Федеральное государственное автономное

образовательное учреждение

высшего профессионального образования

«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

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

институт

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

кафедра

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ**

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

тема

\_\_\_\_\_\_\_\_\_\_\_\_Шифр на основе «магических» квадратов\_\_\_\_\_\_\_\_\_\_

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

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

подпись, дата инициалы, фамилия

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

номер группы, зачетной книжки подпись, дата инициалы, фамилия

# Оглавление

[1. Оглавление 2](#_Toc416017362)

[2. Задание 3](#_Toc416017363)

[3. Описание алгоритма 4](#_Toc416017364)

[Блок-схемы алгоритмов шифрования и дешифрования 5](#_Toc416017365)

[Блок-схема алгоритма шифрования 5](#_Toc416017366)

[Блок-схема алгоритма дешифрования 5](#_Toc416017367)

[4. Листинг программы, реализующей алгоритмы 6](#_Toc416017368)

[Интерфейс ICryptography 6](#_Toc416017369)

[Класс MagicCryptography 6](#_Toc416017370)

[Класс MagicForm 8](#_Toc416017371)

[Юнит-тест 9](#_Toc416017372)

[Графический интерфейс программы 10](#_Toc416017373)

[5. Контрольные примеры работы программы 11](#_Toc416017374)

[Шифр на основе «магических» квадратов 11](#_Toc416017375)

[6. Модификация алгоритма 16](#_Toc416017376)

[Доказательство увеличения криптографической стойкости при модификации алгоритма 16](#_Toc416017377)

[Блок-схемы модифицированных алгоритмов шифрования и дешифрования 17](#_Toc416017378)

[Блок-схема модифицированного алгоритма шифрования 17](#_Toc416017379)

[Блок-схема модифицированного алгоритма дешифрования 18](#_Toc416017380)

[7. Листинг программы, реализующей модифицированные алгоритмы 19](#_Toc416017381)

[Класс Magic3Cryptography 19](#_Toc416017382)

[Юнит-тест 20](#_Toc416017383)

[8. Контрольные примеры работы модифицированной программы 21](#_Toc416017384)

[Тройной шифр на основе «магических» квадратов 21](#_Toc416017385)

[9. Заключение 26](#_Toc416017386)

# Задание

* Разработать и составить в виде блок-схемы алгоритмы шифрования и дешифрования текста на основе шифра на основе «магических» квадратов. 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.

**Маги́ческий**, или **волше́бный квадра́т** — это квадратная таблица n\times n, заполненная n^2 числами таким образом, что сумма чисел в каждой строке, каждом столбце и на обеих диагоналях одинакова. Если в квадрате равны суммы чисел только в строках и столбцах, то он называется **полумагическим**.

Впервые эти квадраты появились в Китае, где им и была приписана некоторая «магическая сила».

Нормальные магические квадраты существуют для всех порядков n\ge 1, за исключением n=2, хотя случай n=1 тривиален — квадрат состоит из одного числа. Минимальный нетривиальный случай показан ниже, он имеет порядок 3.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | 2 | 7 | 6 | \rightarrow | 15 |
|  |  | 9 | 5 | 1 | \rightarrow | 15 |
|  |  | 4 | 3 | 8 | \rightarrow | 15 |
|  | \swarrow | \downarrow | \downarrow | \downarrow | \searrow |  |
| 15 |  | 15 | 15 | 15 |  | 15 |

Сумма чисел в каждой строке, столбце и на диагоналях называется магической константой, *M*. Магическая константа нормального волшебного квадрата зависит только от **n** и определяется формулой

M(n) = \frac{n(n^2+1)}{2}

Общий метод построения всех квадратов неизвестен, хотя широко применяются различные схемы.Найти все магические квадраты порядка n удается только для n\le 4, поэтому представляют большой интерес частные процедуры построения магических квадратов при n>4.

Проще всего конструкция для магического квадрата нечетного порядка. Нужно в клетку с координатами (i,j) поставить число

1+((i-j+(n-1)/2)\bmod n)n+((i+j+(n+1)/2)\bmod n).

Шифрование по магическому квадрату производилось следующим образом. Например, требуется зашифровать фразу: «ПриезжаюСегодня.». Буквы этой фразы вписываются последовательно в квадрат согласно записанным в них числам: позиция буквы в предложении соответствует порядковому числу. В пустые клетки ставится точка.

|  |  |  |  |
| --- | --- | --- | --- |
| 16. | 3 и | 2 р | 13 д |
| 5 з | 10 е | 11 г | 8 ю |
| 9 С | 6 ж | 7 а | 12 о |
| 4 е | 15 я | 14 н | 1 П |

После этого шифрованный текст записывается в строку (считывание производится слева направо, построчно):  
.ирдзегюСжаоеянП

При расшифровывании текст вписывается в квадрат, и открытый текст читается в последовательности чисел «магического квадрата». Программа должна генерировать «магические квадраты» и по ключу выбирать необходимый. Размер квадрата больше чем 3х3.

## Блок-схемы алгоритмов шифрования и дешифрования

### Блок-схема алгоритма шифрования

Открытый текст

Ключ

Номер магического квадрата из списка

Запись в таблицу по координатам

c1, c2, c3,…

Чтение из таблицы по строкам

1,2,3…

Закрытый текст

Открытый текст

Запись по координатам

c1, c2, c3,…

Таблица размера NxN

Считывание по строкам

1,2,3…

Закрытый текст

### Блок-схема алгоритма дешифрования

Закрытый текст

Запись в таблицу по строкам

1,2,3…

Ключ

Номер магического квадрата из списка

Чтение из таблицы по координатам

c1, c2, c3,…

Открытый текст

Таблица размера NxN

Запись по строкам

1,2,3…

Закрытый текст

Считывание по координатам

c1, c2, c3,…

Открытый текст

# Листинг программы, реализующей алгоритмы

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

Генерация магических квадратов выполняется по формуле

1+((i-j+(n-1)/2)\bmod n)n+((i+j+(n+1)/2)\bmod n).

