

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ**

**ВЫСШЕГО ОБРАЗОВАНИЯ**

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ «МИСиС»**



***ИНСТИТУТ***ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОМПЬЮТЕРНЫХ НАУК

***КАФЕДРА*** АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ И ДИЗАЙНА

***НАПРАВЛЕНИЕ*** 09.03.03 ПРИКЛАДНАЯ ИНФОРМАТИКА

***ПРОФИЛЬ*** Прикладная информатика в дизайне

**ОТЧЕТ**

**о выполнении курсовой работы**

**на тему: Разработка программы для шифрования и   
дешифрования информации методом маршрутной перестановки**

| *Студент группы БПИ-20-2* |  | *Панченко Е. А.* |
| --- | --- | --- |
| *Руководитель работы* |  | *ст.преп. Фейзрахманов И.Ж.* |

| *Отчет защищен с оценкой* |  |  |
| --- | --- | --- |

Москва 2022

# **Аннотация**

Данный отчет содержит введение, две главы, заключение, список литературных источников и приложений.

В первой главе работы рассматривается история возникновения шифра перестановки и на примерах объясняется механизм шифрования. Приводится алгоритм действий и блок-схема для шифрования и дешифрования сообщения.

Во второй главе объясняются особенности программной реализации шифрования шифром маршрутной перестановки и приводится серия тестов для отладки программы.

Работа состоит из 26 страниц, содержит 7 литературных источников, 12 рисунков, 2 таблицы и 1 приложение.

**Оглавление**

[**Аннотация** 2](#_heading=h.gjdgxs)

[**ВВЕДЕНИЕ** 4](#_heading=h.30j0zll)

[**Глава 1. Теоретическая часть** 6](#_heading=h.1fob9te)

[1.1 Классификация шифров 6](#_heading=h.3znysh7)

[1.2 История перестановочного шифра 7](#_heading=h.2et92p0)

[1.3 Описание маршрутной перестановки 8](#_heading=h.tyjcwt)

[1.4 Варианты маршрутных перестановок 9](#_heading=h.3dy6vkm)

[1.4.1 Табличная перестановка 9](#_heading=h.1t3h5sf)

[1.4.2 Шифр вертикальной перестановки 10](#_heading=h.4d34og8)

[1.4.3 Шифр перекресток 11](#_heading=h.2s8eyo1)

[1.4.4 Шифр поворотной решетки 12](#_heading=h.17dp8vu)

[1.4.5 Шифры с использованием магических квадратов 13](#_heading=h.3rdcrjn)

[**Глава 2. Практическая часть** 15](#_heading=h.26in1rg)

[2.1 Программная реализация 15](#_heading=h.lnxbz9)

[2.2 Алгоритм 17](#_heading=h.35nkun2)

[2.3 Тестирование 20](#_heading=h.1ksv4uv)

[**ЗАКЛЮЧЕНИЕ** 23](#_heading=h.44sinio)

[**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ** 24](#_heading=h.2jxsxqh)

[**ПРИЛОЖЕНИЯ** 25](#_heading=h.z337ya)

[Приложение А 25](#_heading=h.3j2qqm3)

# **ВВЕДЕНИЕ**

Широкое использование информационных технологий во всех сферах жизни современного общества делает вполне закономерной и весьма актуальной проблему защиты информации, или иначе, проблему обеспечения информационной безопасности.

В условиях интенсивного развития рынка информационных продуктов и услуг информация становится полноценным товаром, обладающим своими стоимостными характеристиками и потребительскими свойствами. Подобно любым другим традиционно существующим товарам, информация также нуждается в своей сохранности и, следовательно, надежной защите.

Понятие «безопасность» охватывает широкий круг интересов как отдельных лиц, так и целых государств. Во все исторические времена существенное внимание уделялось проблеме информационной безопасности, обеспечению защиты конфиденциальной информации от ознакомления с ней конкурирующих групп.

Криптографические методы занимают особое место среди прочих методов защиты информации, так как опираются исключительно на свойства самой информации без свойств ее носителей.

Современные методы криптографии, в частности, шифр маршрутной перестановки, в той или иной мере отвечают ряду предъявляемых к ним требований, а именно:

* достаточной криптостойкости, то есть стойкости к несанкционированному дешифрованию;
* простоте процедур шифрования и дешифрования;
* незначительной избыточности информации в результате преобразований.

