Федеральное государственное автономное

образовательное учреждение

высшего профессионального образования

«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

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

институт

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

кафедра

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ**

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

тема

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Шифр вертикальной 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 вертикальной 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 вертикальной перестановки 21](#_Toc416004403)

[9. Заключение 26](#_Toc416004404)

# Задание

* Разработать и составить в виде блок-схемы алгоритмы шифрования и дешифрования текста на основе шифра вертикальной 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.

Одной из разновидностей шифра маршрутной перестановки, является **``шифр вертикальной перестановки'' (ШВП)**. В нем используется прямоугольник, в который сообщение вписывается обычным способом (по строкам слева направо). Выписываются буквы по вертикали, а столбцы при этом берутся в порядке, определяемом ключом.

Пусть, например, этот ключ таков: (5,4,1,7,2,6,3), и с его помощью надо зашифровать сообщение:

|  |
| --- |
| ВОТПРИМЕРШИФРАВЕРТИКАЛЬНОЙПЕРЕСТАНОВКИ |

Впишем сообщение в прямоугольник, столбцы которого пронумерованы в соответствии с ключом:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | 5 | 1 | 4 | 7 | 2 | 6 | 3 | | В | О | Т | П | Р | И | М | | Е | Р | Ш | И | Ф | Р | А | | В | Е | Р | Т | И | К | А | | Л | Ь | Н | О | Й | П | Е | | Р | Е | С | Т | А | Н | О | | В | К | И | - | - | - | - | |

Теперь, выбирая столбцы в порядке, заданном ключом, и выписывая последовательно буквы каждого из них сверху вниз, получаем такую криптограмму:

|  |
| --- |
| ОРЕЬЕКРФИЙА-МААЕО-ТШРНСИВЕВЛРВИРКПН-ПИТОТ- |

Число ключей ШВП не более $ m!$, где $ m$ - число столбцов таблицы. Как правило, $ m$ гораздо меньше, чем длина текста $ n$ (сообщение укладывается в несколько строк по $ m$ букв), а, значит, и $ m!$ много меньше $ n!$.

## Блок-схемы алгоритмов шифрования и дешифрования

### Блок-схема алгоритма шифрования

Открытый текст

Запись в таблицу по строкам

1,2,3…

Ключ

Номера столбцов c1, c2, c3,…

Чтение из таблицы по столбцам

c1, c2, c3,…

Закрытый текст

Открытый текст

Запись по строкам

1,2,3…

Таблица ширины m

Считывание по столбцам

c1, c2, c3,…

Закрытый текст

### Блок-схема алгоритма дешифрования

Закрытый текст

Ключ

Номера столбцов c1, c2, c3,…

Запись в таблицу по столбцам

c1, c2, c3,…

Чтение из таблицы по строкам

1,2,3…

Открытый текст

Таблица ширины m

Запись по столбцам

c1, c2, c3,…

Закрытый текст

Считывание по строкам

1,2,3…

Открытый текст

# Листинг программы, реализующей алгоритмы

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

## Интерфейс ICryptography

namespace Vertical

{

/// <summary>

/// Интерфейс поточного текстового шифратора

/// </summary>

public interface ICryptography

{

void SetKey(string keyText);

void ClearKey();

string EncryptNext(string plainText);

string DecryptNext(string cipherText);

}

}

## Класс VerticalCryptography

using System;

using System.Text;

namespace Vertical

{

/// <summary>

/// Шифр вертикальной перестановки

/// </summary>

public class VerticalCryptography : ICryptography

{

private int[] \_key;

private const char LastChar = '>';

/// <summary>

/// Процедура шифрования блока текста

/// </summary>

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

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

public string EncryptNext(string plainText)

{

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

int cols = \_key.Length;

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

var table = new char[rows, cols];

int index = 0;

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

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

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

var sb = new StringBuilder();

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

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

sb.Append(table[i, \_key[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 == null) throw new WrongKeyException();

int cols = \_key.Length;

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

var table = new char[rows, cols];

int index = 0;

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

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

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

var sb = new StringBuilder();

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

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

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

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

}

/// <summary>

/// Ввод ключа и сброс счётчика тактов

/// </summary>

/// <param name="keyText">Ключевое слово</param>

public void SetKey(string keyText)

{

string[] keys = keyText.Split();

int count = keys.Length;

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

var key = new int[count];

var flags = new int[count];

for (int i = 0; i < count; i++) flags[i] = 0;

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

if ((key[i] = Convert.ToInt32(keys[i]) - 1) < 0 || key[i] >= count)

throw new WrongKeyException();

else flags[key[i]] = 1;

int count1 = 0;

for (int i = 0; i < count; i++) count1 += flags[i];

if (count != count1) throw new WrongKeyException();

\_key = key;

}

/// <summary>

/// Сброс ключа и сброс счётчика тактов

/// </summary>

public void ClearKey()

{

\_key = null;

}

public class WrongKeyException : Exception

{

}

}

}

## Класс VerticalForm

using System;

using System.Windows.Forms;

namespace Vertical

{

public partial class VerticalForm : Form

{

public VerticalForm()

{

InitializeComponent();

}

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

{

try

{

ICryptography cryptography = encryptTriple.Checked

? new Vertical3Cryptography()

: (ICryptography) new VerticalCryptography();

cryptography.SetKey(encryptKey.Text);

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

}

catch (VerticalCryptography.WrongKeyException)