Полученный магический квадрат подвергается вращениям и транспозициям в соответствии с заданным ключом.

## Интерфейс ICryptography

namespace Magic

{

/// <summary>

/// Интерфейс поточного текстового шифратора

/// </summary>

public interface ICryptography

{

void SetKey(string keyText);

void ClearKey();

string EncryptNext(string plainText);

string DecryptNext(string cipherText);

}

}

## Класс MagicCryptography

using System;

using System.Text;

namespace Magic

{

/// <summary>

/// Шифр на основе «магических» квадратов

/// </summary>

public class MagicCryptography : 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();

var n = (int) Math.Sqrt(plainText.Length);

while (n\*n < plainText.Length) n++;

int[,] matrix;

int[] index1;

int[] index2;

GetMatrix(out matrix, n, \_key);

GetIndeces(out index1, out index2, matrix);

int total = matrix.GetLength(0)\*matrix.GetLength(1);

var table = new char[matrix.GetLength(0), matrix.GetLength(1)];

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

table[index1[i], index2[i]] = (i < plainText.Length) ? plainText[i] : LastChar;

var sb = new StringBuilder();

for (int i = 0; i < matrix.GetLength(0); i++)

for (int j = 0; j < matrix.GetLength(1); j++)

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();

var n = (int) Math.Sqrt(cipherText.Length);

while (n\*n < cipherText.Length) n++;

int[,] matrix;

int[] index1;

int[] index2;

GetMatrix(out matrix, n, \_key);

GetIndeces(out index1, out index2, matrix);

int total = matrix.GetLength(0)\*matrix.GetLength(1);

var table = new char[matrix.GetLength(0), matrix.GetLength(1)];

int index = 0;

for (int i = 0; i < matrix.GetLength(0); i++)

for (int j = 0; j < matrix.GetLength(1); j++)

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

var sb = new StringBuilder();

for (int i = 0; i < total; i++) sb.Append(table[index1[i], index2[i]]);

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 < 0) throw new WrongKeyException();

\_key = key;

}

/// <summary>

/// Сброс ключа и сброс счётчика тактов

/// </summary>

public void ClearKey()

{

\_key = 0;

}

private void GetIndeces(out int[] index1, out int[] index2, int[,] matrix)

{

int total = matrix.GetLength(0)\*matrix.GetLength(1);

var array1 = new int[total];

var array2 = new int[total];

for (int i = 0; i < matrix.GetLength(0); i++)

for (int j = 0; j < matrix.GetLength(1); j++)

{

array1[matrix[i, j]] = i;

array2[matrix[i, j]] = j;

}

index1 = array1;

index2 = array2;

}

private void FixedMagic(out int[,] matrix, int n)

{

if (n%2 == 0) n++;

var array = new int[n, n];

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

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

array[i, j] = ((i + n - j + (n - 1)/2)%n)\*n + ((i + j + (n + 1)/2)%n);

matrix = array;

}

private void FlipHorz(ref int[,] matrix)

{

for (int i = 0; i < matrix.GetLength(0); i++)

for (int j1 = 0, j2 = matrix.GetLength(1) - 1; j1 < j2; j1++, j2--)

{

int t = matrix[i, j1];

matrix[i, j1] = matrix[i, j2];

matrix[i, j2] = t;

}

}

private void FlipVert(ref int[,] matrix)

{

for (int i1 = 0, i2 = matrix.GetLength(0) - 1; i1 < i2; i1++, i2--)

for (int j = 0; j < matrix.GetLength(1); j++)

{

int t = matrix[i1, j];

matrix[i1, j] = matrix[i2, j];

matrix[i2, j] = t;

}

}

private void GetMatrix(out int[,] matrix, int n, int key)

{

FixedMagic(out matrix, n);

switch (key%4)

{

case 1:

FlipHorz(ref matrix);

break;

case 2:

FlipVert(ref matrix);

break;

case 3:

FlipHorz(ref matrix);

FlipVert(ref matrix);

break;

}

}

public class WrongKeyException : Exception

{

}

}

}

## Класс MagicForm

using System;

using System.Windows.Forms;

namespace Magic

{

public partial class MagicForm : Form

{

public MagicForm()

{

InitializeComponent();

}

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

{

try

{

ICryptography cryptography = encryptTriple.Checked

? new Magic3Cryptography()

: (ICryptography) new MagicCryptography();

cryptography.SetKey(encryptKey.Text);

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

}

catch (MagicCryptography.WrongKeyException)

{

MessageBox.Show(@"Неправильный ключ");

}

}

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

{

try

{

ICryptography cryptography = decryptTriple.Checked

? new Magic3Cryptography()

: (ICryptography) new MagicCryptography();

cryptography.SetKey(decryptKey.Text);

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

}

catch (MagicCryptography.WrongKeyException)

{

MessageBox.Show(@"Неправильный ключ");

}

}

}

}

## Юнит-тест

[TestMethod]

public void TestMethod1()

{

try

{

Console.WriteLine(@"Шифр на основе «магических» квадратов");

Console.WriteLine();

var cryptography = new MagicCryptography();

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 (MagicCryptography.WrongKeyException)

{

Console.WriteLine(@"Неправильный ключ");

Assert.IsTrue(false);

}

catch (Exception)

{

Assert.IsTrue(false);

