МИНОБРНАУКИ РОССИИ

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 им. В. А. Котельникова РАН

ПРИМЕНЕНИЕ ХАОТИЧЕСКИХ ДИНАМИЧЕСКИХ СИСТЕМ В ЗАДАЧАХ КРИПТОГРАФИИ

АВТОРЕФЕРАТ МАГИСТЕРСКОЙ РАБОТЫ

Дёмина Игоря Ярославовича,
студента 2 курса, 2225 группы,
направления подготовки 03.04.02 Физика
Института физики

Научный руководитель
д.ф.-м.н. профессор В.М. Аникин

Заведующий кафедрой
компьютерной физики и метаматериалов
на базе Саратовского филиала Института радиотехники
и электроники им. В. А. Котельникова РАН
д.ф.-м.н. профессор В.М. Аникин

Саратов 2021 г.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность работы. В последние десятилетия развитие криптографии как науки о защите информации приобрело особую актуальность в связи, по крайней мере, с двумя причинами:

прогресс в развитии вычислительной техники и широким ее применением в различных сферах человеческой деятельности обусловливает острую необходимость защиты компьютерной информации;

возникала тенденция развития криптографических методов защиты информации не только на государственном уровне, но и на корпоративном и личном уровнях.

Криптографические алгоритмы строятся на различной математической базе (дискретная математика, теория конечных полей, вероятностные методы, методы анализа графов и др.). На рубеже столетий стало развиваться направление, связанное с разработкой и исследованием алгоритмов шифрования на основе динамического хаоса. Применение методов хаотической динамики для шифрования данных теоретически обладает большим потенциалом, что обусловлено фундаментальными свойствами детерминированного хаоса, к которым относятся: высокая чувствительность к начальным условиям; индивидуальным характером траектории в зависимости от начального условия (это воспринимается как случайность), запутанный характер траектории в области определения хаотической системы. В связи с этим стали получать развитие новые криптографические алгоритмы.

Основными проблемами алгоритмов хаотического кодирования являются:

повышение степени защищенности информации,

повышение скорости и эффективности шифрования,

эффективная программно-аппаратная реализация хаотических алгоритмов.

В выпускной квалификационной работе (ВКР) исследуются особенности применения хаотической динамики для решения криптографических задач на базе одномерных хаотических отображений. Решаются прямая (шифрование) и обратная (расшифрование) задачи в общем случае, а затем иллюстрируется применение общего алгоритма для конкретных отображений.

Целью работы является демонстрация принципиальной возможности использования хаотических отображений для решения криптографических задач с учетом фундаментальных свойств чувствительной зависимости траекторий детерминированных хаотических отображений от начальных условий и параметров отображений.

Задачами работы являются:

1) построение некоторого базового алгоритма шифрования текстовой информации на основе свойств детерминированного хаоса;

2) синтез и применение в криптографических схемах новых одномерных отображений, способных увеличить сложность криптографического ключа, главной секретной информации;

3) адаптация общего алгоритма для функционирования на базе конкретного отображения;

4) расчет характеристик, свидетельствующих об уровне криптостойкости предлагаемых схем шифрования.

Фундаментальным признаком всех рассматриваемых отображений является свойство перемешиваемости, признаваемое в качестве одного из условий качественного кодирования.

К числу ***новых (защищаемых) результатов*** можно отнести разработку криптографических схем на основе отображения, которому присущ развитый хаос для *некоторого диапазона* непрерывного изменения параметра.

Достоверность результатов подтверждается работоспособностью развитых алгоритмов для различных хаотических отображений.

Теоретическая значимость работы связана с выявлением особенностей эволюционных и статистических свойств дискретных динамических систем, демонстрирующих хаотическое поведение, демонстрацией направления синтеза новых хаотических отображений, допускающих точное аналитическое решение траекторных, статистических и спектральных характеристик.

Практическая значимость работы обусловлена демонстрацией прикладных возможностей теории детерминированного хаоса в актуальных задачах защиты информации.

Структура ВКР. Выпускная квалификационная работа (ВКР) содержит введение, четыре главы, заключение, список использованных источников (46 наименований) и 2 приложения.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении приводятся аспектные характеристики работы (актуальность, теоретическая и прикладная значимость, цель и задачи работы, особенность подхода).