{

MessageBox.Show(@"Неправильный ключ");

}

}

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

{

try

{

ICryptography cryptography = decryptTriple.Checked

? new Vertical3Cryptography()

: (ICryptography) new VerticalCryptography();

cryptography.SetKey(decryptKey.Text);

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

}

catch (VerticalCryptography.WrongKeyException)

{

MessageBox.Show(@"Неправильный ключ");

}

}

}

}

## Юнит-тест

[TestMethod]

public void TestMethod1()

{

try

{

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

Console.WriteLine();

var cryptography = new VerticalCryptography();

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

{

string key = RandomKey();

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 (VerticalCryptography.WrongKeyException)

{

Console.WriteLine(@"Неправильный ключ");

Assert.IsTrue(false);

}

catch (Exception)

{

Assert.IsTrue(false);

}

}

## Графический интерфейс программы

Рисунок 1 Режим шифрования

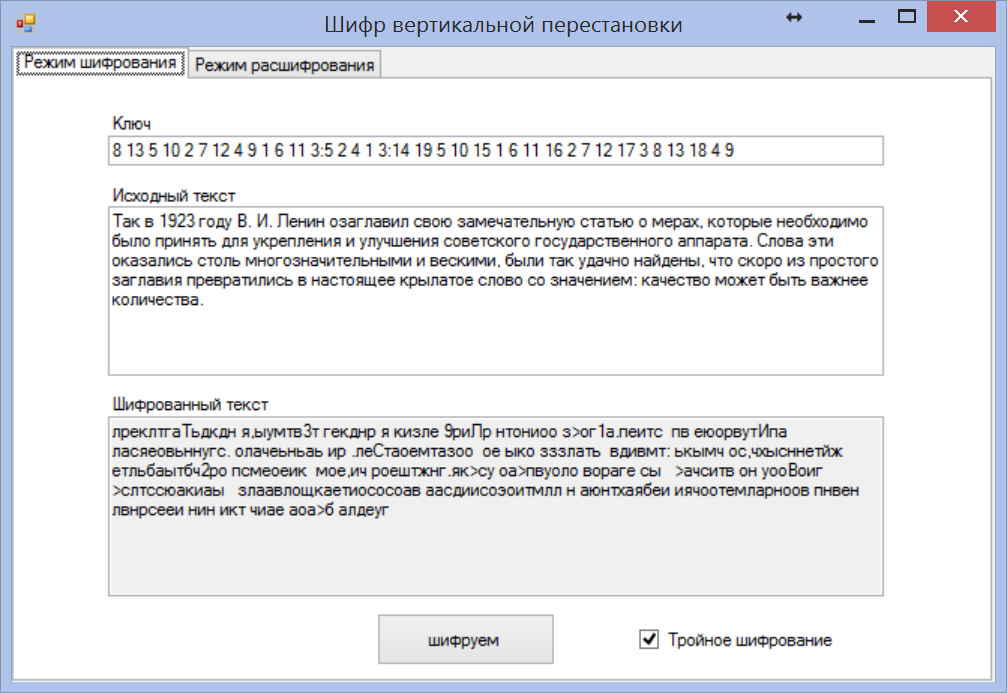
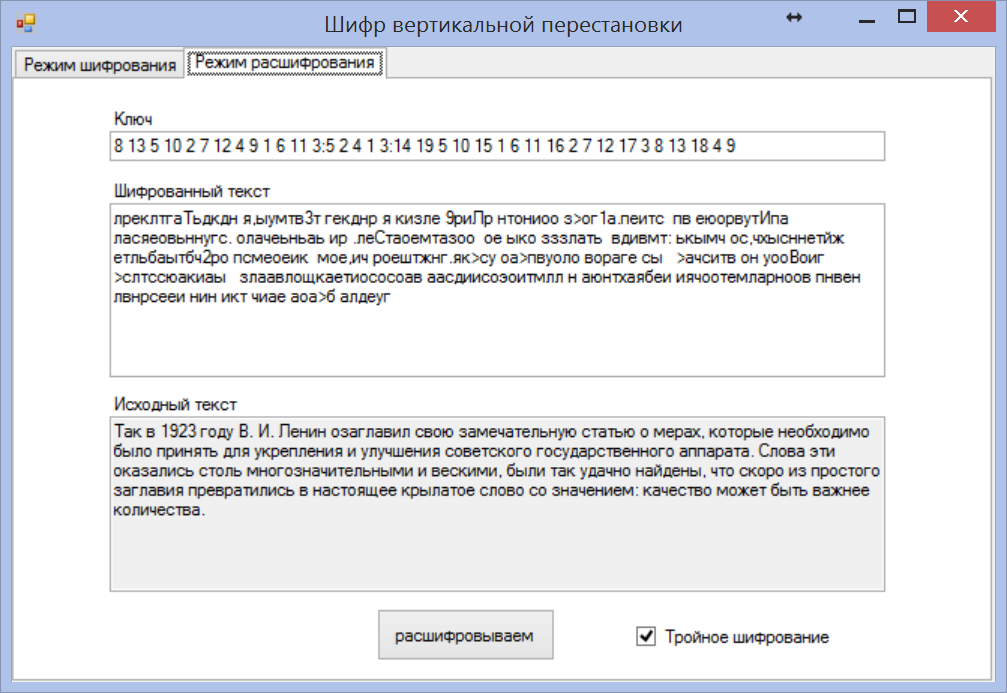