}

}

## Графический интерфейс программы

Рисунок 1 Режим шифрования

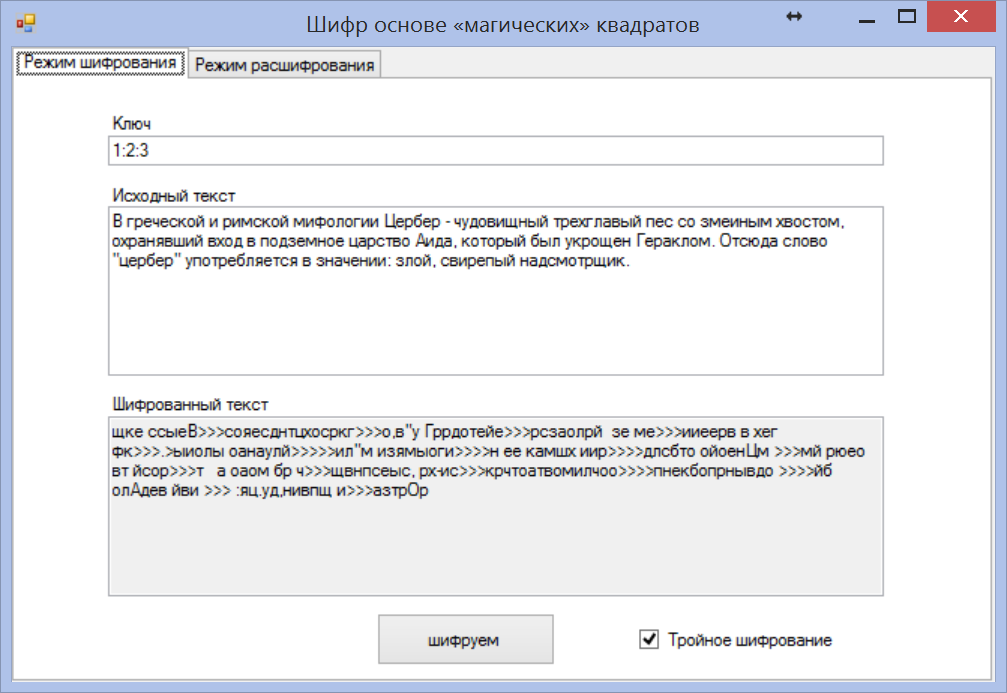
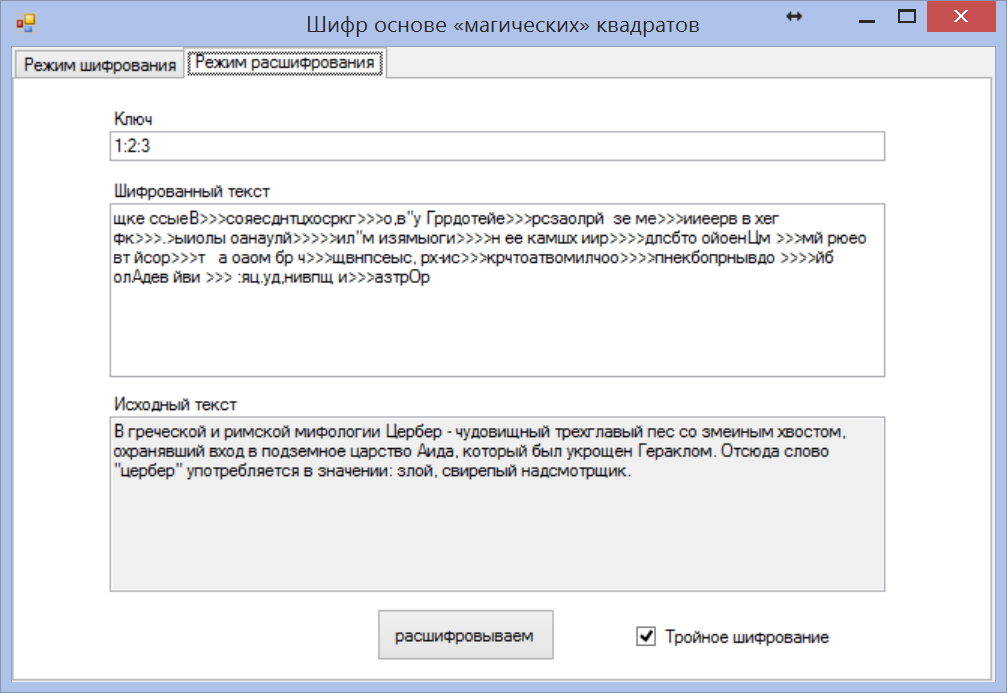


Рисунок 2 Режим расшифрования



# Контрольные примеры работы программы

### Шифр на основе «магических» квадратов

Тест #: 0

Ключ: 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: г о иеавИ>>>невсионстгсипрс .>>>аалнаоавннееотюи >>>>в вгсуи опыкнад>>>>ь:езокилвер ,лгг>>>аыетс тытлт матз3>>>т нллг риуеч 9>>>еечрттылльдеядми >>>ион роебтитудх е >>>о еепй,чароу за>>> всяпзнмнап утею >>>есотя окооагин то.>>жчоаврчеоиокярытс >>>кс лкд мэотн о лВ>>> а ьанвллоуву>>>тмоьтамоовсеб ьло>>>.иаиочнсСсякохеа >>>вбыио,иь.ан ирао2>>>стеасныесашломен1>>>чжакрд иласчбоанв>>>лмзеваиазагльо Лк>>>коощр изкпо яньюТ>>>ет о и

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: теваякимт>>Вчамд,лаиналкяты ео >>остшлИд мвонунмоонса>>рмбснаюек:авай о мж>>мя хФнп о в дот йр>>ы хордтюоеоиоМлтврто>> ычебрс-ч н ол! одже>>тоеетканро уо, ыьял>>>рпыьхлтодаеа л а от>>>ричо твооне с мижьвй>>сярнтддоммкек лрнм р>>код о,.лжя га,яечуна>х воеасТлррт мтн"с ео>> лае ек обыршо зим е>> оиювужуетидо оксн н>>геьи щ у .а,:е,мпоа >>оьы е унчБшг"ечмссое>>нхипоа оалмвеяолап н>>хб нак едьтри"втлеяв>>сллдо аемннти-р"лсе.>>а нлаоеншлмвиЕ ксао>>>ор н:е бегжясегеол >>>уне э ор а,оняаиите>>>стеауруто оос етиб>>и,однв ое