В первой, обзорной по характеру главе, описывается классификация криптографических алгоритмов и формулируются требования, предъявляемые к ним.

Во второй главе разрабатывается вариант общего алгоритма кодирования символа исходного текста на основе динамики хаотического отображения: область задания отображения разбивается несколько подынтервалов (по числу букв алфавита), с каждым интервалом соотносится буква алфавита, при компоновке шифротекста буква заменяется на число итераций, приводящих траекторию в данный подынтервал. Составляющими секретного ключа могут являться: начальная точка для проведения итераций, параметры отображения, механизм продолжения итераций при кодировании очередного

символа, правило соотнесения символов алфавита с отрезками разбиения полного интервала и т.п. Сформулирован также алгоритм восстановления информации из шифротекста.

Рассмотрим некоторое отображение, обладающее свойством хаотичности:

$$x_{n+1} = g(x_n, \lambda),\ x \in \Omega \in (a,b),\ n = 0,1,2,\ldots, \qquad (1)$$

где $g(x,\lambda)$ – определенная на некотором интервале (a,b) итеративная функция, зависящая от параметра λ, изменяющегося в некоторых пределах. Мы будем рассматривать только те отображения, которые заведомо имеют аналитически точно вычисляемые инвариантные распределения для всех значений параметра.

Чтобы построить на основе отображения (1) систему кодирования для N=256 текстовых символов, интервал определения отображения (a,b) разбивается на 256 частей (ячеек), с каждой из которых соотносится некоторый символ используемого алфавита. Такое соотнесение может быть совершенно произвольным и меняться от сеанса к сеансу связи и (или) в процессе одного сеанса. Длина такой ячейки в простейшем случае равенства длин всех подынтервалов есть: $e = (b-a)/N$.

Образец «раскладки» символов алфавита по частичным интервалам отражает таблица, приводимая ниже.

Таблица 1. Вариант соотнесения символов алфавита с подынтервалами области определения отображения для фиксированного значения параметра λ

№ ячейки	1	2	…	k	…	N-1	N
Позиция ячейки	$[a, a+e]$	$[a, a+2e]$	…	$[a, ke]$	…	$[a, (N-1)e]$	$[a, b]$
Кодируемый символ	a	b	…	%	…	$	@

Алгоритм шифрования. В качестве кода символа исходного текста принимается число итераций (например, n), приводящих орбиту отображения в ячейку, с которой соотнесен данный символ. Далее процедура повторяется для очередного символа передаваемого текста, причем в качестве x_0 может выступать значение x_n, полученное при завершении предыдущей серии итераций.

Алгоритм расшифрования. Алгоритм расшифрования сообщения идентичен (симметричен) алгоритму шифрования. Адресат должен знать вид

отображения (1), полный ключ, включая таблицу соответствия. Знание кодов поможет задать необходимое число итераций отображения (1), которые «приведут» точку в подынтервал, с которым соотнесен порядковый номер вполне определенного символа алфавита.

Схема, описанная выше, на самом деле не является оптимальной и может быть усовершенствована по ряду параметров. Прежде всего, нужно иметь в виду, что для передачи информации, закодированной описанным способом, может потребоваться большее число битов по сравнению с оригинальным текстом, если число итераций окажется велико (требующим для представления большего числа битов, чем исходный символ, и выходящим при представлении символа одним байтом значение 11111111). Поэтому для устранения этой коллизии необходимо искать «непрямые» способы задания кодировки символов в рамках хаотического процесса.

Схема, далее, может быть видоизменена с учетом особенностей машинной арифметики. Вычислительная машина оперирует исключительно с вполне определенной выборкой рациональных чисел. Множество машинных чисел обладает весьма специфическими свойствами:

1) оно является дискретным, ограниченным и конечным;

2) каждое число имеет вполне определенное число разрядов (в зависимости от свойств разрядной сетки компьютера);

3) числа этого дискретного множества расположены с определенным шагом, зависящим от области представления числа. В процессе вычислений происходят округления, при этом расчетный машинный результат с учетом особенности множества машинных чисел может зависеть от порядка следования операндов.