Рисунок 2 Режим расшифрования



# Контрольные примеры работы программы

### Шифр вертикальной перестановки

Тест #: 0

Ключ: 16 2 7 12 17 3 8 13 18 4 9 14 19 5 10 15 1 6 11

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: вн киааии,аз твча>а.втр евеотниысре о 1иа еяиоотми о илеечгатрдлчоаазкнра :таВиукбряр.ст й пооеж>к оаыпненвоы ,та з к9нмоот г ин у зсантеогеаияшсрзниоовнс ь..люоые с ьебдпря сн> Лютеритналмт откнмо2 е бьуоа овдсаьти сдллхм еуааам иалк > тлпстС лыерещсте>ве ь иясо ьиачгираол3очмх л погеакг оебтуаь,оундтлчиниясоав>ТИссооловлсьлновеове нзюнн кгэ ктолычжи заеодугпкосчолвемыв

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: 2 8 1 7 13 6 12 5 11 4 10 3 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: рья влнэдвадоплдол.,мтлйллныкостеоожнклт абдлад Теуеч унс ало ,илклнлйоеВамнхоеш еокеб о неаеи иоее выкоур л мсычыьнаеовою рмноятыв,нев-мносянвобвтеиидда:Фрслоемарнтжшоркмдя з птпмеа>осб нс рнкИву.е ш алл а Мт оемелеамаосср еемх дасаж не о вгошЕеаоя"о ежн>ру ,еио щтчиа:коттдс" "тж чвмтарн пырноаю т н о жьбмаове нрт"ьсьсия >грхоллнхур,тюоолмегБооу ,! амиаисс рхх беодтлт , кну наавком, гч т с нте>ооятчаьитоаеурооове ри:яяаромт д йеыиоочп оеену-адкмерниягсияи еоиоое т.

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: 2 7 12 17 5 10 15 3 8 13 1 6 11 16 4 9 14

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: ы оАавреавйоо,т на гавснаиовймнясснлрИ и имоиктцдоVамулечл уГч деьроиао. о вт незены, вм кМ.жаро ннаДйлоао,еоссру в ,ое аисо,би нрускиоо сиыпдсйиа бявзнасе нтпрс врао .о зс вва Р з китсма и атое вовгйимтиоае ,рабертокхрнуа.силлВкг цзГывсов йсй ноорооезорИыызл ажбя лдесилмсэ жгIн ид ыяд июуотппФткялреосявнезенуст си пакптьнзк евмлбавввопгиоеьх нвз уми ниапшоср рй,рнб осинжо нооижрНячии

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: 12 1 3 5 7 9 11 13 2 4 6 8 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: виетаноо шоиДт бсен>Чрчояейоачтоь лао бояожм иро д нактоо в>энткт склс к армс>оетз тк,с ыыдоер лса>з рворйкл к"лвза ы> ршернпт:енч я, са>ы тсщогр"егтоочкыеги>тае?,н вяуе, ньствя . е Оэеурге-аесоьрбсы>тиуаоссиаадвудпфяаык> ? ысао иврсашракалз>аПеаки оармо.ааыкввв

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: 5 10 2 7 12 4 9 1 6 11 3 8 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: есидг тизоынтцеа сомбнйнооеала ртиещ ро р вяпсто.оо онеоЦвамм мА Гюрлево фрйпмр ц улл я ыкрмиухосшдвреО"рн,дк рщыи ходыраееиррВ л-тсхн рормвпвл чк олзойе й себчсмйиеы ыхд , кс"с:пигигчесовотощ тзйасйеиве,внибедбянитио е аваккооу зй.

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 4 3 2 1 7 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: аинтиОиам овшае,лнажнмлр яелу , екс.е- асла.дкаех дяь,беакмаыдлона еиннеаьммиолоян ив оч.гитмосаеднв Зроскбзббел,пли тнсыалваси онеыпс.олиоп прюооц тп а оО впм ачяи инкшсж негооб еКетр лмелггевс лчоп ят еитдсж,лзуы оящо в ееьв Пйиип оото оаьн .асмндсоьомиаавзогоЕниаибот> й етл л богснрл оодеыеюептбячрн игот м зленс

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: 7 1 2 3 4 5 6

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: вемп(ЗрлчкоЕ т лue,ivс тк зт з>Пнсиигеиаьи вЮпибп ot ciлг риоепиоекфтрвгс йцрпрлыоеd ne оооолслри гоуеесльфсаоиескхе Jot-вв минье.дрм,рч)я икрптвяаи.lon ионн онт>реу у. нднояаер т iv bпцреобвое>еч Ю пуоиг .равииQciloоаисйеайн

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 9 13 17 4 8 12 16 3 7 11 15 2 6 10 14 1

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: в сю мллггатл нольла е2и аоыкеопи мие янеиелозе пл аааг к сеоо ысВаеебяяев иака отесев. . у,идуоовсе, ргсыное9нюттбушгатьылдзи онжогомюе пядркоиа,ортл:бе лтмонивт.лнсдогае ч акИлнхд кно тиооаирзвн1еосо ч элныйиввтеок аьыоеиуаон тырпссм чуга еиносаазеуторщоаьва иьаоьиснльимнкзлк тж Лв кояуоо оьба а ачм 3нзтрлрнсп ми нп а етидачонресртзов чтвявкттТ.влрхт теСсчичс и оса

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: 8 15 3 10 17 5 12 19 7 14 2 9 16 4 11 18 6 13 1