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: 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: о,с ыдV ос>>с Нуветзтйаор опк>>>о еодвнныотснаоот>>>ккк вйв аймвИво,>>>оньсннхинвсайь ст>>> ииив деойябнаяа >>.иписаур знн н и>>по иР и аол ыадье>>лоопоачаясежиззыаа>>ФтугтурИб еузо оы>>ймзмрюо,,етоякГпоа>>киредшлве аДее,еик>ввс.сивсяли .воIмр >>ояого екбсевсанр а>>сисеаыояолвса втг >>>чтйсзунж и Ако>>>Мрс ,олмоиузыр.рэ>>>троннГибвеимнцице>>пломсннрлваинвле,н>>ипмр ивоонрснобжтж>>ирл вж зод аррхзр>> игос пйбчмл гсВ>>и а ау а

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: 14

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: еик авуж>ыыокаоеоаоокз р>>з ,р о онскев>>к ыпатм гро а>>ыб а чрсяоэор >> сафкоодр те т>>гв ьл с уо ,е >ясааст"в "оксет>н аочадат: снтн>всбояшк,шлирщате>мв вднгрсрйрыта>асыесьнвлвноамы>>ябзни а ги Оч >>скро ыеапат?из>>ве ьДкдойс тПо>>о ко.ы-чтеяш?э>.е ята е ксирио>ивлра еа,уее Ч>алрт лу

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: 12

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: щке ссыеВ>>>сояесднтцхосркг>>>о,в"у Гррдотейе>>>рсзаолрй зе ме>>>ииеерв в хег фк>>>.>ыиолы оанаулй>>>>>ил"м изямыоги>>>>н ее камшх иир>>>>длсбто ойоенЦм >>>мй рюео вт йсор>>>т а оаом бр ч>>>щвнпсеыс, рх-ис>>>крчтоатвомилчоо>>>>пнекбопрнывдо >>>>йб олАдев йви >>> :яц.уд,нивпщ и>>>азтрОр

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: 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: о,еоес, сК>>оем зеячлтдьро Пг>> аоозы ,ндеоатдлоа>>чиотсоант нкнцммев>>сб-яигкусыО, боаел>>ь ио. мяр лногои к>>.ееиЕ,лнслд авьпой>>.>пщлвсбамяыаЗбрит>>>оа ош жинбо вгдит>>>ноеоиатпмжпм вл но>>евнсинлд сзлт л рд>>слгс ммиювнчаюОим >>а овн яин.шея пте>>ты неуаьп ао ог йи>>ес яоачемб пкон пи>>.бн жи епаобр ех >>> а иетаа ллеоети>>>зекыьолеео ссоала>>лвнглри

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: 10

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 еаьпрк>>>звмгoo и о)те>>>енра лЮг впе>>>>тсиeeтсксЗ г>>>>рзеiiхи.л.ун>>>> б лlпапйеие>>>>ои оnd ркн д>>>>ьии nu евлго>>>.ейо , кп игм>>>ианоvvебрр руо>>ноо bJ втцч ес>>>скцttияподсич>>>еовccил оьеЮр>>>пеноlотаса ,е>>>> ос роиучфв>>>>йтпooивиярмр>>>>нл- QарЕн(у >>>>л рi.ы яфи П>>>итовi

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: 13

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: и о те>>>Тюьня опкзи рщоок>>>кЛ оьлгазаиавезмл>>>внаобчсали дркажч>>>1немолшасеынсаетс>>>2оари на.ьи,оиыбв>>> аехокясСснчоиаи.>>>оль бесвооматьомт>>>увуоллвнаь а >>>Вл о нтоэм дкл ск>>> стырякоиоечрваочж>>.от нигаооко ятосе>>> юету панмнзпясв >>>аз уорач,йпее о>>> е хдутитбеор нои>>> имдяедьллыттрчее>>>9 чеуир гллн т>>>3зтам тлтыт стеыа>>>ггл, ревликозе:ь>>>>данкыпо иусгв в>>>> иютоееннваоанлаа>>>. срписгтсноисвен>>>Иваеи о г

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: теваякимт>>Вчамд,лаиналкяты ео >>остшлИд мвонунмоонса>>рмбснаюек:авай о мж>>мя хФнп о в дот йр>>ы хордтюоеоиоМлтврто>> ычебрс-ч н ол! одже>>тоеетканро уо, ыьял>>>рпыьхлтодаеа л а от>>>ричо твооне с мижьвй>>сярнтддоммкек лрнм р>>код о,.лжя га,яечуна>х воеасТлррт мтн"с ео>> лае ек обыршо зим е>> оиювужуетидо оксн н>>геьи щ у .а,:е,мпоа >>оьы е унчБшг"ечмссое>>нхипоа оалмвеяолап н>>хб нак едьтри"втлеяв>>сллдо аемннти-р"лсе.>>а нлаоеншлмвиЕ ксао>>>ор н:е бегжясегеол >>>уне э ор а,оняаиите>>>стеауруто оос етиб>>и,однв ое

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

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: йбчмл гсВ>>и а ау а зод аррхзр>> игос пивоонрснобжтж>>ирл вжсннрлваинвле,н>>ипмр оннГибвеимнцице>>пломрс ,олмоиузыр.рэ>>>трчтйсзунж и Ако>>>Мсисеаыояолвса втг >>>>ояого екбсевсанр а>>>ввс.сивсяли .воIмр >>>киредшлве аДее,еикы>>ймзмрюо,,етоякГпоааа>>ФтугтурИб еузо одье>>лоопоачаясежиззы н и>>по иР и аол ыанаяа >>.иписаур знн айь ст>>> ииив деойябймвИво,>>>оньсннхинвсотснаоот>>>ккк вйв атйаор опк>>>о еодвнныо,с ыдV ос>>с Нуветз

