Использование же криптографических средств в практически реализуемых системах неразрывно связано со стойкостью алгоритмов шифрования. В вероятностных терминах стойким считается алгоритм, в котором перехват зашифрованных сообщений не приводит к появлению точки единственного принятия решения об используемом ключе или переданном открытом сообщении.

При традиционном подходе стойкость алгоритма шифрования определяется стойкостью к известным видам криптографических атак, применяемых с целью прочтения, замены зашифрованного сообщения или вычисления ключа шифрования. При этом дифференциальный и линейный методы криптоанализа относятся к наиболее известным. Дифференциальный метод заключается в анализе пар открытого и зашифрованного текстов, между которыми существует определенная разность, вычисляемая, как правило, при помощи операции сложения по модулю два. Анализируя вероятности появления определенных разностей на выходе одного раунда преобразования в зависимости от разности на его входе, выделяют дифференциальные характеристики, при которых наиболее вероятная разность на выходе одного раунда соответствует определенной разности на входе следующего раунда. Далее проводится анализ пар текстов по накоплению статистики о возможном значении ключа шифрования или открытого текста.

В данной работе приведены основные параметры результатов алгоритма поиска правильных пар текстов по заданному дифференциалу для проведения анализа n-раундового алгоритма шифрования с использованием динамического хаоса.

Литература

1. *Сидоренко А.В., Мулярчик К.С. Шакинко И.В*. Вестник БГУ. Сер. 1 Физика, математика, информатика. № 4. 2012. С. 44–50.

РАЗРАБОТКА ПРОГРАММНОГО ПРОДУКТА ТЕСТИРОВАНИЯ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Е.В. СТАВЕР

Одной из актуальных задач криптографии является задача исследования статистических свойств бинарных последовательностей, используемых для создания ключей криптографических алгоритмов. Так в основу данной раззработки положен американский стандарт SP 800-90B. Документ SP 800-90B определяет требования к тестированию случайных последоввательнстей, полученных с физических датчиков. Данный программный продукт представляет собой пакет для тестирования битовых последовательностей, согласно документу NIST SP800-90B. Пакет состоит из динамической библиотеки с открытым интерфейсом для тестирования и программы-оболочки над ней. Среда разработки — Microsoft Visual Studio Express 2008, используемый язык программирования — C++

2 Функциональные возможности

Возможность выбрать набор из нескольких тестов для оценки заданной случайной последовательности:

ApproximateEntropy

ChiSquare

Collision

Сохранение результатов тестирования последовательностей в LOG-файл.

Результаты тестирования передаются в Excel и отображаются в виде диаграммы с выводом основных параметров тестов и результатом прохождения или не прохождения набора тестов последовательности.