Таким образом, начальная точка траектории хаотического отображения может быть задана только рациональным числом. Можно искусственно изменяя формат представления этого числа (увеличить и уменьшить число значащих разрядов в представлении этого числа). В силу существенной зависимости орбиты отображения от начального условия «отрицательная» особенность множества машинных чисел может быть превращена в схемах кодирования в некоторый «плюс»: варьируемое число значащих разрядов начального значения может использовать в качестве дополнительного параметра в составе ключа схемы кодирования.

Что касается повышения крипкостойкости алгоритма, то, во-первых, формирование кода можно начинать после некоторого «переходного» процесса (некоторого числа итераций отображения (1)), во-вторых, условие «результативного попадания» в нужный интервал можно усложнить, совместив его с достижением истинности некоторого предиката (условия, сравнения). Например, при достижении интервала провести дополнительный розыгрыш случайной величины R из данного интервала по некоторому закону, и в зависимости от того, больше или меньше R текущее значение x_n, предусмотреть окончание алгоритма «пристрелки» или продолжить его до выполнения условия $x_n > R$. Можно также заранее случайным образом задать свое число

«успешных попаданий», используемое для записи кода, для каждого кодируемого символа.

В третьей главе работы проиллюстрирован способ построения новых хаотических отображений для использования в решении задач криптографии с целью усложнения алгоритмов шифрования (и тем самым, для большей защиты) информации на базе хаотических отображений. На основе эллиптических функций Якоби построено семейство отображений, эволюционные свойства которых зависят от параметра. Этот параметр может быть включен в схему ключа для кодирования информации на основе этих отображений. Алгоритм реализуется в среде программирования «Delphi».

Дополнительные возможности для усложнения алгоритмов шифрования (и тем самым, для большей защиты) информации на базе хаотических отображений обеспечивают отображения, эволюционные (динамические) и вероятностные свойства которых зависят от параметра отображения. Уникальную возможность в этом плане открывают хаотические отображения, которые могут быть построены на основе хаотических кусочно-линейных отображений посредством обратимой замены переменной на базе эллиптических функций Якоби. Эти отображения генерируют развитый хаос, характеризуемый наличием инвариантной плотности, для некоторой области непрерывного изменения параметра и обладают точными аналитическими траекторными и вероятностными характеристиками.

Выберем в качестве базового пирамидальное отображение:

$$z_{n+1} = \begin{cases} 2z_n, & 0 \le z_n < 1/2, \\ 2 - 2z_n, & 0 \le z_n < 1/2, \end{cases} \qquad (2)$$

и делаем в (2) замену переменных по правилу:

$$x = \mathrm{sn}^2(Kz, k),\ z = \frac{1}{K}\mathrm{sn}^{-1}\left(\sqrt{x}, k\right), \quad 0 < k < 1. \qquad (3)$$

Здесь полный эллиптический интеграл определяется как

$$K = \int_0^{\pi/2} \frac{d\varphi}{\sqrt{1 - k^2 \sin^2 \varphi}} = \int_0^1 \frac{dt}{\sqrt{(1-t^2)(1-k^2 t^2)}}.$$

В результате преобразований из (2) получим новое отображение:

$$x_{n+1} = 4x_n(1 - x_n)\frac{1 - k^2 x_n}{\left(1 - k^2 x_n^2\right)^2}, \quad 0 < x_n < 1. \qquad (4)$$

Вид отображения (4) для различных значений параметра k показан на рис. 1. Оно демонстрирует хаотическое поведение при непрерывном изменении параметра k.

Соответствующая инвариантная плотность отображения (4) существует для всех значений параметра k и имеет вид (рис. 2):

$$f^*(x) = \frac{1}{2K} \frac{1}{\sqrt{x(1-x)(1-k^2 x)}}, \; x \in (0,1) \; . \qquad (5)$$