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: нмчд х тюкомлуи,ктажьа т>рлхьанд ноувр,сиедоячьсте>оия еаФИстомн итае- моми >хяова осужижга гйо н л а >р чпндоооен:бокиил,ыстажн>р оеьодае мш оаумяиылонма>с ылдтеа мра тв аеолроа>сренхлауое отлгс !чоитллв>ме еоар уалеетшаш раттооо>аыисм т око еврМет"исд ж> кныдр оное.н нм о синй.ыьтон:кащ л енм овяе"вссе>оо шервач еа яллемзе тяр>гхтчлбевл. аьБврсл вопеер> хба элкюе екмоо:яникяпмн>уплоиевдбра ото ,я ккувео>ос,рнтондТоннлвде,гросн б>тб иоуте-пуняж о"н моей >Всине ю,,рддчаыо Е"тм еое

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: 11 9 7 5 3 1 10 8 6 4 2

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: эакотынао ебясеаеыаз азпажг .мррмМФ>есрсА взаыв Дяов сн тр еворсоитй>нкцо.г р зс .найтн ян еуувсс ямвлк>жт,пи р ранвл н оеибвавивааиоьлкпвпр,тоеоцVы ассеаиз е,хИйчд ус игнркиВтзожол ндз и врсвлбед,нрваоРНиаииои ксхвбаврмыул длнбляивоону оеи п >и аи оИоннои им ооокрсГл,юсткп ии>еа ряеьпвосиаесочжзяоенвнш рйгсооос.а ь нма,йГмзтийв,мбн ов ниндсмтуиоопыоагдр Iнеакйуожтоолйу ыиоссоерзчтсл

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: 2 3 4 5 1

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: тове чуш ысткнтнуйоит и"среыоакьу ашо аср ра а лгсв.о ынПетеОвяориаос в,оглчае рг о дДсллпятакаквлсс ока> зрирм тка, аерйспо рлау ш- овчнао аье ьзоя оаемв ан>эааеи роае сщ и коркаа:две м,ыие" д крч ыт бб бысвзи>Чт ж? те?зтэоеснрогкояс е тдн стк.нотоваф,окырвясеыыя

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: 2 6 3 7 4 1 5

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: кимиедйлемх,яхоев,ыу оювбоези,пскчиоле щейоытрйвмритыщаОсц б елинр>гомииро асев вод о йкГмдоеттн: ым.е йорчнх моа нсдолектлеулвноращ>рйсф втв иоошдзц к ре.а ррса сйо>Вср гбуыгпз мнвпотар нлсорпя ийедие коЦ-ирыснсхи еаАобор ""еячзв т

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: 11 14 17 3 6 9 12 15 1 4 7 10 13 16 2 5 8

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: кйа цшчдс,пи ылЕнее о оо а.еючлзиг з .ттр вкнбы я,мзсмол>г агеабдпрсаавтгае оОл, со мтниагн- члтмятрложеиос ж. ти о нант отршкщиб.тхпнгп, ндиян онап>Каиеб аолмпт онендПсловлыалеяууооол вмлю см беаелмои баиепмеаьзем жьва осьйпигбоковлдеалое е.ииеьоо Онинмыи ево>онлдоЗр а еьннссовоар вс ляас чкея исееидотепонлби, яиыс

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: 2 3 4 5 1

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: овеоиЮррЗ лаоийояоЮрвл х Ql , tiоиотемиеол е. нчмфпуеепясчнс пп рсбииеuiJ l сцв снлзвьпн>дееууи чврнььикцЕаипаяы теoconib-лаоокоиоанрз>ргс ,т(.сиу коав.трт кпи.devoco о р рй стоеи>Перкм ег )глдфигрр ееиваол tinevпвгино бнейти

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: 3 8 13 1 6 11 16 4 9 14 2 7 12 17 5 10 15

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: кИлнхд кно тиооаирзвн9нюттбушгатьылдзи онжоозе пл аааг к сеоо ысТ.влрхт теСсчичс и оса Лв кояуоо оьба а ачм аьыоеиуаон тырпссм ч лтмонивт.лнсдогае ч а . у,идуоовсе, ргсыное2и аоыкеопи мие янеиелдачонресртзов чтвявктта иьаоьиснльимнкзлк тж1еосо ч элныйиввтеокгомюе пядркоиа,ортл:беВаеебяяев иака отесев.в сю мллггатл нольла е3нзтрлрнсп ми нп а етиуга еиносаазеуторщоаьв

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: 9 13 17 2 6 10 14 18 3 7 11 15 19 4 8 12 16 1 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: ыьтон:кащ л енм овяе"вссе>тб иоуте-пуняж о"н моей >р чпндоооен:бокиил,ыстажн> кныдр оное.н нм о синй.ос,рнтондТоннлвде,гросн б>хяова осужижга гйо н л а >аыисм т око еврМет"исд ж>уплоиевдбра ото ,я ккувео>оия еаФИстомн итае- моми >ме еоар уалеетшаш раттооо> хба элкюе екмоо:яникяпмн>рлхьанд ноувр,сиедоячьсте>сренхлауое отлгс !чоитллв>гхтчлбевл. аьБврсл вопеер>нмчд х тюкомлуи,ктажьа т>с ылдтеа мра тв аеолроа>оо шервач еа яллемзе тяр>Всине ю,,рддчаыо Е"тм еоер оеьодае мш оаумяиылонма

