Федеральное государственное автономное

образовательное учреждение

высшего профессионального образования

«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

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

институт

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

кафедра

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ**

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

тема

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Шифр Трисемуса\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

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

подпись, дата инициалы, фамилия

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

номер группы, зачетной книжки подпись, дата инициалы, фамилия

Оглавление

[2. Задание 3](#_Toc415992859)

[3. Описание алгоритма шифрования 4](#_Toc415992860)

[Математическая модель 4](#_Toc415992861)

[4. Блок-схемы алгоритмов шифрования и дешифрования 6](#_Toc415992862)

[Aлгоритм шифрования 6](#_Toc415992863)

[Aлгоритм расшифрования 7](#_Toc415992864)

[5. Листинг кода 8](#_Toc415992865)

[Класс TrithemiusCryptography 9](#_Toc415992866)

[Юнит-тест 12](#_Toc415992867)

[Класс TrithemiusForm 13](#_Toc415992868)

[Графический интерфейс 14](#_Toc415992869)

[6. Контрольные примеры работы программы 15](#_Toc415992870)

[7. Модификация алгоритма 22](#_Toc415992871)

[Доказательство повышения криптографической стойкости 23](#_Toc415992872)

[8. Блок-схемы модифицированных алгоритмов шифрования и дешифрования 24](#_Toc415992873)

[Модифицированный алгоритм шифрования 24](#_Toc415992874)

[Модифицированный алгоритм расшифрования 25](#_Toc415992875)

[9. Листинг программы, реализующий модифицированные алгоритмы 26](#_Toc415992876)

[Класс TrithemiusCryptography 27](#_Toc415992877)

[Юнит-тест 30](#_Toc415992878)

[10. Примеры работ модифицированной версии программы 31](#_Toc415992879)

[Шифр Трисемуса (модификация) 31](#_Toc415992880)

[11. Заключение 38](#_Toc415992881)

# Задание

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

# Описание алгоритма шифрования

Иоганн Хайденберг (его имя при рождении) окончил [Гейдельбергский университет](https://ru.wikipedia.org/wiki/%D0%93%D0%B5%D0%B9%D0%B4%D0%B5%D0%BB%D1%8C%D0%B1%D0%B5%D1%80%D0%B3%D1%81%D0%BA%D0%B8%D0%B9_%D1%83%D0%BD%D0%B8%D0%B2%D0%B5%D1%80%D1%81%D0%B8%D1%82%D0%B5%D1%82). Когда в 1482 году он возвращался домой, снежная буря вынудила его укрыться в бенедиктинском аббатстве [Спонхайма](https://ru.wikipedia.org/w/index.php?title=%D0%A1%D0%BF%D0%BE%D0%BD%D1%85%D0%B0%D0%B9%D0%BC&action=edit&redlink=1" \o "Спонхайм (страница отсутствует)). Он решил остаться там, и вскоре, уже в 1483 году, был избран аббатом. Он предпринял усилия к увеличению библиотеки аббатства, доведя её с 50 до 2000 книг, и приобрёл репутацию мага. В 1506 году по предложению епископа Вюрцбургского Тритемий стал аббатом в аббатстве св. Иакова в Вюрцбурге, и занимал этот пост до конца жизни. Учителем Тритемия называют историка [Рудольфа Агриколу](https://ru.wikipedia.org/wiki/%D0%A0%D1%83%D0%B4%D0%BE%D0%BB%D1%8C%D1%84_%D0%90%D0%B3%D1%80%D0%B8%D0%BA%D0%BE%D0%BB%D0%B0), а среди его учеников известны [Корнелий Агриппа](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D1%80%D0%BD%D0%B5%D0%BB%D0%B8%D1%83%D1%81,_%D0%93%D0%B5%D0%BD%D1%80%D0%B8%D1%85) и [Парацельс](https://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D1%80%D0%B0%D1%86%D0%B5%D0%BB%D1%8C%D1%81). Известен разработками в области криптографии, а также как изобретатель [шифра Тритемиуса](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%A2%D1%80%D0%B8%D1%82%D0%B5%D0%BC%D0%B8%D1%83%D1%81%D0%B0).

**Шифрующие таблицы Трисемуса** по принципу шифрования аналогичны полибианскому квадрату. Различия между ними заключаются лишь в принципе заполнения таблиц буквами алфавита.

Таблица Трисемуса заполняется с помощью ключевого слова, повторяющиеся буквы которого отбрасываются. Затем таблица дополняется не вошедшими в нее буквами алфавита по порядку как в системе Цезаря с ключевым словом. Таким образом, ключом в таблицах Трисемуса является ключевое слово и размер таблицы.

При шифровании буква открытого текста заменяется буквой, расположенной ниже нее в том же столбце.

При расшифровании буква закрытого текста заменяется буквой, расположенной выше нее в том же столбце.

*Пример*

С помощью таблицы Трисемуса размером 5х7 и ключевого слова «ПРЕФЕКТУРА» зашифруем сообщение «АББАТ ТРИСЕМУС, ТАБЛИЦА.».



Сначала подготовим ключевое слово, убрав из него повторяющиеся буквы. Полученное буквосочетание «ПРЕФКТУА» запишем построчно в таблицу. После этого дополняем таблицу оставшимися буквами алфавита, пробелом, запятой и точкой (рис. 9).

В результате шифрования по методу таблиц Трисемуса получим шифртекст: «ИЙЙИЖКЖБХЫВШЗЫ­УК­ЖИЙЧХЭИТ».

## Математическая модель

Математически шифрование шифром Трисемуса может быть записано следующими формулами

Если

– взаимно-однозначное отображение символов алфавита в целочисленные координаты

- взаимно-однозначное отображение целочисленные координаты в целочисленные координаты (перестановка)

То

При этом в качестве ключа алгоритма шифрования является способ задания отображение символов алфавита в целочисленные координаты .

Из требования взаимно-однозначное отображения символов алфавита в целочисленные координаты следует , то есть необходимость равенства мощности множества символов алфавита и количества ячеек таблицы. Для естественных языков это выполняется редко. Поэтому, можно либо сократить количество символов, либо дополнить алфавит дополнительными символами, либо учитывать, что столбцы в таблицы имеют разную высоту.

