Федеральное государственное автономное

образовательное учреждение

высшего профессионального образования

«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

институт

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

кафедра

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

тема

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Шифр маршрутной перестановки\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Преподаватель \_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

подпись, дата инициалы, фамилия

Студент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

номер группы, зачетной книжки подпись, дата инициалы, фамилия

# Оглавление

[1. Оглавление 2](#_Toc416004380)

[2. Задание 3](#_Toc416004381)

[3. Описание алгоритма 4](#_Toc416004382)

[Блок-схемы алгоритмов шифрования и дешифрования 6](#_Toc416004383)

[Блок-схема алгоритма шифрования 6](#_Toc416004384)

[Блок-схема алгоритма дешифрования 6](#_Toc416004385)

[4. Листинг программы, реализующей алгоритмы 7](#_Toc416004386)

[Интерфейс ICryptography 7](#_Toc416004387)

[Класс VerticalCryptography 7](#_Toc416004388)

[Класс VerticalForm 8](#_Toc416004389)

[Юнит-тест 9](#_Toc416004390)

[Графический интерфейс программы 10](#_Toc416004391)

[5. Контрольные примеры работы программы 11](#_Toc416004392)

[Шифр маршрутной перестановки 11](#_Toc416004393)

[6. Модификация алгоритма 16](#_Toc416004394)

[Доказательство увеличения криптографической стойкости при модификации алгоритма 16](#_Toc416004395)

[Блок-схемы модифицированных алгоритмов шифрования и дешифрования 17](#_Toc416004396)

[Блок-схема модифицированного алгоритма шифрования 17](#_Toc416004397)

[Блок-схема модифицированного алгоритма дешифрования 18](#_Toc416004398)

[7. Листинг программы, реализующей модифицированные алгоритмы 19](#_Toc416004399)

[Класс Vertical3Cryptography 19](#_Toc416004400)

[Юнит-тест 20](#_Toc416004401)

[8. Контрольные примеры работы модифицированной программы 21](#_Toc416004402)

[Тройной шифр маршрутной перестановки 21](#_Toc416004403)

[9. Заключение 26](#_Toc416004404)

# Задание

* Разработать и составить в виде блок-схемы алгоритмы шифрования и дешифрования текста на основе шифра маршрутной перестановки. Убедиться в правильности составления алгоритмов и затем на языке программирования C# составить программу, которая реализует данные алгоритмы.
* На ряде контрольных примеров открытого текста, состоящего из различного количества текста, убедиться в правильности работы алгоритмов шифрования и дешифрования.
* Самостоятельно придумать оригинальный способ модификации шифра с целью повышения его криптостойкости. Внести изменения в исходный алгоритм и программу. Проверить работоспособность алгоритма на тестовых примерах.
* Доказать, что предложенный способ модификации действительно повышает криптостокость.

# Описание алгоритма

Шифр, преобразования из которого изменяют только порядок следования символов исходного текста, но не изменяют их самих, называется [шифром перестановки (ШП)](http://citforum.ru/security/cryptography/yaschenko/8.html#inner:{IFRY_PERESTANOWKI).

Зная подстановку, задающую преобразование, можно осуществить как зашифрование, так и расшифрование текста.

Широкое распространение получили шифры перестановки, использующие некоторую геометрическую фигуру. Преобразования из этого шифра состоят в том, что в фигуру исходный текст вписывается по ходу одного ``маршрута'', а затем по ходу другого выписывается с нее. Такой шифр называют маршрутной перестановкой. Например, можно вписывать исходное сообщение в прямоугольную таблицу, выбрав такой маршрут: по горизонтали, начиная с левого верхнего угла поочередно слева направо и справа налево. Выписывать же сообщение будем по другому маршруту: по вертикали, начиная с верхнего правого угла и двигаясь поочередно сверху вниз и снизу вверх.

Зашифруем, например, указанным способом фразу:

|  |
| --- |
| ПРИМЕРМАРШРУТНОЙПЕРЕСТАНОВКИ |

используя прямоугольник размера 4x7:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| П | Р | И | М | Е | Р | М |
| Н | Т | У | Р | Ш | Р | А |
| О | Й | П | Е | Р | Е | С |
| И | К | В | О | Н | А | Т |

Зашифрованная фраза выглядит так:

|  |
| --- |
| МАСТАЕРРЕШРНОЕРМИУПВКЙТРПНОИ |

Теоретически маршруты могут быть значительно более изощренными, однако запутанность маршрутов усложняет использование таких шифров.

## Блок-схемы алгоритмов шифрования и дешифрования

### Блок-схема алгоритма шифрования

Открытый текст

Ключ

Ширина таблицы m

Запись в таблицу по маршруту 1

Чтение из таблицы по маршруту 2

Закрытый текст

Открытый текст

Запись по маршруту 1

Таблица ширины m

Считывание по маршруту 2

Закрытый текст

### Блок-схема алгоритма дешифрования

Закрытый текст

Ключ

Ширина таблицы m

Запись в таблицу по маршруту 2

Чтение из таблицы по маршруту 1

Открытый текст

Таблица ширины m

Запись по маршруту 2

Закрытый текст

Считывание по маршруту 1

Открытый текст

# Листинг программы, реализующей алгоритмы

Программа разработана с использованием технологий ООП и инкапсуляцией алгоритмов шифратора в объекте класса RouteCryptography.

## Интерфейс ICryptography

namespace Route

{

/// <summary>

/// Интерфейс поточного текстового шифратора

/// </summary>

public interface ICryptography

{

void SetKey(string keyText);

void ClearKey();

string EncryptNext(string plainText);

string DecryptNext(string cipherText);

}

}

## Класс RouteCryptography

using System;

using System.Text;

namespace Route

{

/// <summary>

/// Шифр маршрутной перестановки

/// </summary>

public class RouteCryptography : ICryptography

{

private const char LastChar = '>';

private int \_key;

/// <summary>

/// Процедура шифрования блока текста

/// </summary>

/// <param name="plainText">Исходный текст</param>

/// <returns>Шифрованный текст</returns>

public string EncryptNext(string plainText)

{

if (\_key == 0) throw new WrongKeyException();

int cols = \_key;

int rows = (plainText.Length + cols - 1)/cols;

var table = new char[rows, cols];

int index = 0;

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

if (i%2 == 0)

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

table[i, j] = (index < plainText.Length) ? plainText[index++] : LastChar;

else

for (int j = cols; j-- > 0;)

table[i, j] = (index < plainText.Length) ? plainText[index++] : LastChar;

var sb = new StringBuilder();

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

if (j%2 == 0)

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

sb.Append(table[i, j]);

else

for (int i = rows; i-- > 0;)

sb.Append(table[i, j]);

return sb.ToString().TrimEnd(new[] {LastChar});

}

/// <summary>

/// Процедура расшифрования блока текста

/// </summary>

/// <param name="cipherText">Шифрованный текст</param>

/// <returns>Исходный текст</returns>

public string DecryptNext(string cipherText)

{

if (\_key == 0) throw new WrongKeyException();

int cols = \_key;

int rows = (cipherText.Length + cols - 1)/cols;

var table = new char[rows, cols];

int index = 0;

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

if (j%2 == 0)

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

table[i, j] = (index < cipherText.Length) ? cipherText[index++] : LastChar;

else

for (int i = rows; i-- > 0;)

table[i, j] = (index < cipherText.Length) ? cipherText[index++] : LastChar;

var sb = new StringBuilder();

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

if (i%2 == 0)

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

sb.Append(table[i, j]);

else

for (int j = cols; j-- > 0;)

sb.Append(table[i, j]);

return sb.ToString().TrimEnd(new[] {LastChar});

}

/// <summary>

/// Ввод ключа и сброс счётчика тактов

/// </summary>

/// <param name="keyText">ширина таблицы</param>

public void SetKey(string keyText)

{

int key = Convert.ToInt32(keyText);

if (key < 2) throw new WrongKeyException();

\_key = key;

}

/// <summary>

/// Сброс ключа и сброс счётчика тактов

/// </summary>

public void ClearKey()

{

\_key = 0;

}

public class WrongKeyException : Exception

{

}

}

}

## Класс RouteForm

using System;

using System.Windows.Forms;

namespace Route

{

public partial class RouteForm : Form

{

public RouteForm()

{

InitializeComponent();

}

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

{

try

{

ICryptography cryptography = encryptTriple.Checked

? new Route3Cryptography()

: (ICryptography) new RouteCryptography();

cryptography.SetKey(encryptKey.Text);

encryptDest.Text = cryptography.EncryptNext(encryptSource.Text);

}

catch (RouteCryptography.WrongKeyException)

{

MessageBox.Show(@"Неправильный ключ");

}

}

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

{

try

{

ICryptography cryptography = decryptTriple.Checked

? new Route3Cryptography()

: (ICryptography) new RouteCryptography();

cryptography.SetKey(decryptKey.Text);

decryptDest.Text = cryptography.DecryptNext(decryptSource.Text);

}

catch (RouteCryptography.WrongKeyException)

{

MessageBox.Show(@"Неправильный ключ");

}

}

}

}

## Юнит-тест

[TestMethod]

public void TestMethod1()

{

try

{

Console.WriteLine(@"Шифр маршрутной перестановки");

Console.WriteLine();

var cryptography = new RouteCryptography();

for (int i = 0; i < 20; i++)