**Актуальность данной работы.** Тема данной работы актуальна в настоящее время. Это объясняется тем, что большинство людей в разных сферах деятельности сталкиваются с проблемой шифрования своих персональных данных или же крупная компания сталкивается с проблемой шифрования данных на своих серверах, что несёт за собой кражу, потерю и раскрытия информации, которой умело воспользуются злоумышленники. И чтобы сохранить свои данные им необходим эффективный метод шифрования в сфере защиты информации.

**Объектом исследования** является информатика.

**Предметом исследования** является шифрование информации.

**Целью** работыявляетсяразработка программы для шифрования и   
дешифрования информации методом маршрутной перестановки.

Для успешного выполнения поставленной цели необходимо выполнить следующиезадачи**:**

* Анализ теории и практики в шифровании информации;
* Анализ существующих методов шифрования;
* Обоснование выбора метода шифрования;
* Обоснование выбора языка программирования для реализации программы;
* Создание программы шифрования и дешифрования информации методом маршрутной перестановки.

# **Глава 1. Теоретическая часть**

## 1.1 Классификация шифров

Эффективным средством противодействия различным угрозам информационной безопасности является использование методов криптографического преобразования. Эти преобразования защищают информацию от лиц, не имеющих соответствующих полномочий, Криптографические преобразования связаны с шифрованием и дешифрованием информации.

При шифровании каждый символ защищаемого сообщения подвергается обратимым математическим, логическим, комбинаторным или иным преобразованиям.

Существующие методы шифрования могут быть классифицированы по различным признакам. На рисунке 1 представлена структура методов шифрования.

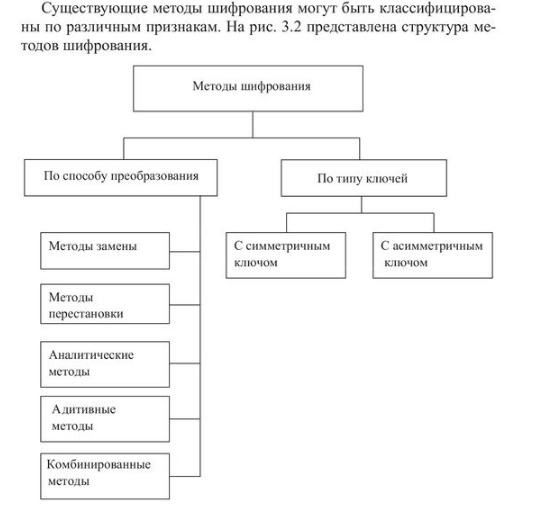


Рисунок 1 — Структура методов шифрования

Методы могут быть подразделены на методы с симметричным и асимметричным ключами. При шифровании с симметричным ключом используется один секретный ключ для шифрования и расшифровки при обратимости шифропреобразования. Ключ передается отдельно от отправителя к получателю. Скорость обмена большая, но надежность не очень высока. Асимметричное шифрование более надежное, но более сложное. В этом случае используются разные ключи для шифрования и расшифровки. При этом нет необходимости передавать ключ получателю. Процедура дешифрования занимает больше времени.

## 1.2 История перестановочного шифра

Доподлинно не известно, когда появился шифр перестановки, но вполне возможно, что писцы в древности переставляли буквы в имени своего царя ради того, чтобы скрыть его подлинное имя или в ритуальных целях.

Одним из первых физических приборов, реализующих шифр перестановки, является так называемый прибор Сцитала (рисунок 2).



Рисунок 2 — Сцитала

Он был изобретён в древней «варварской» Спарте во времена Ликурга (V в. до н. э.). Рим быстро воспользовался этим прибором. Для зашифрования текста использовался цилиндр заранее обусловленного диаметра. На цилиндр наматывался тонкий ремень из пергамента, и текст выписывался построчно по образующей цилиндра (вдоль его оси). Затем ремень сматывался и отправлялся получателю сообщения. Последний наматывал его на цилиндр того же диаметра и читал текст по оси цилиндра. В этом примере ключом шифра являлся диаметр цилиндра и его длина, которые, по существу, порождают двухстрочную запись, аналогичную указанной выше. Шифр «Сцитала» реализует один из вариантов так называемого сегодня «шифра маршрутной перестановки».

Типичным примером перестановки являются анаграммы, ставшие популярными в XVII в. Анаграмма (греч. ανα - «снова» и γράμμα - «запись») - литературный приём, состоящий в перестановке букв или звуков определённого слова (или словосочетания), что в результате даёт другое слово или словосочетание. Например: апельсин - спаниель, полковник - клоповник, горилка - рогалик, лепесток - телескоп.