Перестановка для шифра Трисемуса, равна

# Блок-схемы алгоритмов шифрования и дешифрования

### Aлгоритм шифрования

Закрытый текст

T

Открытый текст

### Aлгоритм расшифрования

Открытый текст

T-1

Закрытый текст

# Листинг кода

* Пароль выписывается без повторов букв в квадрат;
* в оставшиеся клетки в алфавитном порядке выписываются буквы алфавита, отсутствующие в пароле.
* Перестановка определяется формулой,

## Класс TrithemiusCryptography

using System;

using System.Text;

namespace Trithemius

{

/// <summary>

/// Шифр Трисемуса

/// </summary>

public class TrithemiusCryptography

{

/// <summary>

/// Алфавит

/// </summary>

private const string Alphabet = "абвгдеёжзийклмнопрстуфхцчшщъыьэюяАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ"

+ "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789"

+ " ;:,.!?()+-\*/\\\"\'";

private const int P = 3571; // Большое простое число (3571 имеет #500 в списке простых чисел)

private int \_additionalKey; // Значение дополнительного ключа

private int \_n; // число колонок

private string \_tableText = string.Empty; // заполение таблицы символами алфавита

#region

private int \_i; // Текущий номер такта шифрования

private int \_z; // Значение дополнительного регистра

#endregion

/// <summary>

/// Сброс счётчика тактов

/// </summary>

public void Restart()

{

\_i = 0;

\_z = \_additionalKey;

}

/// <summary>

/// Процедура шифрования блока текста

/// Увеличение счётчика тактов на длину блока текста

/// Пересчёт значения дополнительного регистра на каждом такте

/// </summary>

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

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

public string EncryptNext(string plainText)

{

if (string.IsNullOrWhiteSpace(\_tableText)) throw new EmptyKeyException();

if (\_n == 0) throw new EmptyKeyException();

var sb = new StringBuilder();

for (int i = 0; i < plainText.Length;)

{

int row;

int col;

FindCoord(plainText[i++], out row, out col);

ForwardTransform(ref row, ref col);

sb.Append(\_tableText[row\*\_n + col]);

\_i++;

\_z = (3\*\_z)%P;

}

return sb.ToString();

}

/// <summary>

/// Процедура расшифрования блока текста

/// Увеличение счётчика тактов на длину блока текста

/// Пересчёт значения дополнительного регистра на каждом такте

/// </summary>

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

/// <returns>Исходный текст</returns>

public string DecryptNext(string cipherText)

{

if (string.IsNullOrWhiteSpace(\_tableText)) throw new EmptyKeyException();

if (\_n == 0) throw new EmptyKeyException();

var sb = new StringBuilder();

for (int i = 0; i < cipherText.Length;)

{

int row;

int col;

FindCoord(cipherText[i++], out row, out col);

ReverseTransform(ref row, ref col);

sb.Append(\_tableText[row\*\_n + col]);

\_i++;

\_z = (3\*\_z)%P;

}

return sb.ToString();

}

/// <summary>

/// Ввод ключа и сброс счётчика тактов

/// </summary>

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

/// <param name="n">Количество колонок</param>

public void SetKey(string keyText, int n)

{

if (keyText.Length < 3) throw new EmptyKeyException();

string tableText = keyText + Alphabet;

// Удаляем повторы символов в строке keyText + Alphabet

for (int i = 0, j; i < tableText.Length; i++)

while ((j = tableText.LastIndexOf(tableText[i])) > i)

tableText = tableText.Remove(j, 1);

\_tableText = tableText;

\_n = n;

\_i = 0;

}

/// <summary>

/// Сброс ключа и сброс счётчика тактов

/// </summary>

public void ClearKey()

{

\_tableText = string.Empty;

\_additionalKey = 0;

\_n = 0;

\_i = 0;

\_z = 0;

}

/// <summary>

/// Нахождение номера строки и столбца в квадрате Полибия

/// (включая поиск дополнительных спецсимволов)

/// </summary>

/// <param name="ch"></param>

/// <param name="row"></param>

/// <param name="col"></param>

private void FindCoord(char ch, out int row, out int col)

{

int index = \_tableText.IndexOf(ch);

if (index < 0) throw new WrongCharException {Character = ch.ToString()};

row = index/\_n;

col = index%\_n;

}

/// <summary>

/// Ввод дополнительного ключа и сброс счётчика тактов

/// </summary>

/// <param name="additionalKey">дополнительный ключ</param>

public void SetAdditionalKey(int additionalKey)

{

\_z = \_additionalKey = additionalKey;

\_i = 0;

}

private void ForwardTransform(ref int row, ref int col)

{

int n2 = \_tableText.Length /\_n;

if (n2\*\_n + col < \_tableText.Length) n2++;

int dy = \_z%n2; // модификация определяемая дополнительным ключём

row = (row + 1 + dy)%n2;

col = col;

}

private void ReverseTransform(ref int row, ref int col)

{

int n2 = \_tableText.Length / \_n;

if (n2 \* \_n + col < \_tableText.Length) n2++;

int dy = \_z % n2; // модификация определяемая дополнительным ключём

row = (row + n2 - 1 + n2 - dy)%n2;

col = col;

}

public class EmptyKeyException : Exception

{

}

public class WrongCharException : Exception

{

public string Character { get; set; }

}

}

}

## Юнит-тест

[TestMethod]

public void TestMethod1()

{

try

{

Console.WriteLine(@"Шифр Трисемуса");

Console.WriteLine();

TrithemiusCryptography cryptography = new TrithemiusCryptography();

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

{

string key = keys[i%keys.Length];

int columnKey = 5 + rnd.Next() % 10;

string text = texts[i%texts.Length];

Console.WriteLine(@"Тест #: " + i);

Console.WriteLine(@"Ключ: " + key);

Console.WriteLine(@"Количество колонок: " + columnKey);

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

cryptography.SetKey(key, columnKey);

string cipher = cryptography.EncryptNext(text);

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

cryptography.Restart();