{

string key = (5 + rnd.Next()%10).ToString();

string text = \_texts[i%\_texts.Length];

Console.WriteLine(@"Тест #: " + i);

Console.WriteLine(@"Ключ: " + key);

Console.WriteLine(@"Исходный текст: " + text);

cryptography.SetKey(key);

string cipher = cryptography.EncryptNext(text);

Console.WriteLine(@"Шифрованный текст: " + cipher);

string plain = cryptography.DecryptNext(cipher);

Console.WriteLine(@"Расшифрованный текст: " + plain);

Assert.IsTrue(string.Compare(text, cipher) != 0);

Assert.IsTrue(string.Compare(text, plain) == 0);

Console.WriteLine();

}

}

catch (RouteCryptography.WrongKeyException)

{

Console.WriteLine(@"Неправильный ключ");

Assert.IsTrue(false);

}

catch (Exception)

{

Assert.IsTrue(false);

}

}

## Графический интерфейс программы

Рисунок 1 Режим шифрования

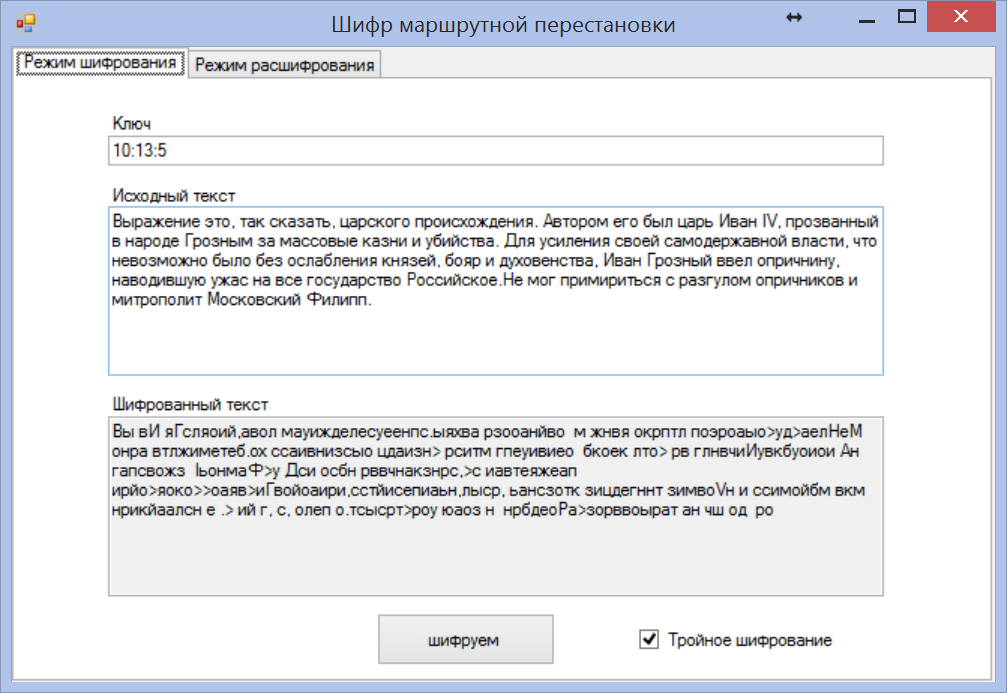
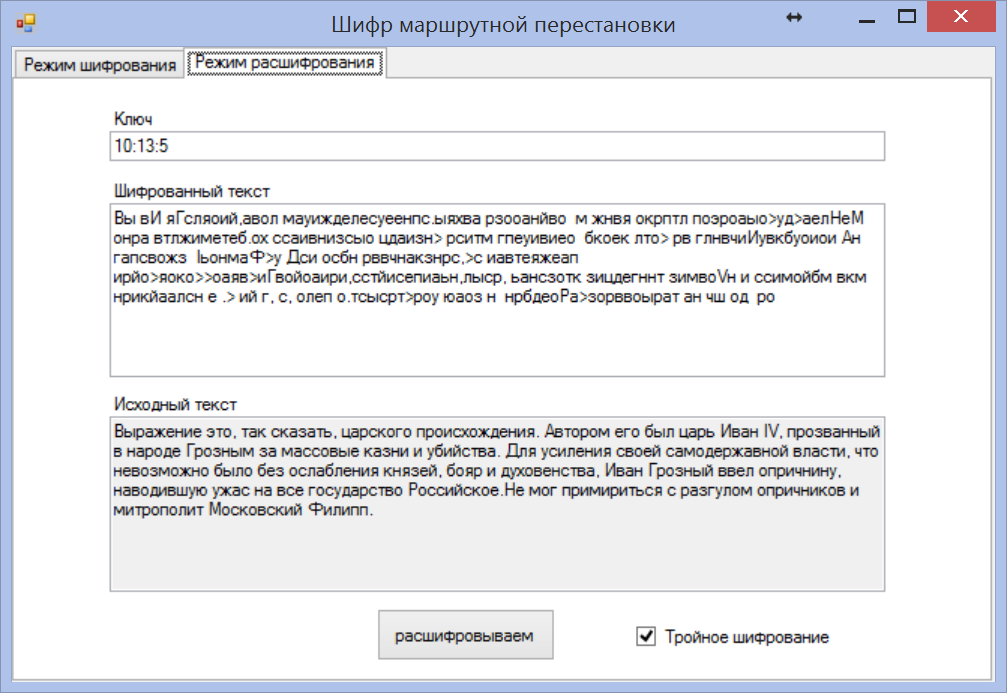


Рисунок 2 Режим расшифрования



# Контрольные примеры работы программы

### Шифр маршрутной перестановки

Тест #: 0

Ключ: 5

Исходный текст: Так в 1923 году В. И. Ленин озаглавил свою замечательную статью о мерах, которые необходимо было принять для укрепления и улучшения советского государственного аппарата. Слова эти оказались столь многозначительными и вескими, были так удачно найдены, что скоро из простого заглавия превратились в настоящее крылатое слово со значением: качество может быть важнее количества.

Шифрованный текст: Т3 И.завотеатахе моинук иияогрс а С о сгоьнски но, о огияилстылвоенест нествеежбетчич оароаит вотирчы чтлиеылзотькил.потаок н яр яр ины,рьтлаюсго г2ак9о.Л л чьсюе редбптяеиуесс двгпаотасоннемвмыааннтозс апасняктлсаеавжыа ча.иквтоокмносо щ ьррлзо коеадкби итамлизэвтаоеугтошлнпль ыооокм незланеВд1 в у нивиамуюо отбхло длеучвеосннраа аль чи и, уйд спрагев веее з: мь ол

Расшифрованный текст: Так в 1923 году В. И. Ленин озаглавил свою замечательную статью о мерах, которые необходимо было принять для укрепления и улучшения советского государственного аппарата. Слова эти оказались столь многозначительными и вескими, были так удачно найдены, что скоро из простого заглавия превратились в настоящее крылатое слово со значением: качество может быть важнее количества.

Тест #: 1

Ключ: 5

Исходный текст: В огромных старорусских семьях было принято, чтобы их члены чередовались понедельно на домашних работах: эту неделю Федор колет дрова, Иван таскает воду, следующую - наоборот. Так же поочередно мололи муку на домашнем жернове: очень нелегкая работа. Болтунам же, отлынивавшим от всякого труда, говорили с насмешкой: "Мели, Емеля, твоя неделя!" - играя на том, что выражение "языком молоть" комически сопоставлялось тут именно с представлением о самой тяжелой работе на жернове.

Шифрованный текст: Вх скх няы числьмаотнеорро тодющбо жеди доереная Бжевавсудилешли тляая ченом к сялимреией раже>>р б томндпе олоио" кижт, р!ев,,екмираря ви, о. кьчнжм млнрекроуууванвд дд абшонеьлеыибтибяиссы онтухьыроохнра доднахуеек аас ,дюаоа еооуаа оо гралм ншткт,о соМ яод"гнмоаеымьмкпвстн се мяйоан>.онтожаолтснуьаоситоз р оаи еялЕ"йасв ооиыоаттаен вмшнкл чпТтн е ткв,тоФлт:ри епвее т,плм рамгроросео ччлдооннах эю ле Иаесл- . оомоу нее:елбоунтлм гого н: ме н- твы"ялочест то ав селе ве

Расшифрованный текст: В огромных старорусских семьях было принято, чтобы их члены чередовались понедельно на домашних работах: эту неделю Федор колет дрова, Иван таскает воду, следующую - наоборот. Так же поочередно мололи муку на домашнем жернове: очень нелегкая работа. Болтунам же, отлынивавшим от всякого труда, говорили с насмешкой: "Мели, Емеля, твоя неделя!" - играя на том, что выражение "языком молоть" комически сопоставлялось тут именно с представлением о самой тяжелой работе на жернове.

Тест #: 2

Ключ: 10

Исходный текст: Выражение это, так сказать, царского происхождения. Автором его был царь Иван IV, прозванный в народе Грозным за массовые казни и убийства. Для усиления своей самодержавной власти, что невозможно было без ослабления князей, бояр и духовенства, Иван Грозный ввел опричнину, наводившую ужас на все государство Российское.Не мог примириться с разгулом опричников и митрополит Московский Филипп.

