Министерство образования и науки Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

*Кафедра компьютерной физики и метаматериалов*
*на базе Саратовского филиала*
*Института радиотехники и электроники*
*имени В.А. Котельникова РАН*

# КОДИРОВАНИЕ ИНФОРМАЦИИ НА ОСНОВЕ МОДИФИЦИРОВАННОГО ОТОБРАЖЕНИЯ «КОТ АРНОЛЬДА»

АВТОРЕФЕРАТ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ
(БАКАЛАВРСКОЙ) РАБОТЫ

студента 4 курса 432 группы
направления 03.03.02 «Физика» физического факультета
Джаиева Эльмара Эльдар оглы

Научный руководитель
к.ф.-м.н. доцент А. С. Ремизов

Заведующий кафедрой
д.ф.-м.н. профессор В.М. Аникин

Саратов
2018

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность и развитие информационных технологий, электроники и техники связи с использованием проводных и беспроводных линий связи сопровождается решением проблем обеспечения конфиденциальности передаваемой информации, которая может иметь разнообразную форму представления – в виде тестовых, табличных, видео и иного рода файлов, голосовых сообщений и т.п. Защита информации может идти в различных направлениях –кодирования информации, создания линий связи. Задачи шифрования информации составляют предмет криптографии.

Применение алгоритмов на основе хаотических отображений вполне естественно и уместно, поскольку они представляют собой генераторы псевдослучайных последовательностей, а использование датчиков псевдослучайных чисел, в том числе получаемых на основе модулярной арифметики, – краеугольный камень схем шифрования.

В основе работы я рассматривал трехмерный аналог хаотического отображения “кот Арнольда”.

**Целью** данной работы является изучение и реализация модифицированного симметричного алгоритма шифрования произвольных данных на основе трехмерного отображения «Кот Арнольда». Алгоритм адаптирован для работы с файлами произвольного формата, а также с любыми байтовыми потоками.

В **задачи** работы входит:

1) методическое изложение теоретической базы, необходимой в работе;

2) изучение свойств отображений, подходящих для кодирования;

3) изучение модифицированного симметричного алгоритма шифрования на основе трехмерного отображения «Кот Арнольда», статистическое тестирование получаемых шифротекстов, сравнение с другими алгоритмами.

**Структура и объем работы.** Выпускная квалификационная работа изложена на 36 страницах, состоит из введения, 3 разделов, и заключения. Библиографический список включает 16 наименований. Текст содержит 3 таблицы и иллюстрирован 8-ю рисунками.

В **первой** главе работы теоретически предоставляются сведения из теории хаоса, виды систем и сопоставление свойств хаотических и криптосистем.

Во **второй** главе излагается алгоритм хаотического кодирования информации на базе отображения "кот Арнольда", приводятся результаты компьютерной реализации процесса кодирования и их анализ.

В **третьей** главе приводятся различные идеи шифрования на хаосе и их реализация.

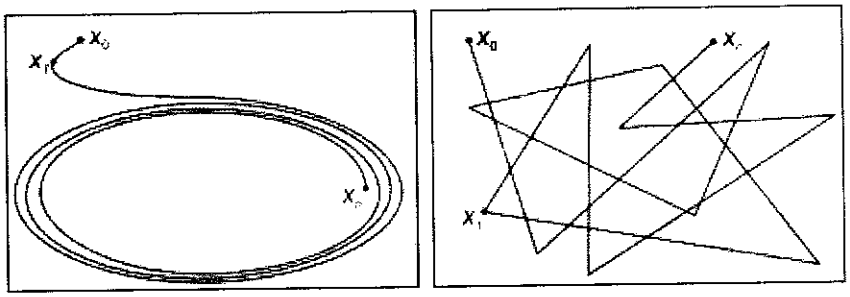

Рисунок 1. Пример фазовых портретов хаотической и криптографической систем.

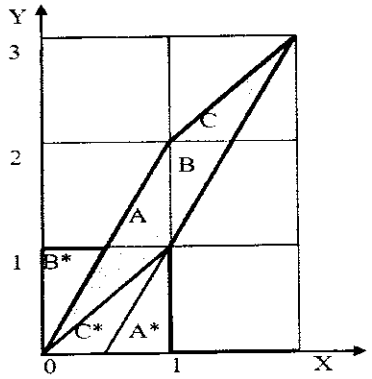


Рисунок 2. Геометрическая иллюстрация отображения «Кот Арнольда»