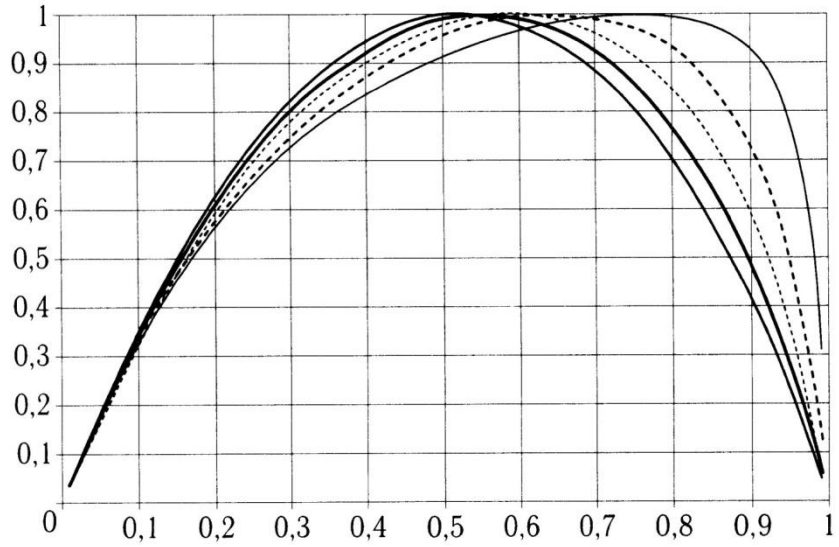

Рис. 1. Семейство хаотических отображений (4), полученных из пирамидального отображения заменой переменной на основе эллиптического синуса Якоби для значений параметра $k = 0{,}18;\ 0{,}36;\ 0{,}54;0{,}72;\ 0{,}9$. С ростом значения параметра вид отображения приближается к параболе. Ось абсцисс – x, ось ординат – $g(x)$ (это в соответствии с обозначениями в формуле (1), но без параметра λ

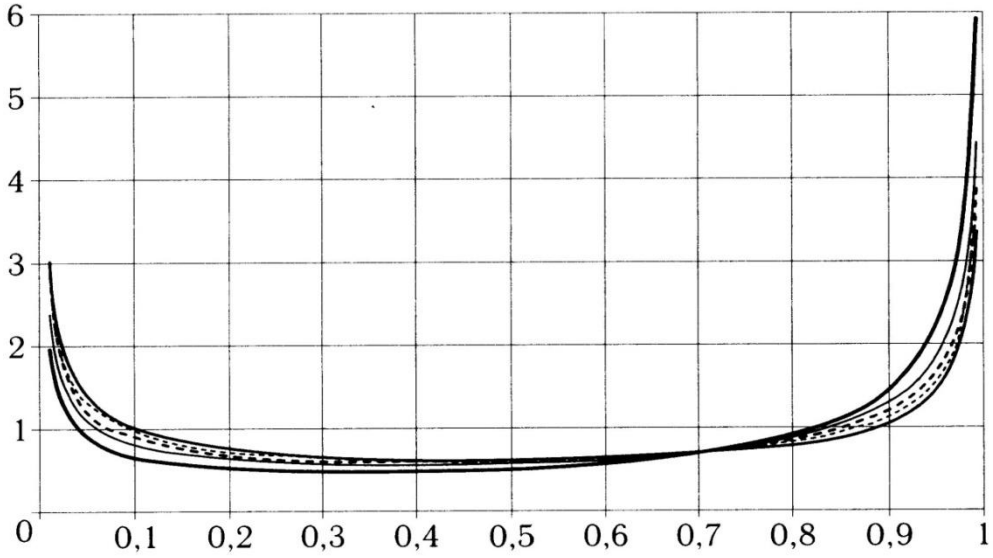

Рис. 2. Инвариантная плотность (5) хаотического отображения (4), полученного из пирамидального отображения заменой переменной на основе эллиптического синуса Якоби, как функция параметра k (с ростом значения параметра график становится все более симметричным, приближаясь к виду инвариантной плотности отображения Улама-фон Неймана). Ось абсцисс – x, ось ординат – $f^*(x)$ (это в соответствии с формулой (5))

Модуль кодирования на базе хаотического отображения (4) реализовано на языке программирования Delphi в среде разработки «Borland Delphi

7» для двух участников компьютерной связи с соответствующими IP-адресами. На рис. 3–6 показаны примеры обмена текстами между участниками переписки: открытом виде (текст вводится в верхнее окно переписки) и зашифрованном виде (текст вводится в нижнее окно переписки). Справа показан шифротекст, сгенерированный с помощью отображения на основе эллиптического синуса. Программа допускает использование для алгоритма шифрования нескольких отображений. Отправка текста осуществляется по команде «Отправить», а визуализация шифрованного текста – по команде «Проверить».В примерах обращается на себя внимание тот факт, что одни и те же текстовые символы кодируются разными числами.