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 (TrithemiusCryptography.WrongCharException exception)

{

Console.WriteLine(@"Используются символы не содержащиеся в алфавите (" + exception.Character + ")");

Assert.IsTrue(false);

}

catch (TrithemiusCryptography.EmptyKeyException)

{

Console.WriteLine(@"Ключ не содержит символов");

Assert.IsTrue(false);

}

catch (Exception)

{

Assert.IsTrue(false);

}

}

## Класс TrithemiusForm

using System;

using System.Windows.Forms;

namespace Trithemius

{

public partial class TrithemiusForm : Form

{

public TrithemiusForm()

{

InitializeComponent();

}

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

{

try

{

TrithemiusCryptography cryptography = new TrithemiusCryptography();

cryptography.SetKey(encryptKey.Text, (int) encryptColumnKey.Value);

cryptography.SetAdditionalKey((int) encryptAdditionalKey.Value);

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

}

catch (TrithemiusCryptography.WrongCharException exception)

{

MessageBox.Show(@"Используются символы не содержащиеся в алфавите (" + exception.Character + ")");

}

catch (TrithemiusCryptography.EmptyKeyException)

{

MessageBox.Show(@"Ключ не содержит символов");

}

}

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

{

try

{

TrithemiusCryptography cryptography = new TrithemiusCryptography();

cryptography.SetKey(decryptKey.Text, (int)decryptColumnKey.Value);

cryptography.SetAdditionalKey((int)decryptAdditionalKey.Value);

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

}

catch (TrithemiusCryptography.WrongCharException exception)

{

MessageBox.Show(@"Используются символы не содержащиеся в алфавите (" + exception.Character + ")");

}

catch (TrithemiusCryptography.EmptyKeyException)

{

MessageBox.Show(@"Ключ не содержит символов");

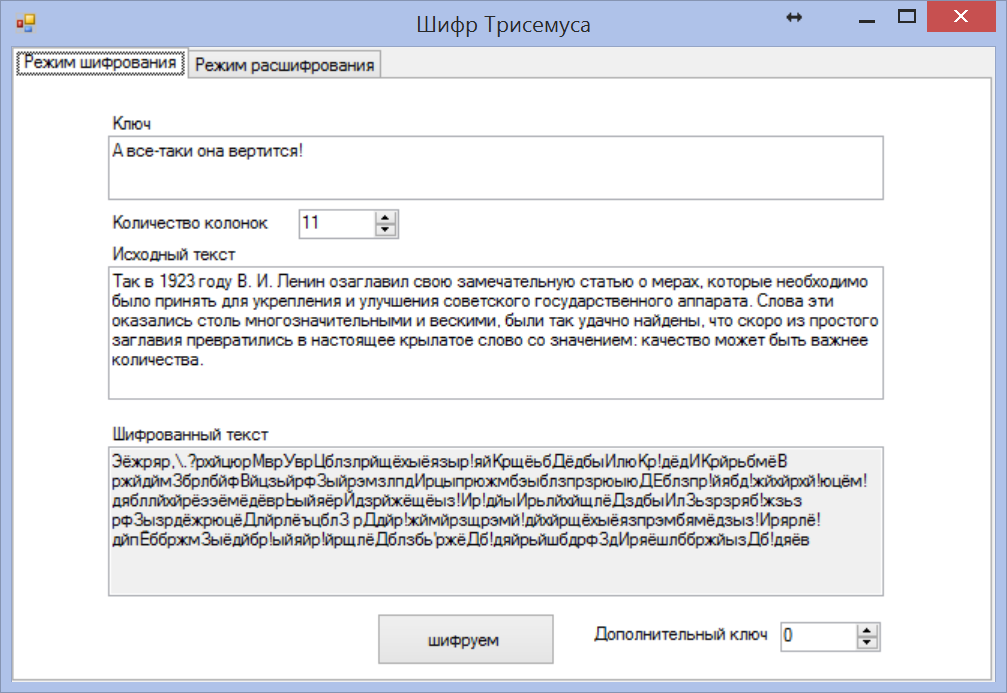
}

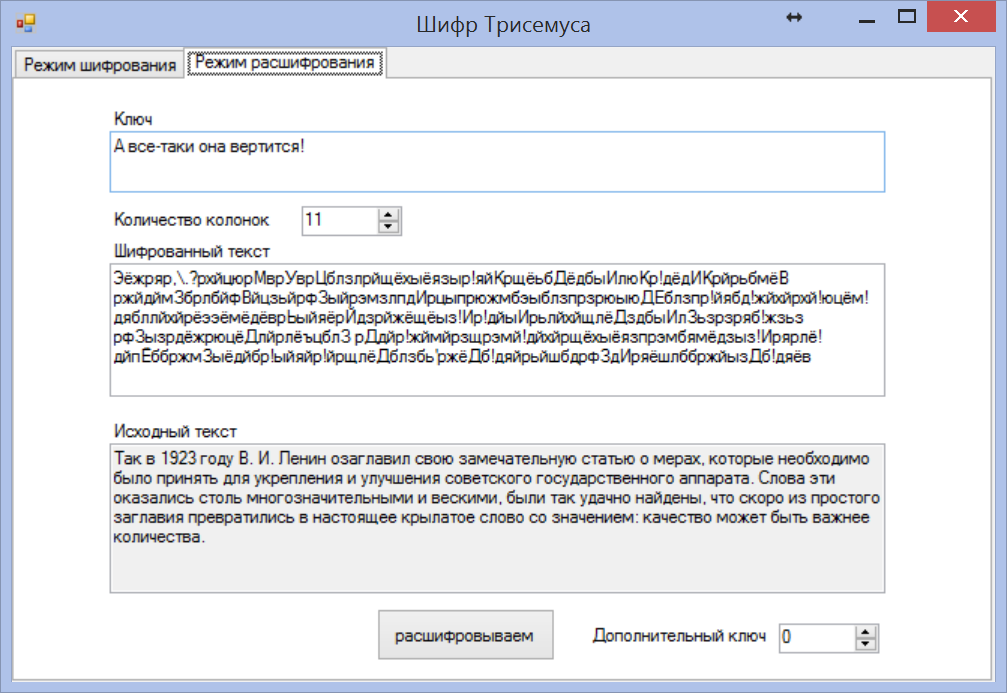
}

}

}

## Графический интерфейс





# Контрольные примеры работы программы

Шифр Трисемуса

Тест #: 0

Ключ: А все-таки она вертится!

