векторные пространства, процедуры процесса шифрования и расшифрования используют непрерывное преобразование этих областей.

Каждый открытый текст представляется как точка топологии пространства X, каждый криптотекст является точкой топологии Y, каждая процедура шифрования/расшифрования рассматривается как непрерывный изоморфизм между X и Y.

При рассмотрении непрерывных криптосистем можно использовать понятие дискретизации непрерывных объектов. Дискретизация предполагает введение в рассмотрение точных раундовых процедур преобразования.

Метрическая система с точки зрения информационного подхода определяется как непрерывная криптосистема со следующими свойствами:

– определено точное конечное подмножество P для X как пространство открытых текстов;

– точно определено конечное подмножество C для Y как пространство криптотекстов;

– каждая процедура шифрования/расшифрования выполняется итеративно в виде раундов преобразований, гарантирующих отображение $P \to C$.

Обнаружение ошибки при передаче криптотекстов. Рассмотрим ситуацию, когда открытый текст представляется как дискретная точка в $\mathbf{R}^n$ (точка, принадлежащая решетке $\mathbf{Z}^n$ в $\mathbf{R}^n$, где $\mathbf{Z}$ – множество всех целых чисел), а криптотекст получается в результате непрерывного не обязательно везде дискретного преобразования. Любая ошибка, произошедшая при передаче криптотекста, делает маловероятным, событие размещения результата расшифрования в дискретной точке. Следовательно, результат расшифрования, размещенный не в дискретный точке, может свидетельствовать об ошибке при передаче криптотекста.

МОДИФИЦИРОВАННЫЙ АЛГОРИТМ ШИФРОВАНИЯ И ЕГО КРИПТОАНАЛИЗ

А.В. Сидоренко, Д.А. Жуковец

В современном мире информационный ресурс стал одним из наиболее мощных рычагов экономического развития.

Наряду с традиционными алгоритмами шифрования, которые постоянно разрабатываются и совершенствуются, все большую популярность в криптографическом сообществе приобретают алгоритмы шифрования на основе систем динамического хаоса.

Целью работы является разработка алгоритма и программных средств для шифрования на основе динамического хаоса, а также исследование его устойчивости к различным видам криптоатак.

В результате проведенных исследований нами был разработан алгоритм, а также программа для шифрования и расшифрования открытого текста с использованием динамического хаоса. Для доказательства стойкости алгоритма шифрования проведено определение количественных параметров, таких как информационная энтропия, числовых характеристик распределения значений байт в открытом и зашифрованном тексте, корреляция, процент бит изменивших значение (лавинный эффект), процент пикселей изменивших значение (Number of Pixels Change Rate), среднее изменение интенсивности (Unified Average Changing Intensity). Проведен линейный и дифференциальный криптоанализ алгоритма шифрования

Литература

1. Chaos-based secure satellite imagery cryptosystem / M. Usama et al. // Computers and Mathematics with Applications 60 (2010) 326-337

2. A chaos-based image encryption scheme using 2D rectangular transform and dependent substitution / Xuanping Zhang, Xing Fan, JiayinWang, Zhongmeng Zhao // Springer (2014)