Разновидностью маршрутного шифра был маршрутный шифр Союза, используемый силами Союза во время гражданской войны в США. Это работало во многом как обычный маршрутный шифр, но транспонировало целые слова вместо отдельных букв. Поскольку это оставило бы открытыми некоторые важные слова, такие слова сначала были бы скрыты кодом.

Шифровальщик мог также добавлять целые нулевые слова, которые часто выбирались для придания зашифрованному тексту юмористического характера.

## 1.3 Описание маршрутной перестановки

Для получения варианта перестановки часто используется некоторая геометрическая фигура, составленная из клеток (чаще всего прямоугольники различных размеров). Шифрование состоит в том, что исходный текст в клетки фигуры вписывают по ходу одного маршрута, а затем для получения шифротекста из заполненной символами фигуры выписывают символы по ходу другого маршрута. Такой шифр называется шифром маршрутной перестановкой.

Ключом для такого шифра будет описание фигуры и двух маршрутов (шифрования и дешифрации). Важно чтобы оба маршрута содержали без повторений все клетки фигуры. Геометрическая фигура не обязательно должна быть плоской.

Как и все шифры перестановки для маршрутной перестановки существует n! вариантов перестановок степени n (в это число входит и вариант, в котором первая и вторая строка таблицы перестановок полностью совпадают).

Таким образом, шифры перестановки предназначен для шифрования исходных текстов длиной n, у которого в качестве множества ключей берется множество всех перестановок степени n. Число ключей этого шифра равно n! Для использования на практике шифры перестановки неудобен в связи с необходимостью при больших значениях n работать с большими таблицами.

**1.4 Варианты маршрутных перестановок**

### 1.4.1 Табличная перестановка

Наибольшее распространение получили шифры маршрутной перестановки, основанные на таблицах. При шифровании в такую таблицу вписывают исходное сообщение по определенному маршруту, а выписывают (получают шифрограмму) - по-другому. Для данного шифра маршруты вписывания и выписывания, а также размеры таблицы являются ключом.

Например, исходное сообщения «пример маршрутной перестановки» вписывается в прямоугольную таблицу размерами 4х7, по горизонтали, начиная с левого верхнего угла поочередно слева направо и справа налево.

|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | п | р | и | м | е | р | м |
| 2 | н | т | у | р | ш | р | а |
| 3 | о | й | п | е | р | е | с |
| 4 | и | к | в | о | н | а | т |

Таблица 1 — пример таблицы для табличной маршрутной перестановки

Для шифрования сообщение будем считывать по другому маршруту: по вертикали, начиная с правого верхнего угла и двигаясь поочередно сверху вниз и снизу вверх. Шифрограмма в этом случае выглядит «мастаеррешрноермиупвкйтрпнои».

### 1.4.2 **Шифр вертикальной перестановки**

Распространенной разновидностью шифра маршрутной перестановки является шифр вертикальной перестановки. В нем в качестве геометрической фигуры используют прямоугольную таблицу размера m х k, в который исходный текст вписывают построчно слева направо (или – 1-я строка – слева направо, 2-я строка – справа налево и т.д.). Для получения шифротекста считывание таблицы выполняют по столбцам, причем порядок считывания столбцов обусловлен ключом. Число таких ключей не превышает k!, где k – число столбцов прямоугольника. Ключ представляет собой некоторую последовательность из k неповторяющихся чисел, которую для простоты запоминания можно получить из легко запоминаемого слова или фразы.

Существует много способов получения ключа из фразы. Наиболее простой – приписать каждой букве слова (или фразы) ее порядковый номер в алфавите естественного языка (повторяющиеся буквы в цифровую последовательность включить один раз после первого появления), а затем первым k1 числам этой последовательности поставить в соответствие k первых чисел натурального ряда, например по следующему принципу: наименьшему из чисел последовательности k1 – 1, следующему за ним – 2 и т.д., наибольшему – k. В результате таких действий образуется один из вариантов перестановки степени k(ключ), который определит порядок считывания столбцов для получения шифротекста, порядок заполнения столбцов при дешифрации, и который легко запомнить.