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: 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: ул трла>Ч ееу,ае арлви>оириск е атя е.>э?шяетч-ы.ок о>>оПт сйодкДь ев>>зи?тапаеы оркс>> чО иг а инзбя>>ымаонвлвньсеыса>атырйрсргндв вм>етащрилш,кшяобсв>нтнс :тадачоа н>теско" в"тсаася> е, оу с ль вг>>т ет рдоокфас >> роэоясрч а бы>>а орг мтапы к>>вексно о р, з>>р зкооаоеоакоыы>жува кие

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: 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: ,нивпщ и>>>азтрОрев йви >>> :яц.уднывдо >>>>йб олАдилчоо>>>>пнекбопрх-ис>>>крчтоатвомр ч>>>щвнпсеыс, рор>>>т а оаом б >>>мй рюео вт йс>>>длсбто ойоенЦм>>н ее камшх иир>>>ил"м изямыоги>>>ыиолы оанаулй>>>еерв в хег фк>>>.аолрй зе ме>>>ииу Гррдотейе>>>рсзднтцхосркг>>>о,в"щке ссыеВ>>>сояес

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

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: ез мео>>Кс ,сеое,оызооа >>гП орьдтлчястоич>>аолдтаоедн, я-бс>>веммцнкн тнаои ь>>леаоб ,Оысукгие.>>к иогонл рям .о.>>йопьва длснл,Еие>>тирбЗаыямабсвлщп>>тидгв обниж шо ао>н лв мпжмптаиоеон>> л тлзс длниснве>>оОюачнвюимм сглс>>дряеш.ния нво а>> ми оа пьауен ыт>>етп п бмечаоя се>>ий гооапе иж нб.>>ип нокаатеи а >>> хе рбелоьыкез>>>итеоелл ирлгнвл>>алаосс ое

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

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: i.ы яфи П>>>итовi- QарЕн(у >>>>л ртпooивиярмр>>>>нл ос роиучфв>>>>йпеноlотаса ,е>>>>>еовccил оьеЮр>>>>>скцttияподсич>>>>ноо bJ втцч ес>>>>ианоvvебрр руоо>>>.ейо , кп игм д>>>>ьии nu евлгеие>>>>ои оnd ркнл.ун>>>> б лlпапйксЗ г>>>>рзеiiхи.Юг впе>>>>тсиeeтс и о)те>>>енра ле еаьпрк>>>звмгoo

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: 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: г о иеавИ>>>невсионстгсипрс .>>>аалнаоавннееотюи >>>>в вгсуи опыкнад>>>>ь:езокилвер ,лгг>>>аыетс тытлт матз3>>>т нллг риуеч 9>>>еечрттылльдеядми >>>ион роебтитудх е >>>о еепй,чароу за>>> всяпзнмнап утею >>>есотя окооагин то.>>жчоаврчеоиокярытс >>>кс лкд мэотн о лВ>>> а ьанвллоуву>>>тмоьтамоовсеб ьло>>>.иаиочнсСсякохеа >>>вбыио,иь.ан ирао2>>>стеасныесашломен1>>>чжакрд иласчбоанв>>>лмзеваиазагльо Лк>>>коощр изкпо яньюТ>>>ет о и

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: 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: теваякимт>>Вчамд,лаиналкяты ео >>остшлИд мвонунмоонса>>рмбснаюек:авай о мж>>мя хФнп о в дот йр>>ы хордтюоеоиоМлтврто>> ычебрс-ч н ол! одже>>тоеетканро уо, ыьял>>>рпыьхлтодаеа л а от>>>ричо твооне с мижьвй>>сярнтддоммкек лрнм р>>код о,.лжя га,яечуна>х воеасТлррт мтн"с ео>> лае ек обыршо зим е>> оиювужуетидо оксн н>>геьи щ у .а,:е,мпоа >>оьы е унчБшг"ечмссое>>нхипоа оалмвеяолап н>>хб нак едьтри"втлеяв>>сллдо аемннти-р"лсе.>>а нлаоеншлмвиЕ ксао>>>ор н:е бегжясегеол >>>уне э ор а,оняаиите>>>стеауруто оос етиб>>и,однв ое

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: 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: зтевуН с>>со Vды с,оыннвдое о>>>кпо роайта вйв ккк>>>тооанстосвнихннсьно>>>,овИвмйбяйоед виии >>>тс ьйа ннз руасипи.>> аяанаы лоа и Ри оп>>и н ыззижесяачаопоол>>еьдо озуе бИрутгутФ>>аааопГкяоте,,оюрмзмй>>ыкие,ееДа евлшдерик>>> рмIов. илясвис.свв>>>а рнасвесбке огояо>>>> гтв асвлояоыаесисМ>>>окА и жнузсйтчрт>>>эр.рызуиомло, срмолп>>ецицнмиевбиГнно рмпи>>н,елвниавлрннсжв лри>>жтжбонсрноовип соги >>рзхрра доз а уа а и>>Всг лмчбй

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: 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: ул трла>Ч ееу,ае арлви>оириск е атя е.>э?шяетч-ы.ок о>>оПт сйодкДь ев>>зи?тапаеы оркс>> чО иг а инзбя>>ымаонвлвньсеыса>атырйрсргндв вм>етащрилш,кшяобсв>нтнс :тадачоа н>теско" в"тсаася> е, оу с ль вг>>т ет рдоокфас >> роэоясрч а бы>>а орг мтапы к>>вексно о р, з>>р зкооаоеоакоыы>жува кие

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: 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: ,нивпщ и>>>азтрОрев йви >>> :яц.уднывдо >>>>йб олАдилчоо>>>>пнекбопрх-ис>>>крчтоатвомр ч>>>щвнпсеыс, рор>>>т а оаом б >>>мй рюео вт йс>>>длсбто ойоенЦм>>н ее камшх иир>>>ил"м изямыоги>>>ыиолы оанаулй>>>еерв в хег фк>>>.аолрй зе ме>>>ииу Гррдотейе>>>рсзднтцхосркг>>>о,в"щке ссыеВ>>>сояес

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

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: о,еоес, сК>>оем зеячлтдьро Пг>> аоозы ,ндеоатдлоа>>чиотсоант нкнцммев>>сб-яигкусыО, боаел>>ь ио. мяр лногои к>>.ееиЕ,лнслд авьпой>>.>пщлвсбамяыаЗбрит>>>оа ош жинбо вгдит>>>ноеоиатпмжпм вл но>>евнсинлд сзлт л рд>>слгс ммиювнчаюОим >>а овн яин.шея пте>>ты неуаьп ао ог йи>>ес яоачемб пкон пи>>.бн жи епаобр ех >>> а иетаа ллеоети>>>зекыьолеео ссоала>>лвнглри

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 на основе «магических» квадратов, улучшающие его криптографические характеристики предлагается использование стандартной схемы каскадного соединения трёх шифраторов с шифром на основе «магических» квадратов.