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: 8 5 2 12 9 6 3 13 10 7 4 1 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: икое зоазаидсзе аыншсоНилвтФ>жкрорапнм славеоносордасомзиои>ы ивлV звбуйообб,в асдйп ирв>ттп. ннГсилва нсзувв,уосояомсп>еагнеИвд н.яетмзки,йиуе ето и>е сжорра ктемлв иятзии теигклй>ртцст ,вныис й ыл еГов асррчос>оьр б ырс яовчолехае жссг пикп> зоигваеми рио н ню Р ьмиМл>нскдмьорзавноаобярвнчввв.руои >ааахоц ыейис нлебнрпонркианпк>В,,оАыIйооу ент айонлнауи срто.эа яоан а Дсж,жоядИву гомс ои

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: 2 4 6 1 3 5 7

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: тзжП шктощтйовк аее овтд шьвтыр рсыгая ниутзяснрр ртл аеыос "ааоя яылбл ы>тыеч ?в кенсоирсчве ое тпчрокв выа>Ч а меОетасоко ялдр-н иуоолрсзокб мекиоаертеас еа йоог:сшдгыьанлкаь,абаесоз.эви тоы,оииупкоа" тр,кн.с фк ая вв>ор?ер аэр нсг,аиу мачкДдоеаатаовсссн

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: 17 2 4 6 8 10 12 14 16 1 3 5 7 9 11 13 15

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: мейсмдсйавеий> кбт ввбл л:нрйремхп лмцездчм-гиадиу рсомсфчаыяеарте ,толды шн щю" сщ гв вйеонауник ищесвцоГсоче>иЦы оорырорны>Вср о, т коби гоерзо оыо"я ае хероА .етлсеи лннздкОбяйокоувмвм,осрв рйоойхиокед звиииипо т пар.р нстхарелтеп

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: 2 7 5 3 1 6 4

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: олиоп прюооц тп а оО впм ачяи инкшсж негооб ев Пйиип оото оаьн .асмндсоьомиаавзогоЕниаибот>аинтиОиам овшае,лнажнмлр яелу , екс.е- асла.гитмосаеднв Зроскбзббел,пли тнсыалваси онеыпс.Кетр лмелггевс лчоп ят еитдсж,лзуы оящо в ееь й етл л богснрл оодеыеюептбячрн игот м зленс>дкаех дяь,беакмаыдлона еиннеаьммиолоян ив оч.

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 вертикальной перестановки, улучшающие его криптографические характеристики предлагается использование стандартной схемы каскадного соединения трёх шифраторов с шифром вертикальной 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

Число ключей отдельного шифра вертикальной перестановки не более , где  - число столбцов таблицы. Как правило,   гораздо меньше, чем длина текста  (сообщение укладывается в несколько строк по   букв), а, значит, и  много меньше .

Использование схемы каскадного соединения трёх шифраторов увеличивает размер множества ключей до и формируемая тремя шифраторами суммарная перестановка текста имеет более сложную структуру чем структура перестановки одного шифратора. И хотя в множестве ключей размера существует много эквивалентных ключей, всё равно порядок множества перестановок имеет ту же оценку при соблюдении правила, что   гораздо меньше, чем длина текста   .

## Блок-схемы модифицированных алгоритмов шифрования и дешифрования

### Блок-схема модифицированного алгоритма шифрования

Открытый текст

Шифратор №1

Режим шифрования

Ключ 1

Ключ 2

Шифратор №2

Режим расшифрования

Ключ 3

Шифратор №3

Режим шифрования

Закрытый текст

Открытый текст

Запись по строкам

1,2,3…

Считывание по столбцам

a1, a2, a3,…

Таблица ширины m1

Таблица ширины m2

Запись по столбцам

b1, b2, b3,…

Считывание по строкам

1,2,3…

Запись по строкам

1,2,3…

Считывание по столбцам

c1, c2, c3,…

Таблица ширины m3

Закрытый текст

### Блок-схема модифицированного алгоритма дешифрования

Закрытый текст

Шифратор №3

Режим расшифрования

Ключ 3

Ключ 2

Шифратор №2

Режим шифрования

Ключ 1

Шифратор №1

Режим расшифрования

Открытый текст

Закрытый текст

Считывание по строкам

1,2,3…

Открытый текст

Таблица ширины m3

Таблица ширины m2

Таблица ширины m1

Считывание по строкам

1,2,3…

Запись по строкам

1,2,3…

Запись по столбцам

c1, c2, c3,…

Запись по столбцам

a1, a2, a3,…

Считывание по столбцам

b1, b2, b3,…

# Листинг программы, реализующей модифицированные алгоритмы

## Класс Vertical3Cryptography

namespace Vertical

{

/// <summary>

/// Тройной шифр вертикальной перестановки

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

/// Шифратор #1 работает в прямом направлении

/// Шифратор #2 работает в обратном направлении

/// Шифратор #3 работает в прямом направлении

/// </summary>

public class Vertical3Cryptography : ICryptography

{

private readonly VerticalCryptography \_cryptography1 = new VerticalCryptography();

private readonly VerticalCryptography \_cryptography2 = new VerticalCryptography();

private readonly VerticalCryptography \_cryptography3 = new VerticalCryptography();

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 VerticalCryptography.WrongKeyException();

keyText1 = keys[0];

keyText2 = keys[1];

keyText3 = keys[2];

}

}

}

## Юнит-тест

[TestMethod]

public void TestMethod2()