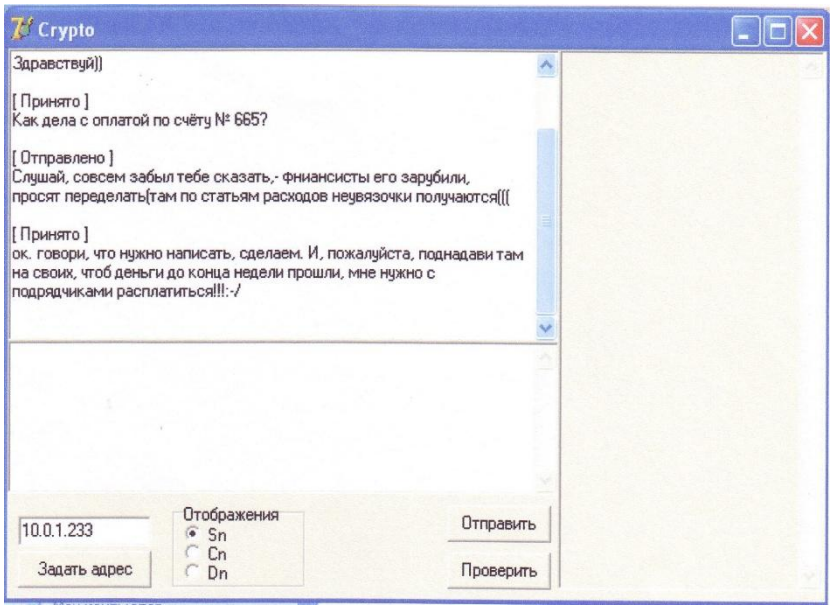

Рис. 3. Модуль первого участника переписки (открытые сообщения)

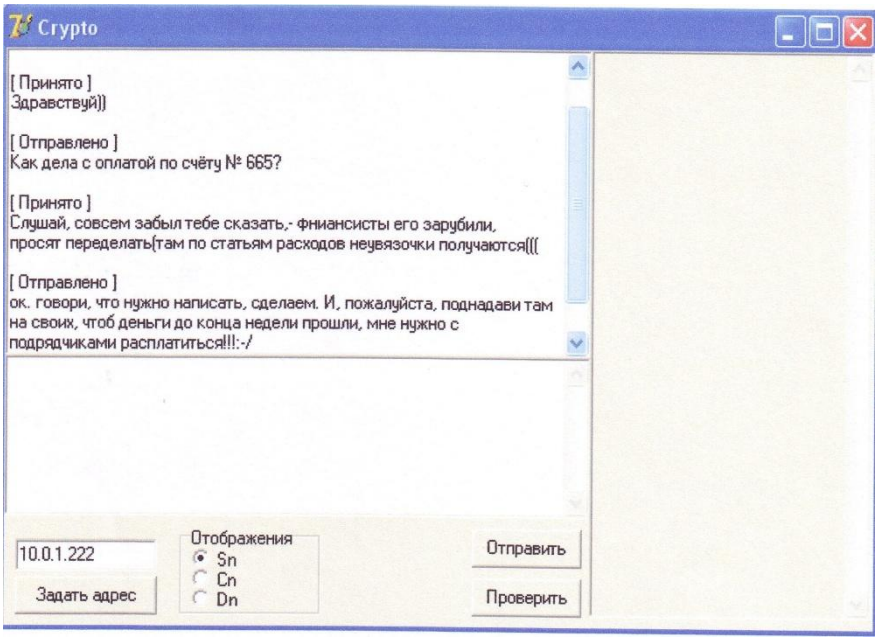

Рис. 4. Модуль второго участника переписки (открытые сообщения)