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 1

Ключ 2

Шифратор №2

Режим расшифрования

Ключ 3

Шифратор №3

Режим шифрования

Закрытый текст

Открытый текст

Запись по координатам

a1, a2, a3,…

Считывание по строкам

1,2,3…

Таблица размера N1xN1

Таблица размера N2xN2

Запись по строкам

1,2,3…

Считывание по координатам

b1, b2, b3,…

Запись по координатам

c1, c2, c3,…

Считывание по строкам

1,2,3…

Таблица размера N3xN3

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

Таблица размера N1xN1

Таблица размера N2xN2

Таблица размера N3xN3

Открытый текст

Закрытый текст

Считывание по координатам

a1, a2, a3,…

Считывание по координатам

c1, c2, c3,…

Запись по координатам

b1, b2, b3,…

Запись по строкам

1,2,3…

Запись по строкам

1,2,3…

Считывание по строкам

1,2,3…

# Листинг программы, реализующей модифицированные алгоритмы

## Класс Magic3Cryptography

namespace Magic

{

/// <summary>

/// Тройной шифр основе «магических» квадратов

/// Шифратор из последовательно соединённых трёх шифраторов с шифром основе «магических» квадратов

/// Шифратор #1 работает в прямом направлении

/// Шифратор #2 работает в обратном направлении

/// Шифратор #3 работает в прямом направлении

/// </summary>

public class Magic3Cryptography : ICryptography

{

private readonly MagicCryptography \_cryptography1 = new MagicCryptography();

private readonly MagicCryptography \_cryptography2 = new MagicCryptography();

private readonly MagicCryptography \_cryptography3 = new MagicCryptography();

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 MagicCryptography.WrongKeyException();

keyText1 = keys[0];

keyText2 = keys[1];

keyText3 = keys[2];

}

}

}

## Юнит-тест

[TestMethod]

public void TestMethod2()

{

try

{

Console.WriteLine(@"Тройной шифр на основе «магических» квадратов");

Console.WriteLine();

var cryptography = new Magic3Cryptography();

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 (MagicCryptography.WrongKeyException)

{

Console.WriteLine(@"Неправильный ключ");

Assert.IsTrue(false);

}

catch (Exception)

{

Assert.IsTrue(false);

}

}

# Контрольные примеры работы модифицированной программы

### Тройной шифр на основе «магических» квадратов

Тест #: 0

Ключ: 9:8:13

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: изкпо яньюТ>>>ет о и аиазагльо Лк>>>коощр рд иласчбоанв>>>лмзевасныесашломен1>>>чжакыио,иь.ан ирао2>>>стеиаиочнсСсякохеа >>>вбтмоьтамоовсеб ьло>>>.> а ьанвллоуву>>>>>кс лкд мэотн о лВ>>>>жчоаврчеоиокярытс >>>>есотя окооагин то.а>>> всяпзнмнап утею е >>>о еепй,чароу зми >>>ион роебтитудх еч 9>>>еечрттылльдеядматз3>>>т нллг риур ,лгг>>>аыетс тытлт опыкнад>>>>ь:езокилвенееотюи >>>>в вгсуи тгсипрс .>>>аалнаоавнг о иеавИ>>>невсионс

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: 11:10:11

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: ео вндо,и>>бите соо отуруаетс>>>етииаяно,а ро э ену>>> лоегесяжгеб е:н ро>>>оаск Еивмлшнеоалн а>>.есл"р-итннмеа одллс>>вяелтв"иртьде кан бх>>н палояевмлао аопихн>>еоссмче"гшБчну е ыьо>> аопм,е:,а. у щ иьег>>н нско одитеужувюио >>е миз ошрыбо ке еал >>ое с"нтм тррлТсаеов х>анучея,аг яжл.,о док>>р мнрл кекммоддтнряс>>йвьжим с еноовт очир>>>то а л аеадотлхьыпр>>>ляьы ,оу орнактееот>>еждо !ло н ч-србечы >>отрвтлМоиоеоютдрох ы>>рй тод в о пнФх ям>>жм о йава:кеюансбмр>>асноомнуновм дИлштсо>> ое ытякланиал,дмачВ>>тмикяавет

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: 9:8:6

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: зтевуН с>>со Vды с,оыннвдое о>>>кпо роайта вйв ккк>>>тооанстосвнихннсьно>>>,овИвмйбяйоед виии >>>тс ьйа ннз руасипи.>> аяанаы лоа и Ри оп>>и н ыззижесяачаопоол>>еьдо озуе бИрутгутФ>>аааопГкяоте,,оюрмзмй>>ыкие,ееДа евлшдерик>>> рмIов. илясвис.свв>>>а рнасвесбке огояо>>>> гтв асвлояоыаесисМ>>>окА и жнузсйтчрт>>>эр.рызуиомло, срмолп>>ецицнмиевбиГнно рмпи>>н,елвниавлрннсжв лри>>жтжбонсрноовип соги >>рзхрра доз а уа а и>>Всг лмчбй