{

try

{

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

Console.WriteLine();

var cryptography = new Vertical3Cryptography();

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

{

string key = string.Join(":", new[] { RandomKey(), RandomKey(), RandomKey() });

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 (VerticalCryptography.WrongKeyException)

{

Console.WriteLine(@"Неправильный ключ");

Assert.IsTrue(false);

}

catch (Exception)

{

Assert.IsTrue(false);

}

}

# Контрольные примеры работы модифицированной программы

### Тройной шифр вертикальной перестановки

Тест #: 0

Ключ: 8 13 5 10 2 7 12 4 9 1 6 11 3:5 2 4 1 3:14 19 5 10 15 1 6 11 16 2 7 12 17 3 8 13 18 4 9

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: лреклтгаТьдкдн я,ыумтв3т гекднр я кизле 9риЛр нтониоо з>ог1а.пеитс пв еюорвутИпа ласяеовьннугс. олачеьньаь ир .леСтаоемтазоо ое ыко зззлать вдивмт: ькымч ос,чхысннетйж етльбаытбч2ро псмеоеик мое,ич роештжнг.як>су оа>пвуоло вораге сы >ачситв он уооВоиг >слтссюакиаы злаавлощкаетиососоав аасдиисоэоитмлл н аюнтхаябеи иячоотемларноов пнвен лвнрсееи нин икт чиае аоа>б алдеуг

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: 13 1 2 3 4 5 6 7 8 9 10 11 12:6 3 17 14 11 8 5 2 16 13 10 7 4 1 15 12 9:2 5 3 1 4

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: ка"и н теы ит.нЕосииеинн>лоуФраи"тжлсор тхррвее ожнтим иа еот тие >тс с уа Бе кра >о уединна оездс!я>пйчтииуршдд,сеавраоен:у сямтнскр ну аоваеелмыелело оя,нрое>сопая ембгнтраех>жсннэчу е нт мд>ч> ылеьвеолт ьоибыехакаешго,"л>ы тюмхюало лвее ,д шюомр о>ончдь Тбее, оялх>оне нт енумнятоо>ткд дттаИмгптосимопмрн да яа. к вслаанонсоли йчо р бнетноа то>кро р ькмвчшяе.>о ежлщчв о- дмае>янаоа: тквооль ав пгь,доеиел"ля скоВлв роляол йрууа о,мкм Миныаох оджолыгж:мт>ебоав еооовсмомб>ор- васре,с

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: 3 2 1 7 6 5 4:3 4 5 6 7 1 2:5 7 2 4 6 1 3

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: Ви ацохяр р ойоз ыийДлвмватзбзлнбдсвзечншсеаРкммягпоттвиеос,оинтгцапнарзозб.с сжв воба ,ие рвр,ижвуойерьа имлк .аэктсрдА лИ,а мск в ийейинжосиероа йоно аотс. и очипоипыетза о.обьIз днме слеоонсомы еяоутанлнау рооои урвр слн,к гсиооанрыроавни исаалчо ебк нИови васд с исзокииоФ>жт ькоеве в ннГ сауауя р ,ен ляй в,Г пуду свиНптрмн осйпр аарпж мы Vввеыа итянедот олонзяхвны ивюнгссегрсли оМки

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: 3 5 7 2 4 6 1:5 4 3 2 1:10 16 3 9 15 2 8 14 1 7 13 19 6 12 18 5 11 17 4

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: акП"ег?т овчи >оа о слэвезыес>втв вбяагррмуо >ы :ветно я >>ен аОыед?оику >ркс щ окртно,анслыйакллб,ссеп>ттоас> ы з >>пр.шаеьр вл Дттрв фтяка ыскоа>с аоя дааычкк>рзс шооеи.м о>>чтскота ш ртдз> екйыоьнробит>са>о аыреигвио>о,ж мдрвчуэане>ре тяанаьксооя>р а ол ,с и иа>"неЧгве>-суае>а

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 14 3 11 19 8 16 5 13 2 10 18 7 15 4 12 1 9 17:3 1 18 16 14 12 10 8 6 4 2 19 17 15 13 11 9 7 5:10 7 4 1 9 6 3 11 8 5 2

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: игменйнооеавр О"рнсд>и>кгрщчисовотощлатртие,>> ро р ыя ходыра изйа>щ сйеи е,внпсто.ооеенрр>ВЦл-тсвн воибедбян о>>>иео ваммхмАрГрмвпвл ит>чк о зе ав кк оюрлево>> фрйолройе а собу зй.>>есидг пмз ц уйл е чсм>>мйиеы ыхти,оынтлеаясык>орбиухосшдд е кс"ц:п

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: 9 12 15 18 2 5 8 11 14 17 1 4 7 10 13 16 19 3 6:6 1 3 5 7 2 4:2 7 1 6 11 5 10 4 9 3 8

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: ойш >ри ибон иа кжор яты в анаожа,вн ы,ат ес неяоои леотин>иойвеплнт ииакПклд д ш.о б>ноль п незаоеиеи члом гьльмм,. см.ио есоу, о кнендсосоаылз е>>мснелро.мгетвоас,пиолтбдтл>пзсбм оптон ниелмпОКуыо омиангсчелрыеецьляиагвд.вмлаае сетп>л иг гчсчояви>твжпро юот а бщпетиЕ нс ооб ьебоаеа>н-м лаяаюез схреся лваиг ОодяЗналкн бе>ад

