УДК 004.421.5

ИССЛЕДОВАНИЕ ГЕНЕРАТОРА КРИПТОСТОЙКИХ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА БАЗЕ АЛГОРИТМА ШИФРОВАНИЯ 2-ГОСТ

Гоева Е.М. (Университет ИТМО)
Научный руководитель – Грозов В.А. (Университет ИТМО)

Введение. Шифрование играет важную роль в обеспечении информационной безопасности. Одним из стандартов криптографической защиты является алгоритм шифрования «Магма» [1], входящий в состав ГОСТ Р 34.12-2015. Для осуществления защиты данных используются генераторы псевдослучайных чисел, создающие последовательности, применяющиеся в дальнейших преобразованиях исходной информации. Таким образом достигается ограничение доступа к первоначальным данным, так как происходит их сокрытие, а для дешифрования требуется секретный ключ. Одной из самых значимых характеристик метода шифрования является его криптостойкость. Она описывает способность используемого криптоалгоритма противостоять попыткам получения злоумышленниками несанкционированного доступа. Как следствие, криптостойкость демонстрирует уровень надёжности защиты информации, прошедшей процесс шифрования.

Основная часть. Основными этапами работы являются:

1. Изучить алгоритм шифрования 2-ГОСТ [2], представляющий собой модифицированную версию стандарта «Магма», детально описать привнесённые в него изменения. Рассмотреть принципы работы генератора псевдослучайных последовательностей с учётом особенностей его применения на базе алгоритма 2-ГОСТ.
2. Определить отличия в устройстве генератора в случаях его использования на основе методов шифрования «Магма» и 2-ГОСТ. Установить преимущества работы рассматриваемого генератора на базе алгоритма 2-ГОСТ в качестве метода криптографического преобразования данных.
3. Провести оценку эффективности и криптостойкости генератора псевдослучайных последовательностей на основании тестов NIST [3], определяющих степень случайности порождённых числовых последовательностей.

Выводы. В ходе выполнения работы были рассмотрены понятия генератора случайных последовательностей и его криптостойкости, изучены такие алгоритмы криптографического преобразования, как «Магма» и 2-ГОСТ, который представляет собой модифицированную версию существующего стандарта. Исходя из сведений, полученных в ходе анализа рассмотренных методов шифрования, были выявлены принципиальные отличия в реализации генераторов на их базе, а также определены преимущества использования криптоалгоритма 2-ГОСТ относительно сравниваемого метода. Данное предположение было проверено при помощи набора тестов, позволяющего оценить качество генератора, которое заключается в криптостойкости создаваемых им числовых последовательностей.

Список использованных источников:

1. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. – Москва: Стандартинформ, 2015. – 21 с.
2. Дмух А., Дыгин Д., Маршалко Г. О возможности модификации алгоритма шифрования ГОСТ 28147-89 с сохранением приемлемых эксплуатационных характеристик [Электронный ресурс]. – URL: https://www.ruscrypto.ru/resource/archive/rc2013/files/07_dmukh_marshalko.pdf (дата обращения: 05.02.2024).
3. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. – NIST, Special Publication 800-22.

Гоева Е.М. (автор) Подпись

Грозов В.А. (научный руководитель) Подпись