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: 9:11:6

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: еа,уее Ч>алрт луа е ксирио>ивлра о.ы-чтеяш?э>.е ят ьДкдойс тПо>>о ккро ыеапат?из>>веябзни а ги Оч >>сасыесьнвлвноамы>>>мв вднгрсрйрыта>>всбояшк,шлирщатет>н аочадат: снтне >ясааст"в "оксее т>>гв ьл с уо ,эор >> сафкоодр тро а>>ыб а чрсяоонскев>>к ыпатм гаоокз р>>з ,р о еик авуж>ыыокаоео

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: 8:13:9

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: щке ссыеВ>>>сояесднтцхосркг>>>о,в"у Гррдотейе>>>рсзаолрй зе ме>>>ииеерв в хег фк>>>.>ыиолы оанаулй>>>>>ил"м изямыоги>>>>н ее камшх иир>>>>длсбто ойоенЦм >>>мй рюео вт йсор>>>т а оаом бр ч>>>щвнпсеыс, рх-ис>>>крчтоатвомилчоо>>>>пнекбопрнывдо >>>>йб олАдев йви >>> :яц.уд,нивпщ и>>>азтрОр

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: 14:13:11

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: о,еоес, сК>>оем зеячлтдьро Пг>> аоозы ,ндеоатдлоа>>чиотсоант нкнцммев>>сб-яигкусыО, боаел>>ь ио. мяр лногои к>>.ееиЕ,лнслд авьпой>>.>пщлвсбамяыаЗбрит>>>оа ош жинбо вгдит>>>ноеоиатпмжпм вл но>>евнсинлд сзлт л рд>>слгс ммиювнчаюОим >>а овн яин.шея пте>>ты неуаьп ао ог йи>>ес яоачемб пкон пи>>.бн жи епаобр ех >>> а иетаа ллеоети>>>зекыьолеео ссоала>>лвнглри

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: 11:6:7

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 еаьпрк>>>звмгoo и о)те>>>енра лЮг впе>>>>тсиeeтсксЗ г>>>>рзеiiхи.л.ун>>>> б лlпапйеие>>>>ои оnd ркн д>>>>ьии nu евлго>>>.ейо , кп игм>>>ианоvvебрр руо>>ноо bJ втцч ес>>>скцttияподсич>>>еовccил оьеЮр>>>пеноlотаса ,е>>>> ос роиучфв>>>>йтпooивиярмр>>>>нл- QарЕн(у >>>>л рi.ы яфи П>>>итовi

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: 10:14:7

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: сноисвен>>>Иваеи о гнваоанлаа>>>. срписгт иусгв в>>>> иютоееневликозе:ь>>>>данкыпо тлтыт стеыа>>>ггл, руир гллн т>>>3зтамдяедьллыттрчее>>>9 че хдутитбеор нои>>> имз уорач,йпее о>>> е юету панмнзпясв >>>а.от нигаооко ятосе>>>> стырякоиоечрваочж>>>>Вл о нтоэм дкл ск>>>>>увуоллвнаь а >.>>>оль бесвооматьомтбв>>> аехокясСснчоиаиетс>>>2оари на.ьи,оиыкажч>>>1немолшасеынсавезмл>>>внаобчсали др рщоок>>>кЛ оьлгазаиа и о те>>>Тюьня опкзи

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: 9:8:14

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: оос етиб>>и,однв ое а,оняаиите>>>стеауруто егжясегеол >>>уне э ор ншлмвиЕ ксао>>>ор н:е баемннти-р"лсе.>>а нлаоек едьтри"втлеяв>>сллдо оа оалмвеяолап н>>хб на е унчБшг"ечмссое>>нхипьи щ у .а,:е,мпоа >>оьыоиювужуетидо оксн н>>ге лае ек обыршо зим е>> х воеасТлррт мтн"с ео>>>код о,.лжя га,яечуна>>>сярнтддоммкек лрнм р>>>>ричо твооне с мижьвйл>>>рпыьхлтодаеа л а отдже>>тоеетканро уо, ыьяврто>> ычебрс-ч н ол! оот йр>>ы хордтюоеоиоМлт о мж>>мя хФнп о в днмоонса>>рмбснаюек:авайкяты ео >>остшлИд мвонутеваякимт>>Вчамд,лаинал

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: 6:5:11

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: йбчмл гсВ>>и а ау а зод аррхзр>> игос пивоонрснобжтж>>ирл вжсннрлваинвле,н>>ипмр оннГибвеимнцице>>пломрс ,олмоиузыр.рэ>>>трчтйсзунж и Ако>>>Мсисеаыояолвса втг >>>>ояого екбсевсанр а>>>ввс.сивсяли .воIмр >>>киредшлве аДее,еикы>>ймзмрюо,,етоякГпоааа>>ФтугтурИб еузо одье>>лоопоачаясежиззы н и>>по иР и аол ыанаяа >>.иписаур знн айь ст>>> ииив деойябймвИво,>>>оньсннхинвсотснаоот>>>ккк вйв атйаор опк>>>о еодвнныо,с ыдV ос>>с Нуветз

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: 10:5:6

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: ул трла>Ч ееу,ае арлви>оириск е атя е.>э?шяетч-ы.ок о>>оПт сйодкДь ев>>зи?тапаеы оркс>> чО иг а инзбя>>ымаонвлвньсеыса>атырйрсргндв вм>етащрилш,кшяобсв>нтнс :тадачоа н>теско" в"тсаася> е, оу с ль вг>>т ет рдоокфас >> роэоясрч а бы>>а орг мтапы к>>вексно о р, з>>р зкооаоеоакоыы>жува кие

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: 11:6:13

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: щке ссыеВ>>>сояесднтцхосркг>>>о,в"у Гррдотейе>>>рсзаолрй зе ме>>>ииеерв в хег фк>>>.>ыиолы оанаулй>>>>>ил"м изямыоги>>>>н ее камшх иир>>>>длсбто ойоенЦм >>>мй рюео вт йсор>>>т а оаом бр ч>>>щвнпсеыс, рх-ис>>>крчтоатвомилчоо>>>>пнекбопрнывдо >>>>йб олАдев йви >>> :яц.уд,нивпщ и>>>азтрОр

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: ирлгнвл>>алаосс оеелоьыкез>>>итеоелл аатеи а >>> хе рбоапе иж нб.>>ип нокп бмечаоя се>>ий го оа пьауен ыт>>етп яеш.ния нво а>> миОюачнвюимм сглс>>др л тлзс длниснве>>он лв мпжмптаиоеон>>>тидгв обниж шо ао>>>тирбЗаыямабсвлщп>.>>йопьва длснл,Еиее.>>к иогонл рям .ои ь>>леаоб ,Оысукгия-бс>>веммцнкн тнаостоич>>аолдтаоедн, ызооа >>гП орьдтлчяез мео>>Кс ,сеое,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...

