для получения в распоряжение генератора псевдослучайных последовательностей необходимо модифицировать программный код алгоритма A5/1 таким образом, чтобы на выход поступала сама последовательность вместо шифрованного текста.

Для изучения равновероятности распределения значений последовальности необходимо получить репрезентабельную выборку. Если выполнить алгоритм 400 раз, то будет получена последовательность длиной 11 400 байт, чего будет достаточно для проведения анализа тестами НИСТ.

Результаты проверки статистических свойств полученной последовательности с помощью тестов, предоставленных НИСТ:

№	Статистический тест	Определяемый дефект	P-value
1	Частотный тест	Слишком много нулей или единиц	0.096914
2	Частотный тест в подпоследовательностях	Слишком много нулей или единиц в подпоследовательностях	0.968156
3	Проверка на равномерность	Большое (малое) число подпоследовательностей нулей и единиц свидетельствует, что колебание потока бит слишком быстрое (медленное)	0.636038
4	Проверка на равномерность в подпоследовательностях	Отклонения в равномерности распределения нулей и единиц в подпоследовательностях	0.599346
5	Проверка рангов матриц	Отклонение распределения рангов матриц от соответствующего распределения для истинно случайной последовательности, связанное с периодичностью подпоследовательностей	0.658825
6	Спектральный тест	Периодические свойства последовательности	0.1781
7	Проверка непересекающихся шаблонов	Непериодические шаблоны встречаются слишком часто	1
8	Проверка пересекающихся шаблонов	Слишком часто встречаются m-битные последовательности единиц	0.1781
9	Универсальный статистический тест Маурера	Сжимаемость (регулярность) последовательности	0.521557
10	Сжатие при помощи алгоритма Лемпела-Зива	Большая сжимаемость, чем истинно случайная последовательность	0.873879
11	Проверка линейной сложности	Отклонение от распределения линейной сложности для конечной длины (под)строки	0.30369
12	Проверка серий	Неравномерность распределения m-битных слов	0.352414
13	Проверка апроксимированной энтропии	Неравномерность распределения m-битных слов. Малые значения означают высокую повторяемость	0
14	Проверка кумулятивных сумм	Слишком много нулей или единиц в начале последовательности	0.183976
15	Проверка случайных отклонений	Отклонение от распределения числа появлений подпоследовательностей определенного вида	0.007205

По критериям проверки аппроксимированной энтропии и случайных отклонений можно

сделать вывод, что генерируемая алгоритмом A5/1 псевдослучайная последовательность статистически неравновероятна.

Литература

1. И.В. Чугунков, «Методы и средства оценки качества генераторов псевдослучайных последовательностей, ориентированных на решение задач защиты информации», 2012.