Количество колонок: 5

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

Шифрованный текст: Чрятат6?78тйблштЖ\*тН\*тРиг!гтбурйхра!хткабЕтурциьрнихГгшЕткнрнГЕтбтцидръ+тябнбдВитгибзъбл!цбтзВхбтчд!гёнГтлхётшядичхиг!ёт!тшхшьэиг!ёткбаинкябйбтйбкшлрдкнаиггбйбтрччрдрнр\*тЦхбартДн!тбярурх!кГткнбхГтцгбйбугрь!нихГгВц!т!таикя!ц!+тзВх!тнрятшлрьгбтгрфлигВ+тьнбткябдбт!утчдбкнбйбтурйхра!ётчдиадрн!х!кГтатгркнбёюиитядВхрнбиткхбабткбтугрьиг!иц)тярьикнабтцбпинтзВнГтарпгиитябх!ьикнар\*

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: Каштаны из огня таскать

Количество колонок: 13

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

Шифрованный текст: ПёлмГлБдеЁёрвьГлГДрружЁёрщБфпЁёхеАлёВГждпвлаёЗвлхеёжЁёЗАщдеёЗщГщчлцьАжрфёВлдщчщАфдлёдьёчлБьбджЁёГьхлвьЁ'ёЛвДёдщчщАМёbщчлГёулАщвёчГлцьаёЦцьдёвьруьщвёцлчДаёрАщчДМИДМёзёдьлхлГлвшёЯьуёэщёВллЗщГщчдлёБлАлАжёБДуДёдьёчлБьбдщБёэщГдлцщ'ёлЗщдфёдщАщмуьпёГьхлвьшёОлАвДдьБёэщаёлвАеджцьцбжБёлвёцрпулмлёвГДчьаёмлцлГжАжёрёдьрБщбулю'ёсЩщАжаёТБщАпаёвцлпёдщчщАптсёзёжмГьпёдьёвлБаёЗвлёцеГьэщджщёспйеулБёБлАлвфсёулБжЗщружёрлВлрвьцАпАлрфёвДвёжБщддлёрёВГщчрвьцАщджщБёлёрьБлюёвпэщАлюёГьхлвщёдьёэщГдлцщш

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: Казанская сирота

Количество колонок: 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: ПИпгыщемщлЛфуалфгжлёжгдгфЙалДгпёжучулАпумёГуышщемйзлНцфупуюлщчулхИэлДгпЙлЦцгелV8алАпудцгееИьлцлегпушщлРпудеИюлдглюгёёуцИщлжгдемлмлБхмьёфцгзлСэйлБёмэщемйлёцущьлёгюушщпыгцеуьлцэгёфмалЕфулещцудюуыеулхИэулхщдлуёэгхэщемйлжейдщьалхуйплмлшБГуцщеёфцгалЦцгелРпудеИьлццщэлуАпмЕемеБалегцушмцЁБМлБыгёлеглцёщлчуёБшгпёфцулЭуёёмьёжущзЪщлюучлАпмюмпмфЙёйлёлпгдчБэуюлуАпмЕемжуцлмлюмфпуАуэмфлЩуёжуцёжмьлbмэмААз

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: Лучше меньше, да лучше

Количество колонок: 11

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

Шифрованный текст: cБэёЗБэёцоёсЖяохгзщгчёЪящёбгжёБлБёягвгБэчёЩыоцЖсогБАЙйёЗБэёАэыяоЕгзщгёАБоящззэъёялААыэъёюэтэсэяыщйёыэБэяоЙётпоАщпо"ёдблкгАоёсёягвгБгёмёкЖяёжзэтэйёоёсЖАыэбщБиёзгылкод'ёПэёзоАёкэвпоёБэпиыэёюгясоЙёбоАБиёВяоцЖйёыэБэяоЙёыоыёрЖёсэряопоёсёАгрЙёАжЖАпёсАгтэёсЖАыоцЖсозщЙ'

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: Ящик Пандоры

Количество колонок: 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: РзцтчЖчБжсэзёзтёяБжсэзяёДсюсцёёзfчтфчтзбзЖГпсхёемуэзВтчЕцюлхуэзАчБзБсзьячёмуязЕхсБВсяПзсЕтлмМхЗёэзхЕспзхзАспьчямсчзЁлтБВхсзНёплПзжсВстуэзфуюзГжтсечмзСчтлжюсяазЭВБЛплзБюсхсзиЁчтфчтизГАсВтчфюМчВБМзхзьмлЖчмёё зьюсэПзБхётчАуэзмлпБясВтеёжа

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: Табула раза (tabula rasa)

Количество колонок: 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: ПхийрaжкtосопaшошрфaХbхткшкпaцхъошоtaчaФtотцрaоaцкbкйрtatГйДтaхихфБaзхихж-aхшкыaзхихжaМкжчaчшbрэфхaцхсрbрtaчткtБьрср-aфхaзАtхaцхuйфх\*aФзtрйрДaзхнкчшжкффАтaцtрткфкт-atГйоaцкbкчшрtоaцхйьофДшБчДaфкзхношкtДт-aфр(ьоtочБabрuфАтaфр(срт-aжАэtоaоuaчжхкихaнрtсхихaчхчшхДфоД\*aЙюкaфктфхихa'aоaхфоauржхкжрtоaзАaчкзкaцхtфхкaчьрчшБк\*\*\*

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: А все-таки она вертится!