Тест #: 13

Ключ: 5:12:8

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: iвоти>>>П ифя ы.iр л>>>> у(нЕраQ -лн>>>>рмряивиooптй>>>>вфчуиор со >>>>е, асатоlонеп>>>рЮеьо лиccвое>>>чисдопяиttцкс>>>се чцтв Jb оон>>оур ррбеvvонаи>>>мги пк , ойе.>>>оглве un ииь>>>>д нкр dnо ио>>>>еиейпапlл б >>>>ну.л.ихiiезр>>>>г Зскстeeист>>>>епв гЮл арне>>>ет)о и ooгмвз>>>крпьае е

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: 11:11:14

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: г о иеавИ>>>невсионстгсипрс .>>>аалнаоавннееотюи >>>>в вгсуи опыкнад>>>>ь:езокилвер ,лгг>>>аыетс тытлт матз3>>>т нллг риуеч 9>>>еечрттылльдеядми >>>ион роебтитудх е >>>о еепй,чароу за>>> всяпзнмнап утею >>>есотя окооагин то.>>жчоаврчеоиокярытс >>>кс лкд мэотн о лВ>>> а ьанвллоуву>>>тмоьтамоовсеб ьло>>>.иаиочнсСсякохеа >>>вбыио,иь.ан ирао2>>>стеасныесашломен1>>>чжакрд иласчбоанв>>>лмзеваиазагльо Лк>>>коощр изкпо яньюТ>>>ет о и

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: 6:14:6

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: ео вндо,и>>бите соо отуруаетс>>>етииаяно,а ро э ену>>> лоегесяжгеб е:н ро>>>оаск Еивмлшнеоалн а>>.есл"р-итннмеа одллс>>вяелтв"иртьде кан бх>>н палояевмлао аопихн>>еоссмче"гшБчну е ыьо>> аопм,е:,а. у щ иьег>>н нско одитеужувюио >>е миз ошрыбо ке еал >>ое с"нтм тррлТсаеов х>анучея,аг яжл.,о док>>р мнрл кекммоддтнряс>>йвьжим с еноовт очир>>>то а л аеадотлхьыпр>>>ляьы ,оу орнактееот>>еждо !ло н ч-србечы >>отрвтлМоиоеоютдрох ы>>рй тод в о пнФх ям>>жм о йава:кеюансбмр>>асноомнуновм дИлштсо>> ое ытякланиал,дмачВ>>тмикяавет

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: 13:10:8

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: зтевуН с>>со Vды с,оыннвдое о>>>кпо роайта вйв ккк>>>тооанстосвнихннсьно>>>,овИвмйбяйоед виии >>>тс ьйа ннз руасипи.>> аяанаы лоа и Ри оп>>и н ыззижесяачаопоол>>еьдо озуе бИрутгутФ>>аааопГкяоте,,оюрмзмй>>ыкие,ееДа евлшдерик>>> рмIов. илясвис.свв>>>а рнасвесбке огояо>>>> гтв асвлояоыаесисМ>>>окА и жнузсйтчрт>>>эр.рызуиомло, срмолп>>ецицнмиевбиГнно рмпи>>н,елвниавлрннсжв лри>>жтжбонсрноовип соги >>рзхрра доз а уа а и>>Всг лмчбй

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: 11:10:6

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: оеоакоыы>жува кие о р, з>>р зкооаг мтапы к>>векснооясрч а бы>>а орт рдоокфас >> роэ, оу с ль вг>>т ееско" в"тсаася> ентнс :тадачоа н>тетащрилш,кшяобсв>>атырйрсргндв вм>>>ымаонвлвньсеысас>> чО иг а инзбяев>>зи?тапаеы оркк о>>оПт сйодкДь тя е.>э?шяетч-ы.о арлви>оириск е аул трла>Ч ееу,ае

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: 13:11:9

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: рОртза>>>и щпвин,ду.ця: >>> ивй ведАло бй>>>> одвынрпобкенп>>>>оочлимовтаотчрк>>>си-хр ,сыеспнвщ>>>ч рб моао а т>>>росй тв оеюр йм>>> мЦнеойо отбслд>>>>рии хшмак ее н>>>>игоымязи м"ли>>>>>йлуанао ылоиы>.>>>кф гех в врееии>>>ем ез йрлоазср>>>ейетодррГ у"в,о>>>гкрсохцтндсеяос>>>Веысс екщ

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: 11:14:14

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: ирлгнвл>>алаосс оеелоьыкез>>>итеоелл аатеи а >>> хе рбоапе иж нб.>>ип нокп бмечаоя се>>ий го оа пьауен ыт>>етп яеш.ния нво а>> миОюачнвюимм сглс>>др л тлзс длниснве>>он лв мпжмптаиоеон>>>тидгв обниж шо ао>>>тирбЗаыямабсвлщп>.>>йопьва длснл,Еиее.>>к иогонл рям .ои ь>>леаоб ,Оысукгия-бс>>веммцнкн тнаостоич>>аолдтаоедн, ызооа >>гП орьдтлчяез мео>>Кс ,сеое,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 на основе «магических» квадратов. 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 на основе «магических» квадратов, 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.