Секция «Математика и механика»

Применение нестандартных операций в алгоритмах симметричного шифрования.

Годнева Анастасия Валерьевна
Аспирант
Московский государственный университет имени М.В. Ломоносова,
Механико-математический факультет, Москва, Россия
E-mail: god139@yandex.ru

Объектом исследования является стандарт шифрования, используемые в республике Узбекистан, а именно алгоритм шифрования данных – симметричный блочный шифр.

По структуре он похож на известные стандарты шифрования – AES и DES, но имеет свои особенности. В качестве функции рассеивания в стандарте используется умножение слева на матрицу, зависящую от сеансового ключа. В качестве функции перемешивания – S-блоки, зависящие от этапного ключа. Для формирования сеансовых ключей используется умножение с параметром. В докладе будет сделана оценка эффективности использования данных операций, поиск слабых ключей и сравнение с AES и DES-алгоритмами шифрования, считающимся надежным. Так исследуется устойчивость алгоритма против линейного и дифференциального криптоанализа и других известных атак.

Литература

1. Государственный стандарт Узбекистана - Информационная технология КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ Алгоритм шифрования данных. Узбекское агентство стандартизации, метрологии и сертификации, Ташкент

2. Mitsuru Matsui Linear Cryptoanalysis method for DES Cipher, Computer & Information Systems Laboratory

3. Зензин А.С., Иванов М.А. Стандарт криптографической защиты – AES. «Кудиц-образ» Москва 2002

4. Menezes, P. van Oorschot, S. Vanstone Handbook of Applied Cryptography, CRC Press, 1996.

Слова благодарности

Автор выражает большую благодарность научным руководителям А.В. Галатенко и А.Е. Панкратьеву за постановку задачи и внимание к работе.