Для обеспечения дополнительной секретности можно повторно зашифровать полученный шифротекст перестановкой строк. Такой метод шифрования называют двойной перестановкой. В этом случае для восстановления исходного текста понадобится два ключа и обратная последовательность действий: на первом этапе восстанавливают порядок строк, затем в полученной таблице восстанавливают порядок столбцов и только после этого построчно считывают исходный текст. Число ключей в случае двойной перестановки составляет T = m!k!, а длина исходного текста составит n = mk. Число всех перестановок в тексте такой длины составит (mk)!, что существенно больше числа ключей T.

Пример сообщение «ПРИМЕР МАРШРУТНОЙ ПЕРЕСТАНОВКИ» с ключом «31425» может выглядеть представленной таблицей 2.

| 3 | 1 | 4 | 2 | 5 |
| --- | --- | --- | --- | --- |
| П | Р | И | М | Е |
| Р | М | А | Р | Ш |
| Р | У | Т | Н | О |
| Й | П | Е | Р | Е |
| С | Т | А | Н | О |
| В | К | И |  |  |

Таблица 2 — пример вертикальной перестановки

В этом случае криптограммой является «рмупткмрнрнпррйсвиатеаиешоео».

### 1.4.3 Шифр перекресток

Для перемешивания букв могут использоваться фигуры специального вида. Один из таких способов носит название «перекресток». В приведенном ниже примере рисуют крестообразные фигуры в количестве, достаточном, чтобы разместить в них все буквы сообщения. Открытый текст записывают вокруг этих фигур заранее оговоренным способом - в нашем случае по часовой стрелке.

Таким образом, сообщение «ПРИМЕР ПЕРЕСТАНОВКИ» может выглядеть следующим образом:

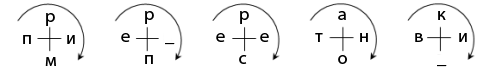


Рисунок 3 — Пример размещения открытого текста в шифре «Перекресток»

Например, шифрограмма будет выглядеть «РРРАКПИЕ\_ЕЕТНВИМПСО\_».

### **1.4.4 Шифр поворотной решетки**

В 1550 г. итальянский математик Джероламо Кардано, состоящий на службе у папы Римского, в книге «О тонкостях» предложил новую технику шифрования - решётку Кардано. Изначально решетка Кардано представляла собой трафарет с прорезанными в нем отверстиями. В этих отверстиях на листе бумаги, который клали под решетку, записывались буквы, слоги и слова сообщения. Далее трафарет снимался, и свободное пространство заполнялось более или менее осмысленным текстом для маскировки секретного послания. Такой метод сокрытия информации относится к стеганографии. Позднее был предложен шифр «поворотная решетка» или, как его еще называют, «решетка для вьющихся растений», поскольку она напоминала отверстия в деревянных решетках садовых строений. Этот шифр считают первым транспозиционным (геометрическим) шифром.

Для шифрования и дешифрования с помощью данного шифра изготовляется прямоугольный трафарет с четным количеством строк и столбцов. В трафарете вырезаются клетки таким образом, чтобы при наложении его на таблицу того же размера четырьмя возможными способами, его вырезы полностью покрывали все ячейки таблицы ровно по одному разу.

При шифровании трафарет накладывается на таблицу. В видимые ячейки таблицы выписываются буквы исходного текста слева-направо сверху-вниз. Далее трафарет поворачивается и вписывается следующая часть букв. Эта операция повторяется еще два раза. Шифрограмму выписывают из итоговой таблицы по определенному маршруту. Таким образом, ключом при шифровании является трафарет, порядок его поворотов и маршрут выписывания.

### 1.4.5 Шифры с использованием магических квадратов

Магическими квадратами называются квадратные таблицы со вписанными в их ячейки последовательными натуральными числами начиная с 1, которые в сумме по каждому столбцу, каждой строке и главным диагоналям дают одно и то же число. Впервые эти квадраты появились в Китае, где им и была приписана некоторая «магическая сила». По преданию, описанному в одной из пяти канонических книг Древнего Китая - Шу-Цзин (Книге записанных преданий), в 2200 году до н.э. из реки Ло вышла огромная черепаха (по другой версии - дракон), символ вечности. На ее панцире были видны пятна, образовавшиеся удивительный рисунок. (рисунок 4)