Шифрованный текст: Вскои еV,деые Дса, о зетвелвшудНе р иск>>ив вас .асуи васйяблчим л. в о Iгмсра ыркзпхоо прГокаяйоттыен,н,водюорем зомой>> кикгяоосг оп е кзбосде васрарн ро ааажттожобаоносзтуоеа бвИйрву ткгсуитсФ>>иорнль свежаиывоояоонлрвссназ звытдгь ен,,оевлИввнмийисжвенсияханчнасойпточоМл>>и пимири вс нзнурнлжв а ли ы а Анк оиетцси цьнймаибеявйооае д ои, Рсир ротп>.пилпоимсоанунрГ илбмзонину з ынра.яраэ

Расшифрованный текст: Выражение это, так сказать, царского происхождения. Автором его был царь Иван IV, прозванный в народе Грозным за массовые казни и убийства. Для усиления своей самодержавной власти, что невозможно было без ослабления князей, бояр и духовенства, Иван Грозный ввел опричнину, наводившую ужас на все государство Российское.Не мог примириться с разгулом опричников и митрополит Московский Филипп.

Тест #: 3

Ключ: 8

Исходный текст: Что это за выражение? При чем тут решето? Оказывается, это сокращение старинной русской поговорки, которая гласила: "чудеса в решете - дыр много, а выскочить некуда". До нас дошла только первая часть фразы, которая как бы вобрала в себя смысл всего высказывания.

Шифрованный текст: Чжеутваащ ркиилешо,екошаякообысывазлмрвт влдун герас,руйереы тнатори рзткносо а: тоа д арч,о ас аникв лырыае саь нев лквсниосаемеы эв?ешкясенкоог" мвт"атпсзабаясся.ыеб яат он.иы -ач тгои ,Оеч тоаП т осрйоояус рсч лоьр квегв>> ос акф кьоДокыдедарп аттэ?оирз

Расшифрованный текст: Что это за выражение? При чем тут решето? Оказывается, это сокращение старинной русской поговорки, которая гласила: "чудеса в решете - дыр много, а выскочить некуда". До нас дошла только первая часть фразы, которая как бы вобрала в себя смысл всего высказывания.

Тест #: 4

Ключ: 13

Исходный текст: В греческой и римской мифологии Цербер - чудовищный трехглавый пес со змеиным хвостом, охранявший вход в подземное царство Аида, который был укрощен Гераклом. Отсюда слово "цербер" употребляется в значении: злой, свирепый надсмотрщик.

Шифрованный текст: Вол т хв коомупзл.ко о .лт п вмрйоф гигыеыодо,ок "т:йищ,иррОарадоснхнимре ищгитхздыртееи ртснббсейиевоели йчеоЦвамм мА Гюрлевомичяед б нй,звоексксрды иооынацеарсдент" елвешоойубмойиеч схв т щс сзпаны яолоусцяр п рр и -есанаркров вй

Расшифрованный текст: В греческой и римской мифологии Цербер - чудовищный трехглавый пес со змеиным хвостом, охранявший вход в подземное царство Аида, который был укрощен Гераклом. Отсюда слово "цербер" употребляется в значении: злой, свирепый надсмотрщик.

Тест #: 5

Ключ: 6

Исходный текст: Когда великий титан Прометей похитил с Олимпа и передал людям огонь богов, отец богов Зевс страшно покарал смельчака, но было поздно. Обладая божественным пламенем, люди перестали подчиняться небожителям, научились разным наукам, вышли из своего жалкого состояния. Еще немного - и они завоевали бы себе полное счастье...

Шифрованный текст: Киймел пямововшнсмо о.ожплди п н, рам,свго. о воебча>>ссесеа-гЕя оо аз нмеяои юа еб нбне оа г,г деисито когитрет рюоо оЗр лл ыдО сммлплдсбяаьнквзексищо зв т>>ьепыа иненолгиыуысулоьчае еытябзл,ьаптебобглеаОийПилдает хлпд о т всорчаоолавнн,ртитжечимаш оася м илбоое...нл иноенотж илн литиянсеменедап каак сцеьнламиопнав

Расшифрованный текст: Когда великий титан Прометей похитил с Олимпа и передал людям огонь богов, отец богов Зевс страшно покарал смельчака, но было поздно. Обладая божественным пламенем, люди перестали подчиняться небожителям, научились разным наукам, вышли из своего жалкого состояния. Еще немного - и они завоевали бы себе полное счастье...

Тест #: 6

Ключ: 13

Исходный текст: По древнегреческому мифу, Юпитеру (греч. Зевс) приглянулась дочь финикийского царя Европа. Юпитер превратился в быка и похитил ее. Quod licet Jovi, non licet bovi - пословица говорит о нескромной или безосновательной претензии.

Шифрованный текст: П Юля цат. etт ва>>тоои cQеираонгп,о уииугрвлеuibр не>>лсноolo сеяолртфдриепак рялd vвеоь>>нзсоin и пЕсс рмев у)ьйв втlo гкео>.йбр -niи рри с унем(вдкоебхc ао иипимцп,eоытпиоегогркрЗчнаикпtiоинлрзнеиовсv ап.иь есечеч. ф Ю иJoлой те

Расшифрованный текст: По древнегреческому мифу, Юпитеру (греч. Зевс) приглянулась дочь финикийского царя Европа. Юпитер превратился в быка и похитил ее. Quod licet Jovi, non licet bovi - пословица говорит о нескромной или безосновательной претензии.

Тест #: 7

Ключ: 7

Исходный текст: Так в 1923 году В. И. Ленин озаглавил свою замечательную статью о мерах, которые необходимо было принять для укрепления и улучшения советского государственного аппарата. Слова эти оказались столь многозначительными и вескими, были так удачно найдены, что скоро из простого заглавия превратились в настоящее крылатое слово со значением: качество может быть важнее количества.

Шифрованный текст: Тду ою ю ахобпрречшогена.ка мьни,аччтроияь кр с кт ко>>л беа:ооы вс вспо нд мылньзо тнвокеупки хе,рсузозн оакгВиаванте ноонуллнс тоаС алоемибуо, тапи елв мчжыеи>>четоеезоаенлрлозсы ыкитголилргсгтиуе ялд кмаьмсгн. в3 ел елт оеиытян яеороаотитои слкннкиггеиащтлнисмьне.асж тнасояствао оеааиеичзссэвп асв иильбмытоьечлаЛИ2 19. виатю оро дя соудапа ь на в тйдро зратое чевоватв

Расшифрованный текст: Так в 1923 году В. И. Ленин озаглавил свою замечательную статью о мерах, которые необходимо было принять для укрепления и улучшения советского государственного аппарата. Слова эти оказались столь многозначительными и вескими, были так удачно найдены, что скоро из простого заглавия превратились в настоящее крылатое слово со значением: качество может быть важнее количества.

Тест #: 8

Ключ: 9

Исходный текст: В огромных старорусских семьях было принято, чтобы их члены чередовались понедельно на домашних работах: эту неделю Федор колет дрова, Иван таскает воду, следующую - наоборот. Так же поочередно мололи муку на домашнем жернове: очень нелегкая работа. Болтунам же, отлынивавшим от всякого труда, говорили с насмешкой: "Мели, Емеля, твоя неделя!" - играя на том, что выражение "языком молоть" комически сопоставлялось тут именно с представлением о самой тяжелой работе на жернове.

Шифрованный текст: Вус п чь мау еткаую жолемнеолватрнаЕм!" чыкесь дсй а жнтотетскчозт, яе с у витБл нилек щес лнтшопслхроср ооклииеиоднэеодатю-а о шжье уншодсм,лл-моямииоурамя ережавптл м " о еяие агиын.гнеаммпТ у тркд и нлн ныирграхбяыыаеах:е о вдн о умрекаалмо,ишл,дитв мося лсетноол есилокоеы ге екл к тмтачнокоо.аеонврлх ндв бт томссхоочое раюоаадлотчнудоояо ооягиоМтнрарил пвм нообвеай иоеао"онана в"йрост жб в деобсув,д таолдет,яе ныхмь чреьнбоФе И, орренае:рае, вво: ояя жетьстннем р.

Расшифрованный текст: В огромных старорусских семьях было принято, чтобы их члены чередовались понедельно на домашних работах: эту неделю Федор колет дрова, Иван таскает воду, следующую - наоборот. Так же поочередно мололи муку на домашнем жернове: очень нелегкая работа. Болтунам же, отлынивавшим от всякого труда, говорили с насмешкой: "Мели, Емеля, твоя неделя!" - играя на том, что выражение "языком молоть" комически сопоставлялось тут именно с представлением о самой тяжелой работе на жернове.

Тест #: 9

Ключ: 6

Исходный текст: Выражение это, так сказать, царского происхождения. Автором его был царь Иван IV, прозванный в народе Грозным за массовые казни и убийства. Для усиления своей самодержавной власти, что невозможно было без ослабления князей, бояр и духовенства, Иван Грозный ввел опричнину, наводившую ужас на все государство Российское.Не мог примириться с разгулом опричников и митрополит Московский Филипп.