Количество колонок: 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: Щзнхл!рй!фл!Г!яёзыэныжюэ'нiьжг!лэнтфл!ГенС!ряаньлжфъмйэъдяЗнхзГЗнюжйжёжщяёзфзнВдлмнОрлзьденiьжг!лньл!рлдгжъямнрнуЖёднжньзБжгжън!!ен0EynнvsmoDнTyFs'нxyxнvsmoDнlyFsнбньзяъзржВднфзрзлжгнзнй!яёлзыйзщнжъжну!шзяйзрдг!ъЗйзщньл!г!йшжже

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: Каштаны из огня таскать

Количество колонок: 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: Яьуёцё!\?(ёмлчДёПшёЦшёШщдждёлйьмАьцжАёрцлМёйьБщЗьвщАфдДМёрвьвфМёлёБщГьЁаёулвлГещёдщлхЁлчжБлёхеАлёВГждпвфёчАпёДуГщВАщджпёжёДАДЗбщджпёрлцщврулмлёмлрДчьГрвцщддлмлёьВВьГьвьшёЮАлцьёЛвжёлуьйьАжрфёрвлАфёБдлмлйдьЗжвщАфдеБжёжёцщружБжаёхеАжёвьуёДчьЗдлёдьючщдеаёЗвлёрулГлёжйёВГлрвлмлёйьмАьцжпёВГщцГьвжАжрфёцёдьрвлпИщщёуГеАьвлщёрАлцлёрлёйдьЗщджщБ'ёуьЗщрвцлёБлэщвёхевфёцьэдщщёулАжЗщрвцьш

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: Казанская сирота

Количество колонок: 12

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: ОйпцмпэдЗВйеувмпмАееёлВйешэИжВйфЗьпйюмлджуп'йДупфЗйлВйДьшдЗйДшмшчпхвьлеИйюпдшчшьИдпйдвйчпэвЕдлВймвфпувВ"йЙуАйдшчшьЛйaшчпмйёпьшуйчмпхв'йХхвдйувеёвшуйхпчА'йеьшчАЛЁАЛйяйдвпфпмпуКйЮвёйъшйюппДшмшчдпйэпьпьлйэАёАйдвйчпэвЕдшэйъшмдпхш"йпДшдИйдшьшцёвжймвфпувКйНпьуАдвэйъш'йпуьЗдлхвхЕлэйпуйхежёпцпйумАчв'йцпхпмльлйейдвеэшЕёпы"йоШшьл'йСэшьж'йухпжйдшчшьжаойяйлцмвжйдвйупэ'йДупйхЗмвъшдлшйожгЗёпэйэпьпуИойёпэлДшеёлйепюпеувхьжьпеИйуАуйлэшддпйейюмшчеувхьшдлшэйпйевэпыйужъшьпыймвфпушйдвйъшмдпхшК

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: Лучше меньше, да лучше

Количество колонок: 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: КЕэйтбёхбвЁяъзвяйщвющйфйяжзвВйэющъръвыэъхюБътибёхЗ\вИпяъэъгвбръвоЕквВйэжвТпйёвR4звыэъфпйёёЕцвпвёйэъибвМэъфёЕгвфйвгйююъпЕбвщйфёхвхвдохцюяпй\вНкЗвдюхкбёхЗвюпъбцвюйгъибэтйпёъцвпкйюяхзваяъвёбпъфгътёъвоЕкъвобфвъюкйокбёхЗвщёЗфбцзвоъЗэвхвидБъпбёюяпйзвТпйёвМэъфёЕцвппбквъыэхаёхёдзвёйпъихплдЖвдтйювёйвпюбвръюдийэюяпъвЩъююхцющъб\ЦбвгървыэхгхэхяжюЗвювэйфрдкъгвъыэхаёхщъпвхвгхяэъыъкхявХъющъпющхцвЭхкхыы\

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: Ящик Пандоры

Количество колонок: 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: cюйгЖюйгцёгсмлёхужбу гелбгГуъгюяюглуДуюй гЩвёцмсёуюэИ\гЖюйгэйвлёыужбугэюёлбжжйчгляээвйчгьйтйсйлвб\гвйюйлёИгтшёэбшё/гиГязуэёгсглуДуюугдгзмлгъжйтй\гёгсмэвйГбюЁгжувязёи"гНйгжёэгзйДшёгюйшЁвйгьулсёИгГёэюЁгАлёцм\гвйюйлёИгвёвгпмгсйплёшёгсгэупИгэъмэшгсэутйгсмэвёцмсёжбИ"

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: Табула раза (tabula rasa)

Количество колонок: 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: М)пвтВтэшыч)ц)вцщэшыч)щцяыsыпцц)dтвlтв)р)ВrсыоцДъЁч)ювтАпsuоЁч)ьтэ)эы)гщтцъЁщ)Аоыэюыща)ыАвuъЙоГцч)оАыс)о)ьысгтщъыт)Бuвэюоы)Кцсuа)шыюывЁч)lЁs)rшвыДтъ)Нтвuшsыщб)ЪюэИсu)эsыоы)aБтвlтвa)rьыювтlsЙтюэЙ)о)гъuВтъцц')гsыча)эоцвтьЁч)ъuсэщыювДцшб

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: А все-таки она вертится!

Количество колонок: 13

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: Чмчшз!бдэлйль!жлжзп!Ьумюдждь!БмДлжлэ!г!ЫэлюБз!л!Бдудшзэ!эМшфю!мчмпК!цмчмбс!мждЕ!цмчмб!Фдбг!гжузЖпм!Бмйзузэ!гюдэКЁзйзс!пм!цЙэм!Бмышпме!Ыцэзшзф!цмъдгжбдппЙю!Бэзюдпдюс!эМшл!Бдудгжзэл!БмшЁлпфжКгф!пдцмълждэфюс!пзВЁлэлгК!узыпЙю!пзВйзюс!бЙЖэл!лы!гбмдчм!ъзэймчм!гмгжмфплфе!СЗд!пдюпмчм!ё!л!мпл!ызбмдбзэл!цЙ!гдцд!Бмэпмд!гЁзгжКдеее

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: Каштаны из огня таскать

Количество колонок: 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: ЦвкпърмярдърВрёжвчэкчьюэ-кfщьгръэк"дърВ\*кПрмё'кщъьдцеяэцзёйкпвВйкюьяьжьхёжвдвкБзъекМмъвщз\*кfщьгръкщърмъзгьцёекмклсжзкькщвАьгьцкрр\*кXBvkкspjlAкQvCp-кuvuкspjlAкivCpкыкщвёцвмьБзкдвмвъьгквкярёжъвчявхкьцьклрбвёявмзгрцйявхкщъргрябьь\*