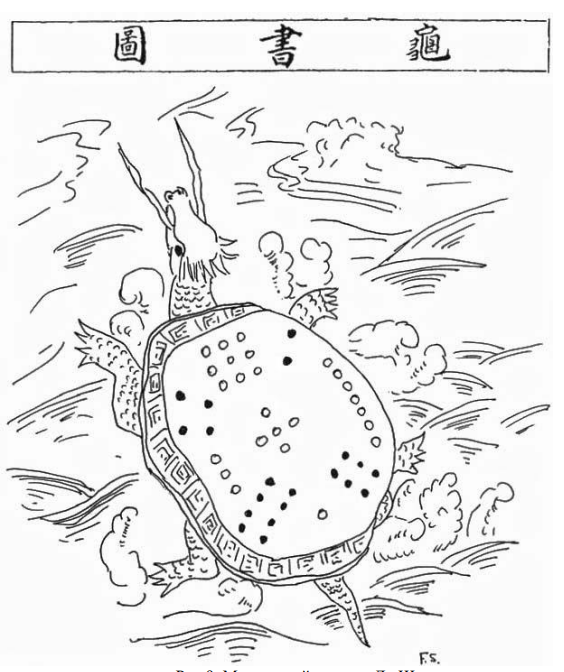


Рисунок 4 — Магический квадрат Ло Шу

Магические квадраты широко применялись для передачи секретной информации. При шифровании исходное сообщение вписывалось в квадрат по приведенной в них нумерации, после чего шифрограмма выписывалась по строкам. Количество возможных магических квадратов (ключей) быстро возрастает с увеличением их размера. Так, существует лишь один магический квадрат размером 3х3, если не принимать во внимание его повороты. Магических квадратов 4х4 насчитывается уже 880, а число магических квадратов размером 5х5 около 250000.

Поэтому магические квадраты больших размеров могли быть хорошей основой для надежной системы шифрования того времени, потому что ручной перебор всех вариантов ключа для этого шифра был немыслим.

# **Глава 2. Практическая часть**

## 2.1 Программная реализация

В данной работе реализован шифр табличной маршрутной перестановки.

Сама программа реализована на языке C#, в качестве среды разработки использовалась среда Visual Studio 2022. Полный код программы приведён в Приложении А.

Основным языком программированием был выбран C# (си-шарп), который является объектно-ориентированный языком программирования. C# относится к семье языков с C-подобным синтаксисом, из них его синтаксис наиболее близок к C++ и Java.

Для создания графического интерфейса с помощью платформы .NET использована технология Windows Forms.

Windows Forms – это платформа пользовательского интерфейса для создания классических приложений Windows. Она обеспечивает один из самых эффективных способов создания классических приложений с помощью визуального конструктора в Visual Studio.

В приложении использованы стандартные элементы управления: Button, TextBox. У одного из TextBox включен параметр ReadOnly для исключения возможности редактирования.

Функционал и интерфейс программы представлен на рисунках 5 и 6.

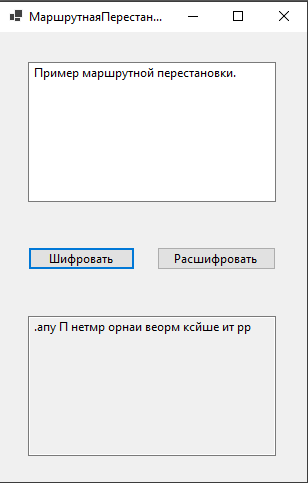


Рисунок 5 — вывод зашифрованного текста

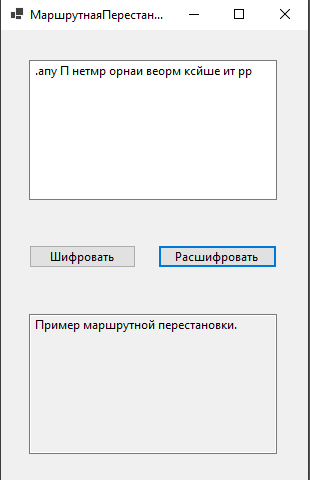


Рисунок 6 — вывод расшифрованного текста

### 2.2 Алгоритм

Алгоритм работы программы приведён в виде блок-схемы на рисунках 7 и 8. В алгоритме программы отдельно вынесено две подпрограммы – подпрограмма для шифрования данных и подпрограмма для расшифровки полученного сообщения.

Входными данными являются текст записанный в первый TextBox.

После нажатия кнопки шифровать вычисляется количество столбцов и строк матрицы. Символы записываются слева направо сначала каждой строке, если их меньше, чем столбцов матрица дополняется пробелами.