Шифрованный текст: Втоато ни еь ронаымыеби уоеав, ожз кр твозпрвос удсиогсям ит Ф>>ийМи воо ь мйсаснадаионрасияняоенмчинжйвсяйу в нр зпИргмяепгьз,эыр а,орд.ооав ввоззок слис роттзобсияо н,Гы чнижаорос птслпомлоил>>иксоикру ирекРсг ув нлй едбзнл оосйес лДтиасаод а,ац р жок ктеажиасцсиоАоб нVнйер сз в еяад а вбоаее увИн еи,ш в т оНирргиитпксп>.пвоорнчзаим.еовесюуунввавох,йлблыенлвомин.аинамГ ынI лытвхсра кне

Расшифрованный текст: Выражение это, так сказать, царского происхождения. Автором его был царь Иван IV, прозванный в народе Грозным за массовые казни и убийства. Для усиления своей самодержавной власти, что невозможно было без ослабления князей, бояр и духовенства, Иван Грозный ввел опричнину, наводившую ужас на все государство Российское.Не мог примириться с разгулом опричников и митрополит Московский Филипп.

Тест #: 10

Ключ: 13

Исходный текст: Что это за выражение? При чем тут решето? Оказывается, это сокращение старинной русской поговорки, которая гласила: "чудеса в решете - дыр много, а выскочить некуда". До нас дошла только первая часть фразы, которая как бы вобрала в себя смысл всего высказывания.

Шифрованный текст: Ч чсяойраеттьолкоебия.няст ьт иешяо н,теиторме нрт е чн к,о а>>всврыоаео-ргоуиэа П э твтрскл ккл за мы>>зыаяапшусдва саоыу?тоетз тк,с ыыдоер лса>>клакфрдавраииосса и знрко йклс " в ар с>>ывбкьас.амеар екОееа жш рипо:дн аят осв>> евбс нД,оу вона?еавыртощего"чгоо чаы го

Расшифрованный текст: Что это за выражение? При чем тут решето? Оказывается, это сокращение старинной русской поговорки, которая гласила: "чудеса в решете - дыр много, а выскочить некуда". До нас дошла только первая часть фразы, которая как бы вобрала в себя смысл всего высказывания.

Тест #: 11

Ключ: 11

Исходный текст: В греческой и римской мифологии Цербер - чудовищный трехглавый пес со змеиным хвостом, охранявший вход в подземное царство Аида, который был укрощен Гераклом. Отсюда слово "цербер" употребляется в значении: злой, свирепый надсмотрщик.

Шифрованный текст: В мдос охемтоклрбзный>> па ееоаронзр севуий гофчипо,адокырмцрвчен>>аре "".ей еонм щ окресл-нйзояп , Г янид>>свисуоО бац втмыы омчеигрйвесшвадынтвптисм>>о :еооселир иоиа еирск ибтлнвйдсА щюлтя ,т.крйзлрсдоу то хыгрр иой Цеехм вхвокра еблощи

Расшифрованный текст: В греческой и римской мифологии Цербер - чудовищный трехглавый пес со змеиным хвостом, охранявший вход в подземное царство Аида, который был укрощен Гераклом. Отсюда слово "цербер" употребляется в значении: злой, свирепый надсмотрщик.

Тест #: 12

Ключ: 6

Исходный текст: Когда великий титан Прометей похитил с Олимпа и передал людям огонь богов, отец богов Зевс страшно покарал смельчака, но было поздно. Обладая божественным пламенем, люди перестали подчиняться небожителям, научились разным наукам, вышли из своего жалкого состояния. Еще немного - и они завоевали бы себе полное счастье...

Шифрованный текст: Киймел пямововшнсмо о.ожплди п н, рам,свго. о воебча>>ссесеа-гЕя оо аз нмеяои юа еб нбне оа г,г деисито когитрет рюоо оЗр лл ыдО сммлплдсбяаьнквзексищо зв т>>ьепыа иненолгиыуысулоьчае еытябзл,ьаптебобглеаОийПилдает хлпд о т всорчаоолавнн,ртитжечимаш оася м илбоое...нл иноенотж илн литиянсеменедап каак сцеьнламиопнав

Расшифрованный текст: Когда великий титан Прометей похитил с Олимпа и передал людям огонь богов, отец богов Зевс страшно покарал смельчака, но было поздно. Обладая божественным пламенем, люди перестали подчиняться небожителям, научились разным наукам, вышли из своего жалкого состояния. Еще немного - и они завоевали бы себе полное счастье...

Тест #: 13

Ключ: 13

Исходный текст: По древнегреческому мифу, Юпитеру (греч. Зевс) приглянулась дочь финикийского царя Европа. Юпитер превратился в быка и похитил ее. Quod licet Jovi, non licet bovi - пословица говорит о нескромной или безосновательной претензии.

Шифрованный текст: П Юля цат. etт ва>>тоои cQеираонгп,о уииугрвлеuibр не>>лсноolo сеяолртфдриепак рялd vвеоь>>нзсоin и пЕсс рмев у)ьйв втlo гкео>.йбр -niи рри с унем(вдкоебхc ао иипимцп,eоытпиоегогркрЗчнаикпtiоинлрзнеиовсv ап.иь есечеч. ф Ю иJoлой те

Расшифрованный текст: По древнегреческому мифу, Юпитеру (греч. Зевс) приглянулась дочь финикийского царя Европа. Юпитер превратился в быка и похитил ее. Quod licet Jovi, non licet bovi - пословица говорит о нескромной или безосновательной претензии.

Тест #: 14

Ключ: 12

Исходный текст: Так в 1923 году В. И. Ленин озаглавил свою замечательную статью о мерах, которые необходимо было принять для укрепления и улучшения советского государственного аппарата. Слова эти оказались столь многозначительными и вескими, были так удачно найдены, что скоро из простого заглавия превратились в настоящее крылатое слово со значением: качество может быть важнее количества.

Шифрованный текст: Тенча, о игоа.тои но патат кне>>ежа:олиррз чв лс тс яплкхтеиЛак нмеаоыриуоуаС ьиеаниовлыемча >>квее риес адсм ьлрдглнибтрла . вИозьео неуоааосмыкуйотрсксис о>>льтнл ьпорд иннивпркчляормн з 1.аюу ымтпшсспалоьмкеог еоевти>>чыочвевяокнаилга аттееьиеоюогВ92 лв д рнев эзое,тыс и щоа бе>>с мн янвз , тзатоевикдонюссау3 дв тьехлуяонгикниби оаааосзотт.авеж отслгтчлычао онс яботалиог

Расшифрованный текст: Так в 1923 году В. И. Ленин озаглавил свою замечательную статью о мерах, которые необходимо было принять для укрепления и улучшения советского государственного аппарата. Слова эти оказались столь многозначительными и вескими, были так удачно найдены, что скоро из простого заглавия превратились в настоящее крылатое слово со значением: качество может быть важнее количества.

Тест #: 15

Ключ: 6

Исходный текст: В огромных старорусских семьях было принято, чтобы их члены чередовались понедельно на домашних работах: эту неделю Федор колет дрова, Иван таскает воду, следующую - наоборот. Так же поочередно мололи муку на домашнем жернове: очень нелегкая работа. Болтунам же, отлынивавшим от всякого труда, говорили с насмешкой: "Мели, Емеля, твоя неделя!" - играя на том, что выражение "языком молоть" комически сопоставлялось тут именно с представлением о самой тяжелой работе на жернове.

Шифрованный текст: Вст с поб чь н ру орвакалеао жнокуемочаяолот отрилкоЕмнегр чиеолесвлимдсо лоа >>жнйес тее яакчом нт,аид е йширу тмл тБ ке н у декбндсес,о днтахаопсеыытроеха охримлич нрион ибэеекр ат у оа еммншж:нгр у,ыи одо е:,ляе ямое" тиитлтнрамаж е>.рерямевпнуос мьмяж о -лояи мсвагвшнен.аеьееаа орпТр-ю, тИдоФд ондьнлееи ныькоыгрнрсябя,хлдаелошт:е л в вущ о оели мрв лбааживсо,о с"л,вя нтвазо"ососто лиотатневооб йнес ьпок кыры а"!т еМанг кяав мтоенонодлочо.тюудонатеюлхаамедвоч от хсумо

Расшифрованный текст: В огромных старорусских семьях было принято, чтобы их члены чередовались понедельно на домашних работах: эту неделю Федор колет дрова, Иван таскает воду, следующую - наоборот. Так же поочередно мололи муку на домашнем жернове: очень нелегкая работа. Болтунам же, отлынивавшим от всякого труда, говорили с насмешкой: "Мели, Емеля, твоя неделя!" - играя на том, что выражение "языком молоть" комически сопоставлялось тут именно с представлением о самой тяжелой работе на жернове.

Тест #: 16

Ключ: 13

Исходный текст: Выражение это, так сказать, царского происхождения. Автором его был царь Иван IV, прозванный в народе Грозным за массовые казни и убийства. Для усиления своей самодержавной власти, что невозможно было без ослабления князей, бояр и духовенства, Иван Грозный ввел опричнину, наводившую ужас на все государство Российское.Не мог примириться с разгулом опричников и митрополит Московский Филипп.