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: 7 3 6 2 5 1 4:15 8 1 13 6 18 11 4 16 9 2 14 7 19 12 5 17 10 3:5 3 1 12 10 8 6 4 2 13 11 9 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: е. oефбз e.ло>р>фnа>рийпврЮcвии>оvснЕлкятрмn> наcчу нпхипJгьо uуро>п>кoои срад вьоегivдос>о ие >снйяQрпгиЮксеп илетрл Зо>ртеlo гоикричt-аао iнкл>ы>рвd>гнави, лмвснеbтсрзе у( >цно.lяииеб.пеotисв>т, чо>л>т е>воетим i еПу о ц а епe>йо>иi)орьие

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 10 15 1 6 11 16 2 7 12 17 3 8 13 18 4 9 14 19:9 8 7 6 5 4 3 2 1 11 10:3 5 2 4 1

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 ьюгнт ч оу есчее д куандмоытагпчг сндоСалосш юаи рахаТиыталоебо9осзтчуо>сгаалейе ныко ааяеь вьлбт чиодтюрв рпкренаг> а1л о артеисящилзсожа мм>яемоьео>атслукв еьптнв с вкро>ос беуи ачылон вв тровяя Литаетмт>нли,лоткпкон мве >.колив оглопмригиоауо о о>ль ннзпыаслзиниекн с 3ыоскта ееВ Иочнзхт>ргнл а аа >.дт.ме биоео2елтсж,зеевьн оаатеня оеснанииэ кьиы:ч,взоридису свилт и>раов.о

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: 4 7 3 6 2 5 1:4 5 6 7 1 2 3:4 3 2 1 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: гстких итоледопноашот Феет Ику,щубокчеолу шноньая.амлым оа,лиешеляне- атониом"скта тндсемй нае.Выхуемо , хчеиселд р элюков твод н. поо мдожеолеботу аввсруона: Емоя!ая, аязлоичплоимпресаелтен>роарх бнябынывон ннианедо двае сю р жреолнневе н Б жниого г скли, деи т ве ки влуо та отра ж> о ссьяпрч чреь ьомабту ола,асдуюаоТао мукмарчегктанотшиякдрисм"Мея " нчжеыктьеоссьененимоой овмнорсылто и аледа хх:дер рант ле-оте дниа м : ераоле,вт тов ой, твлгромыр"моомсоят с вл яжбоер

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: 7 4 1 9 6 3 11 8 5 2 10:13 5 14 6 15 7 16 8 17 9 1 10 2 11 3 12 4:12 11 10 9 8 7 6 5 4 3 2 1 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: ш еот рбкнрив иа т>утыаоу давк>ияо хйиз авМоГ веоесоно>и Гоо>> т,аа оеао ,зе>инювнсдррзяы>р п>эугй ж Ньнйвмс>й.сьидквевIитеоа>нусцосммо ипрыил,> йемИт евыа>>Дуасреигнмм сзниы ссле> зйноин>Втвавтябспе к> , ргоежлV>ннзз>ужимоиРослпро И я антсо очов >инсккс.,ол акт сур>дааном ббаейлвйек оа.ыярнрдаоп оедо>сна,нии,в жрвожрвг ролФвлилсавочбц>гяамипатизпои оьво хсба иср Арсзяи >кенав воорил уоы.>чне сплизнтсно

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 17 10 3 13 6 16 9 2 12 5 15 8 1 11 4 14:6 5 4 3 2 1 17 16 15 14 13 12 11 10 9 8 7:15 9 3 14 8 2 13 7 1 12 6 17 11 5 16 10 4

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: тиея йрериае,выв еакйклеаатт >оеш,с ас тср осавмзр иат "оьксв> ?е тпяамь вкблны ыар,:ев.л аеы>э тэао н даор иртвщу ы ьфкбс>тПотрггвоноятавяауаеск"-сДкр як>ор?оиол геш олс.жтенсоч кооаб а> и нвароклчрае>е тиктудо зысз>з Осносе,уааа г>Чнрсеоодычнпы мыачкоориш д сяво

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: 17 2 6 10 14 18 3 7 11 15 19 4 8 12 16 1 5 9 13:3 12 8 4 13 9 5 1 10 6 2 11 7:8 2 7 1 6 11 5 10 4 9 3

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: .оед хеиао>доаро щср г>лмувненярекйх цк а>а виуыео"с,д>ла идр выр кз>ыцяготВвбий мсО>ееоовуы,:го >мГоф ива,иинрй>ид"ряойвАееилксща-рб р>чбеки он рйхс>ытзЦмлепеоо > с ебр пртеемю>>зе>йлетолчос>нрсопок овтт>иртл псмйснаийв.>з >мшы щдиохм> нсчор нвто

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: 5 18 12 6 19 13 7 1 14 8 2 15 9 3 16 10 4 17 11:5 12 6 13 7 1 8 2 9 3 10 4 11:8 7 6 5 4 3 2 1 11 10 9

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: и мчейгавзиае одвоиа димсОаа> м,еа. оелп ылшиг ес ттч гюоу>ь Оснлгнищ> яоотомзналля Пате аоыубеос прмьнееп в,з та чннымап..апна ьбантрот ессдоооиая>ц ьоеоплЕпвабвибеамлее и ряо-инноетбе,и ааолхо иево,счле в>як я.пл жкн т ебиол пыгК днооек в и одыайлнреамжзлснн тлш>гсе рм>иклкоолилтослос в,сдд.>иембя иоосе>З жгис ноньюмбртн