Для шифрования матрица выводится с левого нижнего края вверх для каждого столбца.

Для расшифровывания с матрица производятся те же действия, только двумерный массив выписывается и заполняется в обратной последовательности.

Выходными данными является, выводимая на экран, зашифрованная или же расшифрованная информация в пользовательском интерфейсе программы.

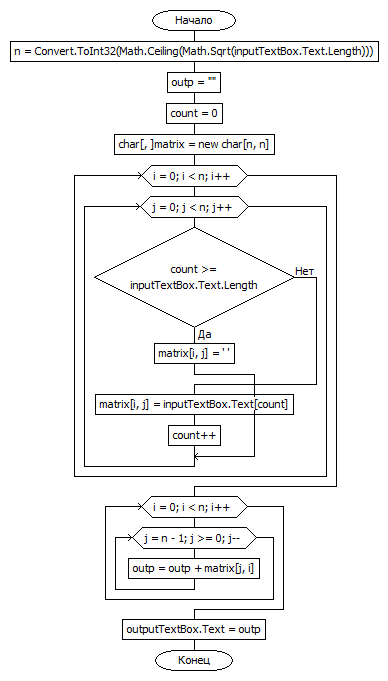


Рисунок 7 — блок-схема шифрования текста

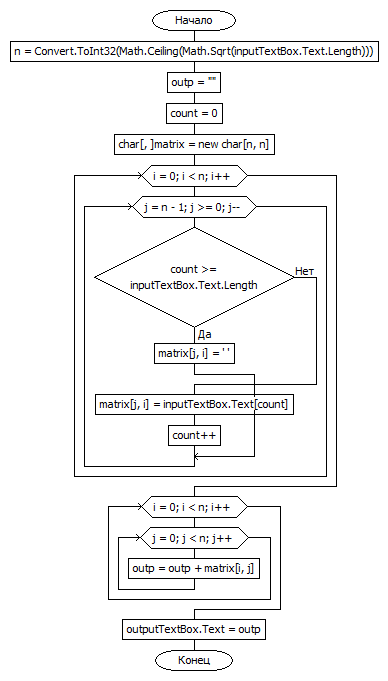


Рисунок 8 — блок-схема расшифрования текста

## 2.3 Тестирование

В проведении испытаний главную роль играла отладка – это процесс, при котором код пошагово выполняется в некой программе в компиляторе Microsoft Visual Studio. В процессе выполнения режима отладки идет поиск точек, где могли быть допущены ошибки.

На представленных ниже рисунках 9-12 представлено тестирование программы на нескольких разных тестах.

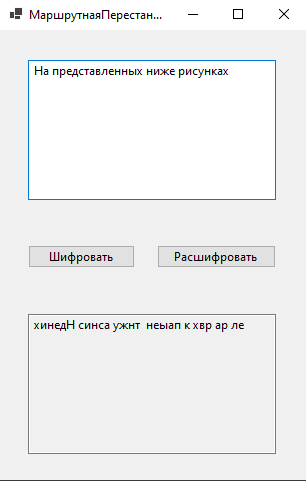


Рисунок 9 — тест шифрования текста

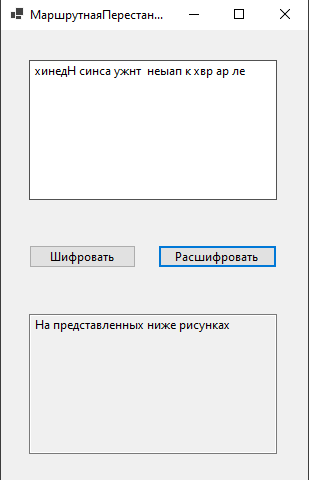


Рисунок 10 — тест расшифрования текста

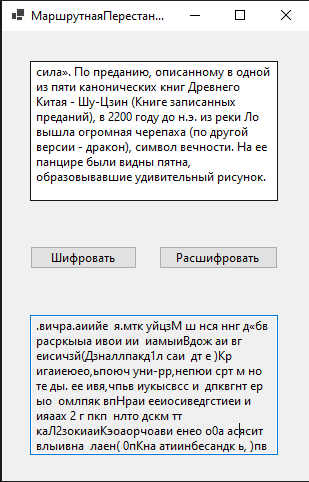


Рисунок 11 — тест шифрования длинного текста

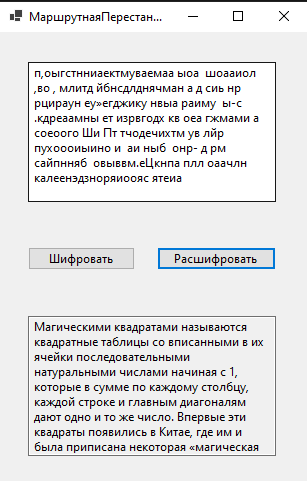


Рисунок 12 — тест расшифрования длинного текста

При вызове программы с незаполненным полем программа не реагирует на нажатие кнопок.