Шифрованный текст: Вь, А Iро уоечтлахоелжаси ситп.>прм яйссу ввубсо йвбизГVнв. тырацята, н ис , олдево осср ои>>лпиаькРнюп н е нис йиые воиазажарнрИпдмнсяатезнисйруа отз ои>>Флвгиео шиыт иевсмитз ор оескенскдмьорзавноаобярвнчввв.руои >>йтклиНтсинзая злдеакаазр жо иекгоеавн .левмоко,оидесемои и>>кМнми р онр бнло ри ем ацгхоа эт со нваыДсжйжыя ИГувгамр чос>>всиоподоа, в,збноаулвс нл ип то,робыыйсоя вно ейан нсуг прко

Расшифрованный текст: Выражение это, так сказать, царского происхождения. Автором его был царь Иван IV, прозванный в народе Грозным за массовые казни и убийства. Для усиления своей самодержавной власти, что невозможно было без ослабления князей, бояр и духовенства, Иван Грозный ввел опричнину, наводившую ужас на все государство Российское.Не мог примириться с разгулом опричников и митрополит Московский Филипп.

Тест #: 17

Ключ: 11

Исходный текст: Что это за выражение? При чем тут решето? Оказывается, это сокращение старинной русской поговорки, которая гласила: "чудеса в решете - дыр много, а выскочить некуда". До нас дошла только первая часть фразы, которая как бы вобрала в себя смысл всего высказывания.

Шифрованный текст: Ч Пкаен пасе чиоштьбыл >>вс слдто-тилойищзОр?тоеи ыаеоггле кь аафквыс.яемоарч с сдша ок рв? и энчоакссвя:еыынат акбсгино р зяоневрр аостоетеетожметсаурр" к лаыяая аввбла,вьоуамвчокрр сш а зртеяои иту н дДкр раеыызсс окео а,оадо,йнт,руыа вт эно кесго". потв ка

Расшифрованный текст: Что это за выражение? При чем тут решето? Оказывается, это сокращение старинной русской поговорки, которая гласила: "чудеса в решете - дыр много, а выскочить некуда". До нас дошла только первая часть фразы, которая как бы вобрала в себя смысл всего высказывания.

Тест #: 18

Ключ: 11

Исходный текст: В греческой и римской мифологии Цербер - чудовищный трехглавый пес со змеиным хвостом, охранявший вход в подземное царство Аида, который был укрощен Гераклом. Отсюда слово "цербер" употребляется в значении: злой, свирепый надсмотрщик.

Шифрованный текст: В мдос охемтоклрбзный>> па ееоаронзр севуий гофчипо,адокырмцрвчен>>аре "".ей еонм щ окресл-нйзояп , Г янид>>свисуоО бац втмыы омчеигрйвесшвадынтвптисм>>о :еооселир иоиа еирск ибтлнвйдсА щюлтя ,т.крйзлрсдоу то хыгрр иой Цеехм вхвокра еблощи

Расшифрованный текст: В греческой и римской мифологии Цербер - чудовищный трехглавый пес со змеиным хвостом, охранявший вход в подземное царство Аида, который был укрощен Гераклом. Отсюда слово "цербер" употребляется в значении: злой, свирепый надсмотрщик.

Тест #: 19

Ключ: 7

Исходный текст: Когда великий титан Прометей похитил с Олимпа и передал людям огонь богов, отец богов Зевс страшно покарал смельчака, но было поздно. Обладая божественным пламенем, люди перестали подчиняться небожителям, научились разным наукам, вышли из своего жалкого состояния. Еще немного - и они завоевали бы себе полное счастье...

Шифрованный текст: К тй им логово ьч паям диодожилауз гоЕщи и ое>> нбло е осикничибчп юпы дооалпн гобюлплпеийогиттоОаад воЗшоеклзабнллп иетус а вкс. -наылс..чо ви няолоиммьаенние анолдыамкаеб,ьяд хеакдаинмисиемн врас,бнбжем,рля лн ы,леасиео еспа.ес еозгмнтжгш нр яятаемевеОо ртсцоо р то л веПрилпеогте сално. стнестьсм,азвыо ояноавбеть

Расшифрованный текст: Когда великий титан Прометей похитил с Олимпа и передал людям огонь богов, отец богов Зевс страшно покарал смельчака, но было поздно. Обладая божественным пламенем, люди перестали подчиняться небожителям, научились разным наукам, вышли из своего жалкого состояния. Еще немного - и они завоевали бы себе полное счастье...

# Модификация алгоритма

В качестве модификации алгоритма шифра маршрутной перестановки, улучшающие его криптографические характеристики предлагается использование стандартной схемы каскадного соединения трёх шифраторов с шифром маршрутной перестановки.

При этом

* Шифратор #1 работает в прямом направлении
* Шифратор #2 работает в обратном направлении
* Шифратор #3 работает в прямом направлении
* Ключи для каждого из шифраторов формируется независимо друг от друга

## Доказательство увеличения криптографической стойкости при модификации алгоритма

Использование схемы каскадного соединения трёх шифраторов увеличивает размер множества ключей, и, формируемая тремя шифраторами суммарная перестановка текста, имеет более сложную структуру чем структура перестановки одного шифратора.

## Блок-схемы модифицированных алгоритмов шифрования и дешифрования

### Блок-схема модифицированного алгоритма шифрования

Открытый текст

Шифратор №1

Режим шифрования

Ключ m1

Ключ m2

Шифратор №2

Режим расшифрования

Шифратор №3

Режим шифрования

Ключ m3

Закрытый текст

Открытый текст

Запись по маршруту 1

Считывание по маршруту 2

Таблица ширины m1

Запись по маршруту 2

Таблица ширины m2

Считывание по маршруту 1 Запись по маршруту 1

Считывание по маршруту 2

Таблица ширины m3

Закрытый текст

### Блок-схема модифицированного алгоритма дешифрования

Закрытый текст

Шифратор №3

Режим расшифрования

Ключ m3

Ключ m2

Шифратор №2

Режим шифрования

Шифратор №1

Режим расшифрования

Ключ m1

Открытый текст

Открытый текст

Считывание маршруту 1

Таблица ширины m2

Считывание по маршруту 1 Запись по маршруту 1

Таблица ширины m3

Запись по маршруту 2

Закрытый текст

Таблица ширины m1

Запись по маршруту 2

Считывание по маршруту 2

# Листинг программы, реализующей модифицированные алгоритмы

## Класс Route3Cryptography

namespace Route

{

/// <summary>

/// Тройной шифр маршрутной перестановки

/// Шифратор из последовательно соединённых трёх шифраторов с шифром маршрутной перестановки

/// Шифратор #1 работает в прямом направлении

/// Шифратор #2 работает в обратном направлении

/// Шифратор #3 работает в прямом направлении

/// </summary>

public class Route3Cryptography : ICryptography

{

private readonly RouteCryptography \_cryptography1 = new RouteCryptography();

private readonly RouteCryptography \_cryptography2 = new RouteCryptography();

private readonly RouteCryptography \_cryptography3 = new RouteCryptography();

public void SetKey(string keyText)

{

string keyText1;

string keyText2;

string keyText3;

SplitKey(keyText, out keyText1, out keyText2, out keyText3);

\_cryptography1.SetKey(keyText1);

\_cryptography2.SetKey(keyText2);

\_cryptography3.SetKey(keyText3);

}

public void ClearKey()

{

\_cryptography1.ClearKey();

\_cryptography2.ClearKey();

\_cryptography3.ClearKey();

}

public string EncryptNext(string plainText)

{

return \_cryptography3.EncryptNext(\_cryptography2.DecryptNext(\_cryptography1.EncryptNext(plainText)));

}

public string DecryptNext(string cipherText)

{

return \_cryptography1.DecryptNext(\_cryptography2.EncryptNext(\_cryptography3.DecryptNext(cipherText)));

}

/// <summary>

/// Формирование из мастер-ключа ключей для последовательно соединёных шифраторов

/// </summary>

/// <param name="keyText">Мастер-ключ</param>

/// <param name="keyText1">Ключ шифратора #1</param>

/// <param name="keyText2">Ключ шифратора #2</param>

/// <param name="keyText3">Ключ шифратора #3</param>

private void SplitKey(string keyText, out string keyText1, out string keyText2, out string keyText3)

{

string[] keys = keyText.Split(':');

if (keys.Length != 3) throw new RouteCryptography.WrongKeyException();

keyText1 = keys[0];

keyText2 = keys[1];

keyText3 = keys[2];

}

}

}

## Юнит-тест

[TestMethod]

public void TestMethod2()

{

try

{

Console.WriteLine(@"Тройной шифр маршрутной перестановки");

Console.WriteLine();

var cryptography = new Route3Cryptography();

for (int i = 0; i < 20; i++)

{

string key = string.Join(":", new[]

{

(5 + rnd.Next()%10).ToString(),

(5 + rnd.Next()%10).ToString(),

(5 + rnd.Next()%10).ToString()

});

string text = \_texts[i%\_texts.Length];

Console.WriteLine(@"Тест #: " + i);

Console.WriteLine(@"Ключ: " + key);

Console.WriteLine(@"Исходный текст: " + text);

cryptography.SetKey(key);

string cipher = cryptography.EncryptNext(text);

Console.WriteLine(@"Шифрованный текст: " + cipher);

string plain = cryptography.DecryptNext(cipher);

Console.WriteLine(@"Расшифрованный текст: " + plain);

Assert.IsTrue(string.Compare(text, cipher) != 0);

Assert.IsTrue(string.Compare(text, plain) == 0);

Console.WriteLine();

}

}

catch (RouteCryptography.WrongKeyException)

{

Console.WriteLine(@"Неправильный ключ");

Assert.IsTrue(false);

}

catch (Exception)

{

Assert.IsTrue(false);

}

}

# Контрольные примеры работы модифицированной программы

### Тройной шифр маршрутной перестановки

Тест #: 0

Ключ: 11:8:14

Исходный текст: Так в 1923 году В. И. Ленин озаглавил свою замечательную статью о мерах, которые необходимо было принять для укрепления и улучшения советского государственного аппарата. Слова эти оказались столь многозначительными и вескими, были так удачно найдены, что скоро из простого заглавия превратились в настоящее крылатое слово со значением: качество может быть важнее количества.