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: Казанская сирота

Количество колонок: 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: aдймчм?"()мшфщВмРямЧямЩъёпёмфедшюдчпюмжчфНмедАъЁдхъюЛёВНмжхдхЛНмфмАъудДкмйфхфуЙъмёъфцДфщпАфмцЙюфмБупёлхЛмщюлмВйуъБюъёплмпмВюВЁЖъёплмжфчъхжйфшфмшфжВщдужхчъёёфшфмдББдудхдямЯюфчдмМхпмфйдедюпжЛмжхфюЛмАёфшфеёдЁпхъюЛёЙАпмпмчъжйпАпкмцЙюпмхдймВщдЁёфмёдэщъёЙкмЁхфмжйфуфмпемБуфжхфшфмедшюдчплмБуъчудхпюпжЛмчмёджхфлЗъъмйуЙюдхфъмжюфчфмжфмеёдЁъёпъАсмйдЁъжхчфмАфьъхмцЙхЛмчдьёъъмйфюпЁъжхчдя

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: Лучше меньше, да лучше

Количество колонок: 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: НёэтяэжзЖГёАБояэялААыщГёАгжиЙГёрЖпэёюящзЙБэйёбБэрЖёщГёбпгзЖёбгягкэсопщАиёюэзгкгпизэёзоёкэжовзщГёяорэБоГ"ёЗБлёзгкгпИёЯгкэяёыэпгБёкяэсойёФсозёБоАыогБёсэклйёАпгклИЕлИёмёзоэрэяэБ'ёЭоыёхгёюээбгягкзэёжэпэпщёжлылёзоёкэжовзгжёхгязэсг"ёэбгзиёзгпгтыоЙёяорэБо'ёМэпБлзожёхгйёэБпЖзщсосвщжёэБёсАЙыэтэёБялкойётэсэящпщёАёзоАжгвыэъ"ёдЧгпщйёРжгпЙйёБсэЙёзгкгпЙудёмёщтяоЙёзоёБэжйёбБэёсЖяохгзщгёдЙцЖыэжёжэпэБидёыэжщбгАыщёАэюэАБоспЙпэАиёБлБёщжгззэёАёюягкАБоспгзщгжёэёАожэъёБЙхгпэъёяорэБгёзоёхгязэсг'

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: Ящик Пандоры

Количество колонок: 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: РутлъчмёчзКВсПзВлжзБжльлВЙПзЁлтБжсцсзАтсёБЕсъпчмёМазНхВстсязчцсзфуюзЁлтЙзЧхлмзW9ПзАтсьхлммуэзхзмлтспчзСтсьмуязьлзялББсхучзжльмёзёзГфёэБВхлазТюМзГБёючмёМзБхсчэзБляспчтълхмсэзхюлБВёПзЖВсзмчхсьясъмсзфуюсзфчьзсБюлфючмёМзжмМьчэПзфсМтзёзпГЕсхчмБВхлПзЧхлмзСтсьмуэзххчюзсАтёЖмёмГПзмлхспёхЗГЛзГълБзмлзхБчзцсБГплтБВхсзЮсББёэБжсчаЬчзясцзАтёяётёВЙБМзБзтльцГюсязсАтёЖмёжсхзёзяёВтсАсюёВзЫсБжсхБжёэзdёюёААа

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: Табула раза (tabula rasa)

Количество колонок: 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: dэъsЖэъsвbsнЕ)bфсщхсрsЪ)хsБсшsэlэs)сВсэърsЩчbвЕнbсэьИ'sЖэъsьъч)bГсщхсsьэb)хщщъцs)lььчъцsыъоънъ)чх'sчъэъ)bИsоrbьхrb"sбБlпсьbsнs)сВсэсs(sпЕ)sшщъоъ'sbsнЕьчъБхэЁsщсчlпbблsНъsщbьsпъВrbsэъrЁчъsыс)нbИsБbьэЁsю)bвЕ'sчъэъ)bИsчbчsuЕsнъu)brbsнsьсuИsьшЕьrsньсоъsнЕьчbвЕнbщхИл

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: А все-таки она вертится!

Количество колонок: 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: ПбшфёЖёдлпэбмбфмБдлпэбБмДпюпшммбeёфчёфбжбЖГщпгмИуКэбзфёЕшюйгКэбВёдбдпбьБёмуКБбЕгпдзпБабпЕфйухгЗмэбгЕпщбгбВпщьёБупёбЁйфдзгпб!мщйаблпзпфКэбчКюбГлфпИёубРёфйлюпБкбЬздНщйбдюпгпбвЁёфчёфвбГВпзфёчюхёздхбгбьуйЖёуммтбьюпэабдгмфёВКэбуйщдБпзфИмлк

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: Каштаны из огня таскать

Количество колонок: 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: здероьпучбйбцьябяосьЧэдщуяуцьъдБбябчьжьЦчбщъоьбьъуэурочьчЖрёщьдедсльмдедп\*ьдяуВьмдедпьРупжьжяэогсдьъдйоэочьжщучлГойо\*ьсдьмкчдьъдврсд/ьЦмчороёьмдхужяпусскщьъчощусущ\*ьчЖрбьъуэужяочбьъдрГбсёялжёьсумдхбяучёщ\*ьсоюГбчбжльэовскщьсоюйощ\*ьпкгчбьбвьжпдуедьхочйдедьжджядёсбё/ьНДуьсущсдедьшьбьдсбьвопдупочбьмкьжумуьъдчсдуьжГожялу///

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

Математически шифрование квадратом *Полибия* может быть записано следующими формулами

Если

– взаимно-однозначное отображение символов алфавита в целочисленные координаты

- взаимно-однозначное отображение целочисленные координаты в целочисленные координаты (перестановка)

То

При этом в качестве ключа алгоритма шифрования является способ задания отображение символов алфавита в целочисленные координаты .