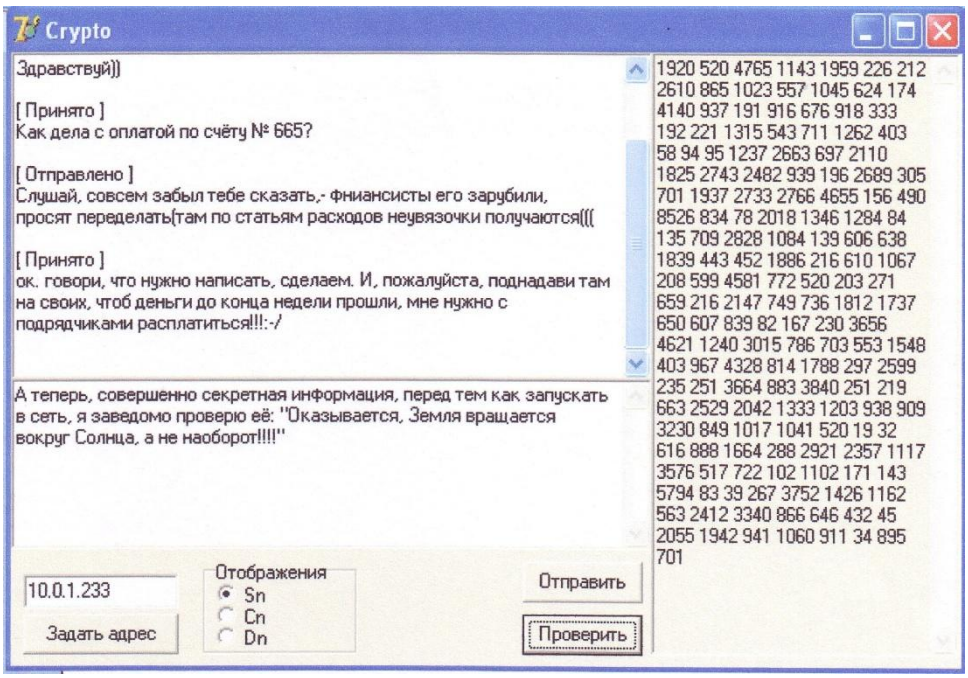

Рис. 5. Занесение закрытой информации (нижнее поле)
и ее визуализация в специальном окне

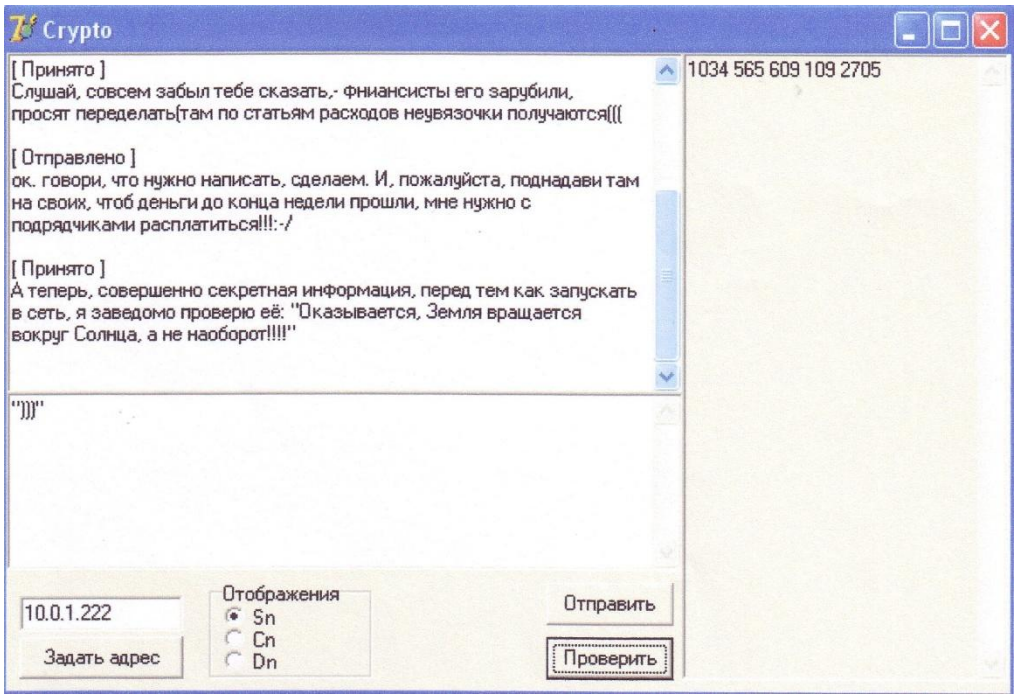

Рис. 6. Пример шифрования одинаковых символов («кавычки» и «закрывающая скобка»)

В главе 4 работы описана криптографическая схема на основе нескольких хаотических отображений для шифрования компьютерных данных.