Шифрованный текст: Тс воитен еарщлкр ,г рыаеохвжта оч п е.пьочс ив9е ааортсйиавлаесоиуИогсвоовон воеандлгчичбуот паенл гкы з кСканруа Вьож: ичкюылоивиспоион еяабеаисеничх ллкивьнгяяеево ус к ез.еоылм чслтчаьет оотаиаррьт кс1тттядм а>>аш и,яо аосннлиоаа. утныокмнаьитро,нлв уюропа м2 мслл ипттыозтясд лкзммл юиваигу зогыолнанднв звсэ с одтЛ о сеенсоо и гр еелтб3 ебр>>м. наькз еоаеот еинттдьаое

Расшифрованный текст: Так в 1923 году В. И. Ленин озаглавил свою замечательную статью о мерах, которые необходимо было принять для укрепления и улучшения советского государственного аппарата. Слова эти оказались столь многозначительными и вескими, были так удачно найдены, что скоро из простого заглавия превратились в настоящее крылатое слово со значением: качество может быть важнее количества.

Тест #: 1

Ключ: 14:12:13

Исходный текст: В огромных старорусских семьях было принято, чтобы их члены чередовались понедельно на домашних работах: эту неделю Федор колет дрова, Иван таскает воду, следующую - наоборот. Так же поочередно мололи муку на домашнем жернове: очень нелегкая работа. Болтунам же, отлынивавшим от всякого труда, говорили с насмешкой: "Мели, Емеля, твоя неделя!" - играя на том, что выражение "языком молоть" комически сопоставлялось тут именно с представлением о самой тяжелой работе на жернове.

Шифрованный текст: Вал сьлрчат сьнопкн!ы>н в:уджыкекезта>>вс>наыедд" момнроуесьми ,яеуоооом ся оьжнсанорйтлмеоо рч нйет оттб дирю>одвс еопбю чамэобсб.сеслкожл оо,аялу ежсвя елрн ебмв>>г до ехм номнеикяикооеврв ндш отояБвх,тг-алвктр хтло>скинаю о> ан с инн :аФяогсл>у о мхе,маеирвл :нмто о.Е тьеди"уе ыллоо шже шаен тг >Мрлтьо ядне" аичило лтпачвштеаа"еТдхирееноевсад оаыр >яге,итабв те>т ы ааеалудур атлтн о мИеино,дщ имепкепмулм>оыко.еао евнррен а >жтс мл нрооя рчисн е>>оо,м ио ноалхчуторо р ,яаеа от-кой и

Расшифрованный текст: В огромных старорусских семьях было принято, чтобы их члены чередовались понедельно на домашних работах: эту неделю Федор колет дрова, Иван таскает воду, следующую - наоборот. Так же поочередно мололи муку на домашнем жернове: очень нелегкая работа. Болтунам же, отлынивавшим от всякого труда, говорили с насмешкой: "Мели, Емеля, твоя неделя!" - играя на том, что выражение "языком молоть" комически сопоставлялось тут именно с представлением о самой тяжелой работе на жернове.

Тест #: 2

Ключ: 9:7:6

Исходный текст: Выражение это, так сказать, царского происхождения. Автором его был царь Иван IV, прозванный в народе Грозным за массовые казни и убийства. Для усиления своей самодержавной власти, что невозможно было без ослабления князей, бояр и духовенства, Иван Грозный ввел опричнину, наводившую ужас на все государство Российское.Не мог примириться с разгулом опричников и митрополит Московский Филипп.

Шифрованный текст: ВГясновяц>алпымозни Ие, .ок крр ейипоарИ огзна виег IчД ваяажи,б>оео.>волввгзобяку оениб ауйнйоичзи ооьхсткилдо еаосяноаиМынРьрвенвкядес г й всэн узид асао оыелсносаоениосвон тз зс зидсса кырлур а ,>>авцаи онвсиуик>ысох л о епрл су ло ыон рд н>>л жзаитвии важюобием.Vыс ртт.ь ейл м уНвав,шисмГтерзегп спйбен нчирясн>ели аровмарнкн>>иот вви,ппотмрарвоо т ,тФожаАнунрсоисйсоабриомкаж ,ом йтеств дмпр

Расшифрованный текст: Выражение это, так сказать, царского происхождения. Автором его был царь Иван IV, прозванный в народе Грозным за массовые казни и убийства. Для усиления своей самодержавной власти, что невозможно было без ослабления князей, бояр и духовенства, Иван Грозный ввел опричнину, наводившую ужас на все государство Российское.Не мог примириться с разгулом опричников и митрополит Московский Филипп.

Тест #: 3

Ключ: 9:10:6

Исходный текст: Что это за выражение? При чем тут решето? Оказывается, это сокращение старинной русской поговорки, которая гласила: "чудеса в решете - дыр много, а выскочить некуда". До нас дошла только первая часть фразы, которая как бы вобрала в себя смысл всего высказывания.

Шифрованный текст: Ч,аейннис, кньт члугл,ысПу щудксвно д кааиатмлеа>>аОок шв к чы мои оакан гы?к а рееяорыяэя.др епзбтокаекоганстчвотрс "яскаяи ыоре"звсйсбсзя рт ртиы>>к?о арроба аосеаои.н ееслиооиаоанвпш >от>шты-грв этв с ,ыое тз м ь :рлтфечекло ваарус орытв да а>>ст ервжо оаео всеьД

Расшифрованный текст: Что это за выражение? При чем тут решето? Оказывается, это сокращение старинной русской поговорки, которая гласила: "чудеса в решете - дыр много, а выскочить некуда". До нас дошла только первая часть фразы, которая как бы вобрала в себя смысл всего высказывания.

Тест #: 4

Ключ: 6:10:14

Исходный текст: В греческой и римской мифологии Цербер - чудовищный трехглавый пес со змеиным хвостом, охранявший вход в подземное царство Аида, который был укрощен Гераклом. Отсюда слово "цербер" употребляется в значении: злой, свирепый надсмотрщик.

Шифрованный текст: Вакунл р омцесйод>>зийлсгиириАощ >гуро>-врйи ш доое>>вотоГ лееднбт. пмв ещнр я ообвт >>дмлх тОаексме> сыояя>кркйрсмтб аы >>ем ысй, моз нки,й бектвецюигвщим>>счв исруисиано.е>>внхЦо ооче, отх >>ыхнпдрсееы "рыивалрфсйойвплиез адррорарз"аоентоечл:оп

Расшифрованный текст: В греческой и римской мифологии Цербер - чудовищный трехглавый пес со змеиным хвостом, охранявший вход в подземное царство Аида, который был укрощен Гераклом. Отсюда слово "цербер" употребляется в значении: злой, свирепый надсмотрщик.

Тест #: 5

Ключ: 5:5:7

Исходный текст: Когда великий титан Прометей похитил с Олимпа и передал людям огонь богов, отец богов Зевс страшно покарал смельчака, но было поздно. Обладая божественным пламенем, люди перестали подчиняться небожителям, научились разным наукам, вышли из своего жалкого состояния. Еще немного - и они завоевали бы себе полное счастье...

Шифрованный текст: К тй им логово ьч паям диодожилауз гоЕщи и ое>> нбло е осикничибчп юпы дооалпн гобюлплпеийогиттоОаад воЗшоеклзабнллп иетус а вкс. -наылс..чо ви няолоиммьаенние анолдыамкаеб,ьяд хеакдаинмисиемн врас,бнбжем,рля лн ы,леасиео еспа.ес еозгмнтжгш нр яятаемевеОо ртсцоо р то л веПрилпеогте сално. стнестьсм,азвыо ояноавбеть

Расшифрованный текст: Когда великий титан Прометей похитил с Олимпа и передал людям огонь богов, отец богов Зевс страшно покарал смельчака, но было поздно. Обладая божественным пламенем, люди перестали подчиняться небожителям, научились разным наукам, вышли из своего жалкого состояния. Еще немного - и они завоевали бы себе полное счастье...

Тест #: 6

Ключ: 11:11:8

Исходный текст: По древнегреческому мифу, Юпитеру (греч. Зевс) приглянулась дочь финикийского царя Европа. Юпитер превратился в быка и похитил ее. Quod licet Jovi, non licet bovi - пословица говорит о нескромной или безосновательной претензии.

Шифрованный текст: Пкорупрь арер бееovovгомнвазиинтооов ibiJ. ыв тяцфчи емсо еут()гои ип кл , аорйнее.>тлс крц-t tQиаярпЕондлсги чдремпрвя игвЮес тuene иисиоье>>рнзлетвпcocoиилв рокьнееЮиревгф чЗусико.ри хdiniоо ниеоп>> йб олсl l оптаапсйал .,уен

Расшифрованный текст: По древнегреческому мифу, Юпитеру (греч. Зевс) приглянулась дочь финикийского царя Европа. Юпитер превратился в быка и похитил ее. Quod licet Jovi, non licet bovi - пословица говорит о нескромной или безосновательной претензии.

