набору комбинаций слов (при генерации словаря), и иерархические правила мутации, определяющие схему модификации элементов словаря в ходе атаки. Рассмотренные модели используются для организации атак по словарю и могут находить применение в задачах раскрытия и расследования компьютерных преступлений, предполагающих обеспечение доступа к закрытой паролем информации.

ТЕСТИРОВАНИЯ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ ЭЛЕКТРОННЫХ ПЛАСТИКОВЫХ КАРТ ПО МЕТОДОЛОГИИ NIST

Н.Г. КИЕВЕЦ

Обсуждаются результаты тестирования генераторов случайных чисел (ГСЧ) электронных пластиковых карт (ЭПК) с помощью созданного программно-аппаратного комплекса (АПК) и методологии NIST версии 2010 г., реализованной в системе MATLAB. Анализировалась последовательность длиной 1000192 бит, сформированная из ключей длиной 256 бит, используемых для шифрования по ГОСТ 28147-89. В целях экономии временных ресурсов для тестов, не требующих последовательностей в один миллион бит, была использована начальная часть сформированной последовательности длиной 128000 бит. Частотный тест в подпоследовательностях проводился для последовательности, составленной из первых 100 ключей.

Многократное тестирование с помощью вышеуказанных методик позволило определить требования к параметрам тестирования. Так, прохождение частотного теста в подпоследовательностях при длине подпоследовательности, равной 256 бит, говорит о том, что в каждом из ключей исследуемой последовательности количество единиц примерно равно количеству нулей. В тесте пересекающихся шаблонов длина подпоследовательности была взята равной 256 бит. Тест «блоков» в подпоследовательностях и универсальный статистический тест Маурера четко определяют значение длины подпоследовательности в зависимости от длины тестируемой последовательности. С учетом параметров, рекомендуемых NIST, для теста непересекающихся шаблонов выбрана длина шаблона m=8, так как длина ключа кратна этому значению.

При уровне значимости α=0,01, рекомендуемом NIST, ГСЧ ЭПК прошел все 15 тестов и может быть использован в носителях ключевой информации.

О СВОЙСТВАХ ДЕКАРТОВЫХ ПРОИЗВЕДЕНИЙ НЕПРИМИТИВНЫХ КОДОВ ХЕММИНГА

В.А. ЛИПНИЦКИЙ, А.А. БЕРЕЗОВСКИЙ

Развитие помехоустойчивого кодирования происходит в преодолении противоречивых требований к кодам: высокая скорость передачи информации в сочетании с необходимостью коррекции ошибок большой кратности. Выполнение последнего требования неизбежно вязнет в громоздких процедурах декодирования.

Существует мнение, что коды произведения могут дать неплохой выход из сложившейся ситуации. Теоретический анализ демонстрирует неплохие свойства кодов произведений с сомножителями — непримитивными кодами Хемминга. Проведенные компьютерные расчеты подтверждают теоретические выводы. Правда, обнаружился любопытный факт — при формировании кодов произведений следует избегать самодвойственных неприводимых примитивных полиномов: коды произведения на их основе имеют аномально высокую размерность, но их минимальное расстояние меньше теоретически рассчитанного.