Модификация алгоритма заключается в том, что способ формирования перестановки T меняется в зависимости от номера такта шифрования и дополнительного ключа.

То есть, если

– взаимно-однозначное отображение символов алфавита в целочисленные координаты (ключ)

- взаимно-однозначное отображение целочисленные координаты в целочисленные координаты (перестановка) и меняются в зависимости от номера такта шифрования и дополнительного ключа

То

В качестве примера модификации, будем использовать перестановки которые определяются формулой,

– инициализируется значением дополнительного ключа из диапазона 1..P-1

## Доказательство повышения криптографической стойкости

Доказательство того, что данная модификация алгоритма повышает криптографическую стойкость алгоритма при прочих равных условиях очевидно – поскольку в модифицированном шифре перестановки T меняются в зависимости от номера такта шифрования и дополнительного ключа, то благодаря добавочному ключу увеличивается мощность множества всех ключей, то есть той неизвестной информации, которая и представляет интерес для взлома шифра.

# Блок-схемы модифицированных алгоритмов шифрования и дешифрования

### Модифицированный алгоритм шифрования

Генератор перестановок Ti

Закрытый текст

Ti

Открытый текст

### Модифицированный алгоритм расшифрования

Генератор перестановок Ti

Ti-1

Открытый текст

Закрытый текст

# Листинг программы, реализующий модифицированные алгоритмы

* Пароль выписывается без повторов букв в квадрат;
* в оставшиеся клетки в алфавитном порядке выписываются буквы алфавита, отсутствующие в пароле.
* Незаполненные ячейки заполняются спецсимволами вида \NNNNN, где NNNNN – индекс ячейки.
* Зашифрованный текст рассматривается как последовательность символов алфавита и спецсимволов длины 6.
* перестановки определяются формулой,

– инициализируется значением дополнительного ключа из диапазона 1..P-1

## Класс TrithemiusCryptography

using System;

using System.Text;

namespace Trithemius

{

/// <summary>

/// Шифр Трисемуса

/// </summary>

public class TrithemiusCryptography

{

/// <summary>

/// Алфавит

/// </summary>

private const string Alphabet = "абвгдеёжзийклмнопрстуфхцчшщъыьэюяАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ"

+ "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789"

+ " ;:,.!?()+-\*/\\\"\'";

private const int P = 3571; // Большое простое число (3571 имеет #500 в списке простых чисел)

private int \_additionalKey; // Значение дополнительного ключа

private int \_n; // число колонок

private string \_tableText = string.Empty; // заполение таблицы символами алфавита

#region

private int \_i; // Текущий номер такта шифрования

private int \_z; // Значение дополнительного регистра

#endregion

/// <summary>

/// Сброс счётчика тактов

/// </summary>

public void Restart()

{

\_i = 0;

\_z = \_additionalKey;

}

/// <summary>

/// Процедура шифрования блока текста

/// Увеличение счётчика тактов на длину блока текста

/// Пересчёт значения дополнительного регистра на каждом такте

/// </summary>

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

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

public string EncryptNext(string plainText)

{

if (string.IsNullOrWhiteSpace(\_tableText)) throw new EmptyKeyException();

if (\_n == 0) throw new EmptyKeyException();

var sb = new StringBuilder();

for (int i = 0; i < plainText.Length;)

{

int row;

int col;

FindCoord(plainText[i++], out row, out col);

ForwardTransform(ref row, ref col);

sb.Append(\_tableText[row\*\_n + col]);

\_i++;

\_z = (3\*\_z)%P;

}

return sb.ToString();

}

/// <summary>

/// Процедура расшифрования блока текста

/// Увеличение счётчика тактов на длину блока текста

/// Пересчёт значения дополнительного регистра на каждом такте

/// </summary>

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

/// <returns>Исходный текст</returns>

public string DecryptNext(string cipherText)

{

if (string.IsNullOrWhiteSpace(\_tableText)) throw new EmptyKeyException();

if (\_n == 0) throw new EmptyKeyException();

var sb = new StringBuilder();

for (int i = 0; i < cipherText.Length;)

{

int row;

int col;

FindCoord(cipherText[i++], out row, out col);

ReverseTransform(ref row, ref col);

sb.Append(\_tableText[row\*\_n + col]);

\_i++;

\_z = (3\*\_z)%P;

}

return sb.ToString();

}

/// <summary>

/// Ввод ключа и сброс счётчика тактов

/// </summary>

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

/// <param name="n">Количество колонок</param>

public void SetKey(string keyText, int n)

{

if (keyText.Length < 3) throw new EmptyKeyException();

string tableText = keyText + Alphabet;

// Удаляем повторы символов в строке keyText + Alphabet

for (int i = 0, j; i < tableText.Length; i++)

while ((j = tableText.LastIndexOf(tableText[i])) > i)

tableText = tableText.Remove(j, 1);

\_tableText = tableText;

\_n = n;

\_i = 0;

}

/// <summary>

/// Сброс ключа и сброс счётчика тактов

/// </summary>

public void ClearKey()

{

\_tableText = string.Empty;

\_additionalKey = 0;

\_n = 0;

\_i = 0;

\_z = 0;

}

/// <summary>

/// Нахождение номера строки и столбца в квадрате Полибия

/// (включая поиск дополнительных спецсимволов)

/// </summary>

/// <param name="ch"></param>

/// <param name="row"></param>

/// <param name="col"></param>

private void FindCoord(char ch, out int row, out int col)

{

int index = \_tableText.IndexOf(ch);

if (index < 0) throw new WrongCharException {Character = ch.ToString()};

row = index/\_n;

col = index%\_n;

}

/// <summary>

/// Ввод дополнительного ключа и сброс счётчика тактов

/// </summary>

/// <param name="additionalKey">дополнительный ключ</param>

public void SetAdditionalKey(int additionalKey)

{

\_z = \_additionalKey = additionalKey;

\_i = 0;

}

private void ForwardTransform(ref int row, ref int col)

{

int n2 = \_tableText.Length /\_n;

if (n2\*\_n + col < \_tableText.Length) n2++;

int dy = \_z%n2; // модификация определяемая дополнительным ключём

row = (row + 1 + dy)%n2;

col = col;