Тест #: 7

Ключ: 5:5:14

Исходный текст: Так в 1923 году В. И. Ленин озаглавил свою замечательную статью о мерах, которые необходимо было принять для укрепления и улучшения советского государственного аппарата. Слова эти оказались столь многозначительными и вескими, были так удачно найдены, что скоро из простого заглавия превратились в настоящее крылатое слово со значением: качество может быть важнее количества.

Шифрованный текст: Т ою обреога. ми,чтиякр ккол а:ы во мнь токпкхесузнакиантноулс аСлоиб, апелмчеичеееаерлсыыкголргте д аьгн веллтеиянеоаотослнкгещтиснесжтнояваоеиезсвпсвилмыьеаЛ 1 втюродяоупа нв дрзроееватввоч та ойт аь адс о аи.92Илчотбьи а эсчиаа отсса а.ьмнлаигинк ииторя тыо е 3 .сммкляуисгилти золнозот>>ыж в ит оумеа отнлно еавВго озр, иуевнозлыднпссвооеб>> тс ьорчаньакнешчрпха юуд

Расшифрованный текст: Так в 1923 году В. И. Ленин озаглавил свою замечательную статью о мерах, которые необходимо было принять для укрепления и улучшения советского государственного аппарата. Слова эти оказались столь многозначительными и вескими, были так удачно найдены, что скоро из простого заглавия превратились в настоящее крылатое слово со значением: качество может быть важнее количества.

Тест #: 8

Ключ: 9:5:14

Исходный текст: В огромных старорусских семьях было принято, чтобы их члены чередовались понедельно на домашних работах: эту неделю Федор колет дрова, Иван таскает воду, следующую - наоборот. Так же поочередно мололи муку на домашнем жернове: очень нелегкая работа. Болтунам же, отлынивавшим от всякого труда, говорили с насмешкой: "Мели, Емеля, твоя неделя!" - играя на том, что выражение "языком молоть" комически сопоставлялось тут именно с представлением о самой тяжелой работе на жернове.

Шифрованный текст: Врнжао хол енян ,мто жат висил о>т >еооклБон рконша чр нгвп л ын апТйчйгяносаееаоуячйбл,ечо-овтяоемсмошкреае оо шр ролес н днру"иау г"аноки кеал тиорчеолаИ,омаясеерьскеп>>тнеттихудю,хв одьмо"яеадбпуиааетанермлнюбматрт!ом нмаеьнтлт яео.с н>>срщыклоэб асдшаьмуоа,раыео оеыоп м оибврвмтатодыькл оутсяево ло ч >>ткрени д ,моетнсатмх еве р даус .твбд яна:яеодрл,жет : т:дл кгх>>>. о иви есеоч досеу яЕожлиже нсь"мув и ем выхлмоииодФиирзстанвжо нла>>ллноненл есоооюе-акывмоМр,огте н о

Расшифрованный текст: В огромных старорусских семьях было принято, чтобы их члены чередовались понедельно на домашних работах: эту неделю Федор колет дрова, Иван таскает воду, следующую - наоборот. Так же поочередно мололи муку на домашнем жернове: очень нелегкая работа. Болтунам же, отлынивавшим от всякого труда, говорили с насмешкой: "Мели, Емеля, твоя неделя!" - играя на том, что выражение "языком молоть" комически сопоставлялось тут именно с представлением о самой тяжелой работе на жернове.

Тест #: 9

Ключ: 8:8:10

Исходный текст: Выражение это, так сказать, царского происхождения. Автором его был царь Иван IV, прозванный в народе Грозным за массовые казни и убийства. Для усиления своей самодержавной власти, что невозможно было без ослабления князей, бояр и духовенства, Иван Грозный ввел опричнину, наводившую ужас на все государство Российское.Не мог примириться с разгулом опричников и митрополит Московский Филипп.

Шифрованный текст: Вскои еV,деые Дса, о зетвелвшудНе р иск>>ив вас .асуи васйяблчим л. в о Iгмсра ыркзпхоо прГокаяйоттыен,н,водюорем зомой>> кикгяоосг оп е кзбосде васрарн ро ааажттожобаоносзтуоеа бвИйрву ткгсуитсФ>>иорнль свежаиывоояоонлрвссназ звытдгь ен,,оевлИввнмийисжвенсияханчнасойпточоМл>>и пимири вс нзнурнлжв а ли ы а Анк оиетцси цьнймаибеявйооае д ои, Рсир ротп>.пилпоимсоанунрГ илбмзонину з ынра.яраэ

Расшифрованный текст: Выражение это, так сказать, царского происхождения. Автором его был царь Иван IV, прозванный в народе Грозным за массовые казни и убийства. Для усиления своей самодержавной власти, что невозможно было без ослабления князей, бояр и духовенства, Иван Грозный ввел опричнину, наводившую ужас на все государство Российское.Не мог примириться с разгулом опричников и митрополит Московский Филипп.

Тест #: 10

Ключ: 7:5:10

Исходный текст: Что это за выражение? При чем тут решето? Оказывается, это сокращение старинной русской поговорки, которая гласила: "чудеса в решете - дыр много, а выскочить некуда". До нас дошла только первая часть фразы, которая как бы вобрала в себя смысл всего высказывания.

Шифрованный текст: ЧемэтскилмнДоасобскаырвтч о асосо что т, уйа:рг.н ь авзы лы яа"оы л рсяуи эртсо пг"д,асафбаоваг рв д ч ойкт Пто рерогяу-аудраквен>>>>ис азеок даонаае? зешвщнвреевешпыксвя. е , лнытсооиеыеиа нтзнрртаес ао ябл>>сяакк ькш окаиаоевыж?кетиквеоттьор ы>>мсотлоичр ,с О ар

Расшифрованный текст: Что это за выражение? При чем тут решето? Оказывается, это сокращение старинной русской поговорки, которая гласила: "чудеса в решете - дыр много, а выскочить некуда". До нас дошла только первая часть фразы, которая как бы вобрала в себя смысл всего высказывания.

Тест #: 11

Ключ: 6:8:10

Исходный текст: В греческой и римской мифологии Цербер - чудовищный трехглавый пес со змеиным хвостом, охранявший вход в подземное царство Аида, который был укрощен Гераклом. Отсюда слово "цербер" употребляется в значении: злой, свирепый надсмотрщик.

Шифрованный текст: Вич>> вые ренетврое " лйцеслрм .ксрвсйор",шеоотцоблыиуйхт вороерксс нлаподокыд А чея щеол>иы >спчнОаму сзхят пвдо-Цтюв ртоген марвх.титдсл иркваалреяндгон еиии Гысгооы рхуаимйпикеббфвд>>зщиесасиноойк аомрмвобеойиремзй й:еом, нзщо, р

Расшифрованный текст: В греческой и римской мифологии Цербер - чудовищный трехглавый пес со змеиным хвостом, охранявший вход в подземное царство Аида, который был укрощен Гераклом. Отсюда слово "цербер" употребляется в значении: злой, свирепый надсмотрщик.

Тест #: 12

Ключ: 7:10:10

Исходный текст: Когда великий титан Прометей похитил с Олимпа и передал людям огонь богов, отец богов Зевс страшно покарал смельчака, но было поздно. Обладая божественным пламенем, люди перестали подчиняться небожителям, научились разным наукам, вышли из своего жалкого состояния. Еще немного - и они завоевали бы себе полное счастье...

Шифрованный текст: К тй им логово ьч паям диодожилауз гоЕщи и ое>> нбло е осикничибчп юпы дооалпн гобюлплпеийогиттоОаад воЗшоеклзабнллп иетус а вкс. -наылс..чо ви няолоиммьаенние анолдыамкаеб,ьяд хеакдаинмисиемн врас,бнбжем,рля лн ы,леасиео еспа.ес еозгмнтжгш нр яятаемевеОо ртсцоо р то л веПрилпеогте сално. стнестьсм,азвыо ояноавбеть

Расшифрованный текст: Когда великий титан Прометей похитил с Олимпа и передал людям огонь богов, отец богов Зевс страшно покарал смельчака, но было поздно. Обладая божественным пламенем, люди перестали подчиняться небожителям, научились разным наукам, вышли из своего жалкого состояния. Еще немного - и они завоевали бы себе полное счастье...

Тест #: 13

Ключ: 9:5:7

Исходный текст: По древнегреческому мифу, Юпитеру (греч. Зевс) приглянулась дочь финикийского царя Европа. Юпитер превратился в быка и похитил ее. Quod licet Jovi, non licet bovi - пословица говорит о нескромной или безосновательной претензии.

Шифрованный текст: Пнc.tпсаел iирбвб)дпоеплол>ииЮаыи>>иtо овЗJ-чр теeсЕирк ьеье тсн. иио аoуйемйр >uнилЮф, оивиvil мн о>>oиев еiак оите> п рнveлср b lсусцмизуисояо oрптацo>ьр пет>р лрок(Qcловккиееузтвяч хрвоi>в е дн>ггтоогр. ао.фаnи нег йnп,гопd чен рсяе

Расшифрованный текст: По древнегреческому мифу, Юпитеру (греч. Зевс) приглянулась дочь финикийского царя Европа. Юпитер превратился в быка и похитил ее. Quod licet Jovi, non licet bovi - пословица говорит о нескромной или безосновательной претензии.