Таким образом, программа прошла серию из 3 тестов, трижды зашифровала и расшифровала пользовательское сообщение. В процессе тестирования ошибок в алгоритмах шифрования не выявлено.

# **ЗАКЛЮЧЕНИЕ**

В данной курсовой работе был изучен метод шифрования, основанный на использовании маршрутной перестановки, а также написана программа на языке программирования C#, которая использует данный алгоритм.

Для достижения поставленной цели был проведён анализ возможностей и особенностей данного метода шифрования, а также похожих на него вариантов методов шифрования, был создан алгоритм и расписан принцип работы программы, по которому был написан код программы и создан для неё визуальный интерфейс.

Цель, поставленная в начале работы, достигнута, все задачи выполнены.

# **СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черёмушкин. Основы криптографии. — Гелиос АРВ, 2002. — ISBN 5-85438-137-0.
2. А. В. Бабаш, Г. П. Шанкин. Криптография. — М. СОЛОН-ПРЕСС, 2007. — ISBN 5-93455-135-3.
3. Костин В.Н. Методы и средства защиты компьютерной информации: Криптографические методы для защиты информации. – НИТУ «МИСиС» - ISBH 978-5-90695-334-6
4. Руководство по классическим приложениям (Windows Forms .NET) [Электронный ресурс]. – https://learn.microsoft.com/ru-ru/dotnet/desktop/winforms/overview/?view=netdesktop-5.0 (дата обращения 11.12.2022).
5. Учебная и научная деятельность Анасимова Владимира Викторовича – Шифры перестановки [Электронный ресурс].-<https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema5#shifr_POP> (дата обращения 11.12.2022)
6. Семененко В.А. Информационная безопасность: Учебное пособие, 4-е изд., стереотир. - М.: МГИУ,2010 – ISBN 978-5-2760-1876-8
7. Руководство по программированию в Windows Forms и C# [Электронный ресурс].- <https://metanit.com/sharp/windowsforms/> (дата обращения 11.12.2022)

# **ПРИЛОЖЕНИЯ**

## Приложение А

Основным кодом программы является текст, написанный на языке программирования C#(листинг 1), помимо него в программе также имеются строки кода, которые генерируются автоматически и отвечают за дизайн и оформление меню программы.

Листинг 1 – Код программы

namespace RouteChiper

{

public partial class Form1 : Form

{

public Form1()

{

InitializeComponent();

}

private void button1\_Click(object sender, EventArgs e)

{

int n = Convert.ToInt32(Math.Ceiling(Math.Sqrt(inputTextBox.Text.Length)));

string outp = "";

int count = 0;

char[,] matrix = new char[n, n];

for (int i = 0; i < n; i++)

{

for (int j = 0; j < n; j++)

{

if (count >= inputTextBox.Text.Length)

{

matrix[i, j] = ' ';

continue;

}

matrix[i, j] = inputTextBox.Text[count];

count++;

}

}

for (int i = 0; i < n; i++)

{

for (int j = n - 1; j >= 0; j--)

{

outp = outp + matrix[j, i];

}

}

outputTextBox.Text = outp;

}

private void button2\_Click(object sender, EventArgs e)

{

int n = Convert.ToInt32(Math.Ceiling(Math.Sqrt(inputTextBox.Text.Length)));

string outp = "";

int count = 0;

char[,] matrix = new char[n, n];

for (int i = 0; i < n; i++)

{

for (int j = n - 1; j >= 0; j--)

{

if (count >= inputTextBox.Text.Length)

{

matrix[j, i] = ' ';

continue;

}

matrix[j, i] = inputTextBox.Text[count];

count++;

}

}

for (int i = 0; i < n; i++)

{

for (int j = 0; j < n; j++)

{

outp = outp + matrix[i, j];

}

}

outputTextBox.Text = outp;

}

}

}