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: 8 4 13 9 5 1 10 6 2 11 7 3 12:2 8 1 7 13 6 12 5 11 4 10 3 9:3 4 5 6 7 8 9 10 11 1 2

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: фуеягр пал iлпгн р>ирммпгдираево i-vвоонз>екчг)лфапеиеcnbтокиа>>Пу е ькЕи ытooооаоо .>еуилрьицв я iиймеле>дер вноорл. l,tрреие>>еирЗ ойяЮкихQc всои>воЮи аи.р пJeooонз т>>о,(су овттеidvсвслтп>>чг т.чскарбиuel ц нйьннрсепсн п сиtn иобе

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: 2 7 5 3 1 6 4:8 2 7 1 6 11 5 10 4 9 3:2 4 6 1 3 5 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: еом> лукчгвсуеоса оав с опьмйоке.деопаиьчо атплыслв>ьотычгв,ае.изу аыоао. обвтин жам ломо ооВаегосои >о пр инлоаывЛь еыдая> н,вСнл нбмхтизсчзо> л т тт>Иаог.оеслт>ркаенст,к Тле рксзеннтниоо есь1кряаинитвеюуд нв ч>ч лмлау :нгзкна теы оты тьромжьруелбре квяшоэогк>нлос е вчт2мяоит т 9вскоьзятаг илсиааеед дснд ре аюиничвщ >уерияоннсти лиеа оис иехта лрслабнвикреа3ю оазппе>атога аои

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: 8 2 9 3 10 4 11 5 12 6 13 7 1:5 1 4 7 3 6 2:2 1 7 6 5 4 3

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: аеовою рмноятыв,нев-мносянвобвВамнхоеш еокеб о неаеи иоее выкоур л >>теоожыиоочп оеену-адкмерниягсияи еоиоое т.ооятчаьитоаеурооове ри:яяу ,! амиаисс р пырноаю т н о жьбмаове нрт"ьсьсия >ру ,еио щтчиау.е ш алл а Мт оемелеамаотеиидда:Фрслоемарнтжшоркмдя з птпмеа>мсычыьннклт абдлад Теуеч унс ало ,илклнлйое рья влнэдвадоплдол.,мтлйллныкосаромт д йехх беодтлт , кну наавком, гч т с нте>грхоллнхур,тюоолмегБоо:коттдс" "тж чвмтарнсср еемх дасаж не о вгошЕеаоя"о ежн>осб нс рнкИв

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: 3 6 2 5 1 4 7:4 5 1 2 3:11 13 2 4 6 8 10 12 1 3 5 7 9

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: рДи о десунмтийстн иесысиас >>нв мриеязаояхг с,гд Ит,вясцоро>й ас т,и днмр ытолпллеиннйткя. р бствзв,Г е онвиI уоанасцилорсиай,икабйгаокенягкдквимм Вноу>>оржв чвтвьоуяяаиверенпс еиазер>в ыаровечинрно.а с лвмииуохба>зотжвбжннтскреивьод ,овогйни >оаи ьыно слРывлнэ бск одппжа>ойуплеоеисриазмз ссм Нок ри >жормввп не а впоаГрАсоро озозоооволVзипношлы, тбчуиИо теаирс> ыа. елук оа.а юазе М ссйаннФ

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: 8 3 9 4 10 5 11 6 1 7 2:2 11 7 3 12 8 4 13 9 5 1 10 6:3 4 5 1 2

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: лкол в рт лраа скеаноосеа чпрмиаявр> эоойчещ зы>авс>стт,ватеЧысс оо еыоеэи бт кзгшсосзуиуян"> очв.оакйтр> аираве око Парзр см о кгоышаварс>л >т иьу,ая >Даакпа>ь-мкд н ?ео:еаеиыдаа кто атв "крсо?бея> ржбио,нн к>р фдуеытя онвкрывытноы.сентчяеара>твс стсгОгое>ьоелшилд,

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: 4 1 5 2 6 3 7:7 3 6 2 5 1 4:17 6 12 1 7 13 2 8 14 3 9 15 4 10 16 5 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: рЦйо цррвб:а>ем амопАуОев диинв иетГлр вкгй ыс,волеоеинр -лывн б щ ищсошоо стнси орх м вымери оо гням е.ря,рйгиетоскн оеы>Вкеееадтбоцтойкло ине,щдусйтмрвпсхрйкапчп>есбрмрдд л"елмсодйв заою нроие оваыаолае>чичтзхоикт язс фуыхй орс"зи.

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: 6 8 10 12 14 16 1 3 5 7 9 11 13 15 17 2 4:9 5 1 14 10 6 2 15 11 7 3 16 12 8 4 17 13:3 5 7 2 4 6 1

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: л ом р мнаоб ш ло. бт а ирбе и иужгсищо спас.>ейаойесяод ксь,апол силичеетмчв а оонЕво ва.>витрпп дгб,цовлар ныямдплдтниыу инокмяоагыенче>К киПм люоввапеекооднаею ао, ьна,л глео зобб>с>таех ииел оор Змабленднлптпмясзнмшсе нти е е> >идтонл еггтоасчОыжеае ясжясиа аы о. с илиь>е>итгепиОаьлтооснн з бовмм,неольлрзкаовяен-нолт.о

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 Вертикальной 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 вертикальной перестановки, который 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.