ЗАКЛЮЧЕНИЕ

В выпускной квалификационной работе рассмотрено применение одномерных хаотических отображений к решению задачи защиты информации при передаче данных в компьютерных сетях.

В целом, в работе показана принципиальная возможность создания программных продуктов для криптографических задач на базе хаотических отображений. Рассмотрены некоторые основные технические требования к соответствующей организации компьютерной сети для передачи зашифрованных данных (создание сокетов, настройка защитных программ от вирусов, запрещенной информации и т.п.).

Оптимальность модулей кодирования (в том объеме, в котором он был развит в работе) может быть подвергнута критике за необходимость передачи большего объема информации по сравнению с исходным текстом. Эта проблема может найти решение на пути совершенствования базового алгоритма кодирования, обеспечивающего более оптимальную кодировку. При любых вариантах алгоритма полезно проведение статистического анализа шифротекста и времени его расшифровывания (в случае несанкционированного доступа).

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М. : Триумф, 2002, 2003. 816 с.
2. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М.: Госстандарт СССР, 1989.
3. Указ Президента РФ № 334 от 03.04.95. О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставление услуг в области шифрования информации // Собрание законодательства РФ. 1995. № 29.
4. *Ященко В.В*. Введение в криптографию. СПб. : Питер, 2011. 288 с.
5. *Дмитриев А.С., Панас А.И.* Динамический хаос: новые носители информации для систем связи. – М.: Изд-во физ.-мат. лит., 2002. 252 с.
6. *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.
7. *Baptista M.S.* Cryptography with chaos // Phys. Lett. 1998. V. A240. Pp. 50–54.
8. *Fridrich I.* Symmetric ciphers based on two-dimrnsional chaotic maps // Int. J. of Bifurcation and Chaos // 1998. V. 8. Pp. 1259–1284.
9. *Wong K.W.* A fast chaotic cryptographic scheme with dynamic look-up table // Phys. Lett. 2002. V. A289. Pp. 238–242

10. *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.
11. *Chen G., Mao Y., Chui Ch. K.* A symmetric image encryption scheme based on 3D chaotic cat maps // Chaos, Solitons and Fractals. 2004. V. 21. Pp. 749–761.
12. *Machado R.F., Baptista M.S., Grebogi C.* Cryptography with chaos at the physical level // Chaos, Solitons and Fractals. 2004. V. 21. Pp. 1265–1269.
13. *Чебаненко С.В., Аникин В.М.* Устройство криптографической защиты данных сетевого обмена ПК // Всероссийская молодежная выставка-конкурс прикладных исследовании, изобретений и инноваций. Саратов, 27-28 октября 2009 г.: Сб. материалов. Саратов: изд-во Сарат. ун-та, 2009. С. 41.
14. *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.
15. *Аникин В.М., Чебаненко С.В.* Хаотические отображения и кодирование информации: модификации исторически первого алгоритма // Гетеромагнитная микроэлектроника. 2011. Вып.9. С. 81-95.
16. *Аникин В.М., Василенко Л.П., Ремизов А.С., Чебаненко С.В.* Алгоритм шифрования произвольных данных на основе трехмерного аналога хаотического отображения «Кот Арнольда» // Компьютерные науки и информационные технологии: Материалы межд. научной конф. Саратов, Россия, 1-4 июля 2012 г. Саратов: Издат. Центр «Наука», 2012. С. 29-31. ISBN 978-5-9999-1304-3.
17. *Аникин В.М., Ремизов А.С., Самойлов Н.Д.* Схема шифрования на основе произвольного набора пар хаотических отображений // Компьютерные науки и информационные технологии: Материалы межд. научной конф. Саратов, Россия, 1-4 июля 2012 г. Саратов: Издат. Центр «Наука», 2012. С. 31-33. ISBN 978-5-9999-1304-3.
18. *Аграновский А.В., Хади Р.А*. Практическая криптография. М. : СОЛОН-пресс, 2009. 256 с.
19. *Авдошин С.* Дискретная математика. Модулярная алгебра, криптография, кодирование. М.: СИНТЕГ**,** 2016. **260** с.
20. *Адаменко М*. Основы классической криптологии. Секреты шифров и кодов М. : Машиностроение, 2014. 256 с.
21. *Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В*. Основы криптографии. М.: Гелиос АРВ, 2001. 479 с.
22. *Бабаш, А.В., Шанкин Г.П.* Криптография / под. ред. В.П. Шерстюка, Э.А. Применко. М.: СОЛОН-ПРЕСС, 2007. 512 с.
23. *Бауэр Ф.* Расшифрованные секреты. Методы и принципы криптологии. М.: Мир, 2007. 550 с.
24. Баричев, С. Г., Гончаров В.В., Серов Р.Е.. Основы современной криптографии Москва: **СИНТЕГ**, 2011. 176 с.
25. *Василенко О.Н.* Теоретико-числовые алгоритмы в криптографии. Москва, МЦНМО, 2003, 328 с.
26. *Герман, О. Н. Нестеренко Ю.В*. Теоретико-числовые методы в криптографии. М.: Академия, 2012. 272 с.