**Результаты тестирования в DIEHARD.**

| № | Название теста | Значение P-value |
|---|---|---|
| 1 | Дни рождения (Birthday Spacings) | 0.779656 |
| 2 | Пересекающиеся перестановки (Overlapping Permutations) | 1 |
| 3 | Ранги матриц (Ranks of matrices) | 1 |
| 4 | Обезьяньи тесты (Monkey Tests) (приведен только один по словам) | 0,77792 |
| 5 | Подсчёт единичек (Count the 1's) | 1 |
| 6 | Тест на парковку (Parking Lot Test) | 0.691421 |
| 7 | Тест на минимальное расстояние (Minimum Distance Test) | 1 |
| 8 | Тест случайных сфер (Random Spheres Test) | 0.791671 |
| 9 | Тест сжатия (The Squeeze Test) | 1 |
| 10 | Тест пересекающихся сумм (Overlapping Sums Test) | 0.972431 |
| 11 | Тест последовательностей (Runs Test) | 0.998649 (up)<br>0.992545 (down) |
| 12 | Тест игры в кости (The Craps Test) | 0.126239 (wins)<br>1 (throws) |

В **заключении** проанализирована принципиальная возможность использования трехмерного отображения “кот Арнольда” в схемах хаотического кодирования информации.

Поступающие на вход алгоритма данные помещаются во входной буфер, откуда алгоритм шифрования выбирает последовательно по три байта для каждой итерации.

По статистическим тестам видно, что в результате обобщения схемы качество шифрования не уменьшилось. Шифротексты, получаемые на выходе схемы при включенной диффузии, демонстрируют отсутствие статистических закономерностей.

**Список использованных источников.**

1. *Дмитриев А.С., Панас А.И.* Динамический хаос: новые носители информации для систем связи. – М.: Изд-во физ.-мат. лит., 2002. 252 с.

2. *Владимиров С.Н., Измайлов И.В., Пойзнер Б.Н.* Нелинейно-динамическая криптология. Радиофизические и оптические системы / Под ред.С.Н. Владимирова. М.: ФИЗМАТЛИТ, 2009. 208 с.

3. *Лоскутов А.Ю., Рыбалко С.Д., Чураев А.А.* Система кодирования информации посредством стабилизации циклов динамических систем // Письма в ЖТФ. 2004. Т. 30, вып. 20. С. 1-7.

4. *Годунов С.К., Антонов А.Г., Кирилюк О.П., Костин В.И.* Гарантированная точность решения систем линейных уравнений в евклидовых пространствах. Новосибирск: Наука, 1988. Гл. 4.

5. *Сикорский Ю.С.* Элементы теории эллиптических функций с приложениями к механике. М.:ОНТИ, 1936. Гл. 1.

6. *Голубенцев А.Ф., Аникин В.М., Ноянова С.А.* Модификации отображения пекаря: особенности асимптотического поведения // Известия вузов – Прикладная нелинейная динамика. 2004. Т. 12. № 3. С. 45-57.

7. *Лоскутов А.Ю., Рыбалко С.Д.* Динамические системы с внешними возмущениями как системы кодирования и скрытой передачи информации // Радиотехника и электроника. 2005. Т. 50. № 2. С. 1466–1475.

8. *Аникин В.М., Чебаненко С.В.* Хаотические отображения и кодирование информации: модификации исторически первого алгоритма // Гетеромагнитная микроэлектроника. 2011. Вып.9. С. 81-95.

9. *Шредер М.* Фракталы, хаос, степенные законы. Миниатюры из бесконечного рая. Москва: Ижевск: НИЦ "Регулярная и хаотическая динамика", 2001. С. 333-336.

10. *Chen Guanrong, Mao Yaobin, Chui Charles K.* A Symmetric Image Encryption Scheme based on 3D Chaotic Cat maps // Chaos, Solitons and Fractals. 2004. V. 21, N 3. P. 749–761.

11. *Аникин В.М., Голубенцев А.Ф.* Аналитические модели детерминированного хаоса. М.: ФИЗМАТЛИТ, 2007. 328 с.

12. *Лоскутов А.Ю., Чураев А.А.* Использование хаотических отображений для за-щиты информации // Вестник Моск. ун-та. Сер. Физика, астрономия. 2008. № 2. С. 15-19.

13. *Romuel F. Machado, Murilo S. Baptista, C. Grebogi.* «Cryptography with chaos at the physical level», // Chaos, Solitons and Fractals 21 (2004) p. 1265–1269;

14. *Mao YB, Chen G.* Chaos-based image encryption.// Handbook of Computational Geometry for Pattern Recognition, Computer Vision, Neurocomputing and Robotics. New York: Springer-Verlag; in press, 2004.

15. *Дмитриев А., Старков С.* «Новые подходы к решению проблем в системах связи и компьютерных сетях: динамический хаос»// Компьютера (2001), № 46.

16. Аникин В.М., Василенко Л.П., Чебаненко С.В.Компьютерные науки и информационные тех-нологии: Материалы межд. научной конф. Саратов, Россия, 1-4 июля 2012 г. Саратов: Издат. Центр «Наука», 2012. С. 29-31.