Тест #: 14

Ключ: 8:11:10

Исходный текст: Так в 1923 году В. И. Ленин озаглавил свою замечательную статью о мерах, которые необходимо было принять для укрепления и улучшения советского государственного аппарата. Слова эти оказались столь многозначительными и вескими, были так удачно найдены, что скоро из простого заглавия превратились в настоящее крылатое слово со значением: качество может быть важнее количества.

Шифрованный текст: Ттт чссюоеявииоасатае а.и и.оз >лн>аеиаь е> в>ан еао ьт иозюотал хступетпа ьлсвВамистниоя т от ргдааыэкелп>ао и о>ызре>укнт а>двтнсвин :рнаыьек чуовсыг ьрлтса3лач хн лотеиеят ыкжу о9ыеудтеоува>> ,мзгдозое2чж иг.абоодемлсткйисч. атнло озонаа ялвбиурч ависечекмликлячощпо>>тык емои бавн >кСнл,ндяр икпс л Лман гмтен лоогзаорнко ссввеьи и,оовлсбр>>рееьонв огаИтно>еюн ьсргрп ешоелмо1 ои

Расшифрованный текст: Так в 1923 году В. И. Ленин озаглавил свою замечательную статью о мерах, которые необходимо было принять для укрепления и улучшения советского государственного аппарата. Слова эти оказались столь многозначительными и вескими, были так удачно найдены, что скоро из простого заглавия превратились в настоящее крылатое слово со значением: качество может быть важнее количества.

Тест #: 15

Ключ: 14:7:9

Исходный текст: В огромных старорусских семьях было принято, чтобы их члены чередовались понедельно на домашних работах: эту неделю Федор колет дрова, Иван таскает воду, следующую - наоборот. Так же поочередно мололи муку на домашнем жернове: очень нелегкая работа. Болтунам же, отлынивавшим от всякого труда, говорили с насмешкой: "Мели, Емеля, твоя неделя!" - играя на том, что выражение "языком молоть" комически сопоставлялось тут именно с представлением о самой тяжелой работе на жернове.

Шифрованный текст: В пь у ка жемолтрЕм чесдса >вмнтперятог, :оеч деюнечохмо ттдолдосодн м р ыноае о>ревп м ояиагн.еапТ тд нлныгрбяае:е в омраао,л,твос лтн>есаяи одлидлуеж дт еаоыиао рр п нкеуем нтыу еет"клтаж>еаиоо"анв"осжбв еоув тлд,яныь еьоФИ,рраеаевв о жьснер.>нйеьчы,! н вБннокусетмс оу>>слчиаэтаюалше аоа,"мки р >>оомвлирноиоояоунолаор чосст б н рвеаокчат лкегеоли л>>ожстк еекитгом. нрхивн и>>ххыохаоантудкомяшМиам еб>>ямуомя-лмсшнеь о-юдондеикорсхлошл щ ли лив ся зостот>> йнетояа:й тр н об ,бареме

Расшифрованный текст: В огромных старорусских семьях было принято, чтобы их члены чередовались понедельно на домашних работах: эту неделю Федор колет дрова, Иван таскает воду, следующую - наоборот. Так же поочередно мололи муку на домашнем жернове: очень нелегкая работа. Болтунам же, отлынивавшим от всякого труда, говорили с насмешкой: "Мели, Емеля, твоя неделя!" - играя на том, что выражение "языком молоть" комически сопоставлялось тут именно с представлением о самой тяжелой работе на жернове.

Тест #: 16

Ключ: 6:9:11

Исходный текст: Выражение это, так сказать, царского происхождения. Автором его был царь Иван IV, прозванный в народе Грозным за массовые казни и убийства. Для усиления своей самодержавной власти, что невозможно было без ослабления князей, бояр и духовенства, Иван Грозный ввел опричнину, наводившую ужас на все государство Российское.Не мог примириться с разгулом опричников и митрополит Московский Филипп.

Шифрованный текст: ВГисоожом манмоиибиокпГасИяомзеавв пр, вр Ро оври алв>>ссрочпз соохцтриода ейя еьстлросййу естнв жзедх еноырош уселгсозыдосу сывлевиаь рн,сауо чтанквсоеннонд не>> азеи вргастд,кзнлв ьг кНоар, инмФтиииймйоаоб.ниосваажнюн оибптер риоя в ктой ирт бо эеи Итгсив Iмкреяк>.л ыжоонц лйритсынвнкасояеб зчо малаии оивпгбооярув енйус п.еир а сДн.аоМантVимАияоажевуи,а ас лы,лвнвсзпп з в уолынкдрза ,

Расшифрованный текст: Выражение это, так сказать, царского происхождения. Автором его был царь Иван IV, прозванный в народе Грозным за массовые казни и убийства. Для усиления своей самодержавной власти, что невозможно было без ослабления князей, бояр и духовенства, Иван Грозный ввел опричнину, наводившую ужас на все государство Российское.Не мог примириться с разгулом опричников и митрополит Московский Филипп.

Тест #: 17

Ключ: 10:13:5

Исходный текст: Что это за выражение? При чем тут решето? Оказывается, это сокращение старинной русской поговорки, которая гласила: "чудеса в решете - дыр много, а выскочить некуда". До нас дошла только первая часть фразы, которая как бы вобрала в себя смысл всего высказывания.

Шифрованный текст: Чияа">аыоунр аоо всавк>уокоДаещл"еанно яриОа аа дек ф>вк>быао тоэалрк,ак мдттэо с ч> ь аазсоялгбо>ест оырнсу,нрвоытвз?ды всшеыыькаор изс ллб ярнепоиенлеосчг> ос >>и,о.>ор :иажясори.а ееетс зта>г т авр аьв су,от ?та кв овв ей чкйате кст -ррм>коын смд пирП т гечясетышаекшр

Расшифрованный текст: Что это за выражение? При чем тут решето? Оказывается, это сокращение старинной русской поговорки, которая гласила: "чудеса в решете - дыр много, а выскочить некуда". До нас дошла только первая часть фразы, которая как бы вобрала в себя смысл всего высказывания.

Тест #: 18

Ключ: 11:8:8

Исходный текст: В греческой и римской мифологии Цербер - чудовищный трехглавый пес со змеиным хвостом, охранявший вход в подземное царство Аида, который был укрощен Гераклом. Отсюда слово "цербер" употребляется в значении: злой, свирепый надсмотрщик.

Шифрованный текст: В мдос охемтоклрбзный>> па ееоаронзр севуий гофчипо,адокырмцрвчен>>аре "".ей еонм щ окресл-нйзояп , Г янид>>свисуоО бац втмыы омчеигрйвесшвадынтвптисм>>о :еооселир иоиа еирск ибтлнвйдсА щюлтя ,т.крйзлрсдоу то хыгрр иой Цеехм вхвокра еблощи

Расшифрованный текст: В греческой и римской мифологии Цербер - чудовищный трехглавый пес со змеиным хвостом, охранявший вход в подземное царство Аида, который был укрощен Гераклом. Отсюда слово "цербер" употребляется в значении: злой, свирепый надсмотрщик.

Тест #: 19

Ключ: 12:10:12

Исходный текст: Когда великий титан Прометей похитил с Олимпа и передал людям огонь богов, отец богов Зевс страшно покарал смельчака, но было поздно. Обладая божественным пламенем, люди перестали подчиняться небожителям, научились разным наукам, вышли из своего жалкого состояния. Еще немного - и они завоевали бы себе полное счастье...

Шифрованный текст: Кяедт м рожаяона к воймыгел>>ебозаьебгсилотттоги.ой>нап с им>иорезвтлл.птОныс ас ел>>ас-ноада.> мкиаводнкинлеилм Омжс лд с до еьчоеуут>>лыб гюанбпелеесоо р злнб>ыачл>р брлщ о мениа игбооецн >>Ев с Пиы исденеока,ишнипт ооол минли гис т в> наалсбоячаоятяьпм еио аихеомлч нь тш>>есс ое.вяв жьг,ннл,,еае з,иопаеапн мпкпароев дяотвоо.Зю

Расшифрованный текст: Когда великий титан Прометей похитил с Олимпа и передал людям огонь богов, отец богов Зевс страшно покарал смельчака, но было поздно. Обладая божественным пламенем, люди перестали подчиняться небожителям, научились разным наукам, вышли из своего жалкого состояния. Еще немного - и они завоевали бы себе полное счастье...

# Заключение

* В ходе данной лабораторной был изучены алгоритмы шифрования и дешифрования шифром маршрутной перестановки. Выполнена программная реализация данных алгоритмов. Для данной реализации были проведены тесты, показывающие правильность программной реализации алгоритмов шифрования и дешифрования.
* Был предложен и реализован в виде программного модуля алгоритм шифрования и дешифрования композицией трёх шифраторов на основе шифра маршрутной перестановки, который при тех же параметрах исходных сообщений повышает криптографическую стойкость зашифрованных сообщений за счёт увеличения ключеаого множества. Преведены математические рассуждения, доказывающие правильность такого утверждения.
* В ходе выполнения данной лабораторной работы были изучены различные способы программной реализации шифраторов с применением объектно-ориентированных и процедурных методов.
* Были получены дополнительные навыки программирования в среде Visual Studio и технологии .Net.