27. *Земор Ж.* Курс криптографии. М.: Регулярная и хаотическая динамика, Институт компьютерных исследований, 2006. 256 с.
28. *Кудряшов Б.Д.* Основы теории кодирования. СПб : БХВ-Петербург,2016. 400 с.
29. *Мао В.* Современная криптография. Теория и практика. М.: Вильямс, 2005. 763 с.
30. Мир математики. Т.2: Жуан Гомес. Математики, шпионы и хакеры. Кодирование и криптография. М.: Де Агостини, 2014. 144 с.
31. *Панасенко С.П.* Алгоритмы шифрования. Специальный справочник. СПб : БХВ-Петербург,2009. 576 с.
32. *Петров А.А.* Компьютерная безопасность. Криптографические методы защиты. М. : ДМК, 2000. 448 с.
33. *Риксон Фред Б.* Коды, шифры, сигналы и тайная передача информации. М.: АСТ: Астрель, 2011. 656 с.
34. *Сингх С.* Книга шифров. Тайная история шифров и их расшифровки. М.: Аст, Астрель, 2006. 447 с.
35. *Смарт Н.* Криптография. М. : Техносфера, 2005. 528 с.
36. *Фомичев В.М.* Дискретная математика и криптология. М.: ДИАЛОГ-МИФИ, 2003. 400 с.
37. *Черемушкин А. В*. Лекции по арифметическим алгоритмам в криптографии. М.: МЦНМО, 2002. 104 с.
38. Шумский, А.А. Системный анализ в защите информации. Москва: **СПб. : Питер**, 2005. 224 с.
39. Классическая криптография. URL : https://topuch.ru/kolsoderjanie-teoreticheskie-osnovi-kriptografii-9/index2.html#pages (дата обращения 17.05.2021).
40. Стойкость алгоритмов шифрования. https://topuch.ru/kolsoderjanie-teoreticheskie-osnovi-kriptografii-9/index3.html (дата обращения 17.05.2021).
41. Классификация алгоритмов шифрования. URL : https://topuch.ru/kolsoderjanie-teoreticheskie-osnovi-kriptografii-9/index4.html#pages (дата обращения 17.05.2021)
42. Реализация алгоритмов шифрования. URL :https://topuch.ru/kolsoderjanie-teoreticheskie-osnovi-kriptografii-9/index5.html#pages (дата обращения 17.05.2021)/
43. *Аникин В.М., Голубенцев А.Ф.* Аналитические модели детерминированного хаоса. М.: ФИЗМАТЛИТ, 2007. 328 с.
44. *Сикорский Ю.С.* Элементы теории эллиптических функций с приложениями к механике. М.:ОНТИ, 1936. Гл. 1.
45. *Уиттекер Э.Т., Ватсон Дж. Н.* Курс современного анализа. Ч. 2. Трансцендентные функции. М.: ГИФМЛ, 1962. Гл. 1.
46. *Лоскутов А.Ю., Чураев А.А.* Использование хаотических отображений для защиты информации // Вестник Моск. ун-та. Сер. Физика, астрономия. 2008. № 2. С. 15–19.