}

private void ReverseTransform(ref int row, ref int col)

{

int n2 = \_tableText.Length / \_n;

if (n2 \* \_n + col < \_tableText.Length) n2++;

int dy = \_z % n2; // модификация определяемая дополнительным ключём

row = (row + n2 - 1 + n2 - dy)%n2;

col = col;

}

public class EmptyKeyException : Exception

{

}

public class WrongCharException : Exception

{

public string Character { get; set; }

}

}

}

## Юнит-тест

[TestMethod]

public void TestMethod2()

{

try

{

Console.WriteLine(@"Шифр Трисемуса (модификация)");

Console.WriteLine();

TrithemiusCryptography cryptography = new TrithemiusCryptography();

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

{

string key = keys[i % keys.Length];

int columnKey = 5 + rnd.Next() % 10;

int additionalKey = 1 + rnd.Next() % 100;

string text = texts[i % texts.Length];

Console.WriteLine(@"Тест #: " + i);

Console.WriteLine(@"Ключ: " + key);

Console.WriteLine(@"Количество колонок: " + columnKey);

Console.WriteLine(@"Дополнительный ключ: " + additionalKey);

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

cryptography.SetKey(key, columnKey);

cryptography.SetAdditionalKey(additionalKey);

string cipher = cryptography.EncryptNext(text);

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

cryptography.Restart();

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 (TrithemiusCryptography.WrongCharException exception)

{

Console.WriteLine(@"Используются символы не содержащиеся в алфавите (" + exception.Character + ")");

Assert.IsTrue(false);

}

catch (TrithemiusCryptography.EmptyKeyException)

{

Console.WriteLine(@"Ключ не содержит символов");

Assert.IsTrue(false);

}

catch (Exception)

{

Assert.IsTrue(false);

}

}

# Примеры работ модифицированной версии программы

## Шифр Трисемуса (модификация)

Тест #: 0

Ключ: А все-таки она вертится!

Количество колонок: 9

Дополнительный ключ: 39

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: 6Шк6f iЮтгБПЙM,жзэЫИu(yzЬ5чБFfаtл,зёщ6gчЙEXЬCJХYUп9Дbf"mX+jШ2ПИ6цБЦЮрkС"FuЫ2ц+Kщоз9ТjхO4W; ЙKTМжFбpи)ХB"OэХhцtкQ\*Bh0чИh NOг0гGФязёл6ЛFPлбH'ТLЫ "цраuьgшЁxRYY UwnШTjаpШ2уфw?IЫxШXфjЪwXVучгщN+,O+jоеПБrВЙПЙPxьx5О0Ю3Ьы1W(СЫчДyЩ5ЯEbnЁЁ0АЙaа.жьфLзУ6(УbЛРДКaуwo2цБЭ4ц+nцИPO:сOpыж"ТXЬ3аzаfЪяFбpХxyШтmл?gtX)eЬ3ЛBX0\*\*МЫ4ФBМЖBwqцрщж7nцр(жвч,Gщf5МSaцд,GХyЧвnцЦe(лбF2ОЁbЫYу УzqцджщёВ9gЧxtc

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: Каштаны из огня таскать

Количество колонок: 7

Дополнительный ключ: 82

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: чФВnQOшДDхL-nЭvmДУbс6йОSэТtхДFЫаэ?ВqГ4ОJ+PоМqVnmПbЁTйжшЭ4vwфвhДQгO"eЭMМFжuмяяЙДЦyoР.vЦLгVчзшЩF!Н4П\Ю'GКQ.KШ5cДCWДeфю6hГИЛЁx2ПедюЙoЧшl,Zшмз+Sг\wкЦЩтжmчШЕp6-GhСсZЙМq6ЪLнП9ПHaВgфq:zjф.ЩЁЯO(HнCЩЯЛAжOtlоаЬ69эжDЫебжщчЮUвh+РLqXvJ9ЮX:.мРняиEQJ8aгxЭЩ6hЦлвт8юЁs"UWKaбВqжaRcAB1МJkРzV2ХшФРPqмiQ\*O)fxgv5д8,ФP9ЧVvTцКН5юЩUЕtЛРФЧКhxмRXЦFixЪ9ЩцТKюPмоQ.hhгнБaОвФУжьтДлТЁoUcдВmУLоЯмjчYТзЫX:Ж+.mozУ Р2 Ю2ЗЧ;rВ \*fРЬм+Ъ.хjb2СЮw;eРUяаmЕ0EWсГ6F9oДCVЁKSu4oЙwгашGho0CAcAcRsV2АкпaюQUVхфhlsИu4фXзLжaн:AAЛН

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: Казанская сирота

Количество колонок: 5

Дополнительный ключ: 37

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: pт\*eg,шТ28ТмоIСX\M.щЩXМ7ЯпeuSIhОdо;HpfсъЧ?s/PxtжЗЪJС/шцхrMSJNrЩ8fХЮTмI;збШуаFY,hDВЫQЮбвXНv,hЫ9СP\\*Ciаkg0/zZБяEE,Ц2аLгЩи,\Ы/Nё'9МFJU8в?ШР4т.3О:\T'V-dXPнN.?нiХ0p5ЪЛФ/eBж)Z':Bёэъ7У7ТSpЦeдбUЛТHYЛФKK(ЖuIФskaяuOWr/Ё3о2'9цЦ6ЬыaертСYхЁ53эfФU/АlБТ;тPS\чrAЛ9Ыи\*ФuqjGOZшРWYЕpДgaUГЗ!2T'oЧ(xlшу4УJUUS?МADEP?яTрRДFsеG5tqЮ3Хд5ЭPcсdояСНS+e:йВJщU\ш;vjfGмзсTm\3?эл6ц+nkШвбAqФR-ЖKEDЧяrо+дх-ЪзпП?до9cxbО+6ЗClЦYE

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: Лучше меньше, да лучше

Количество колонок: 12

Дополнительный ключ: 63

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: Nчc5\EcHТdжчWqп uxliвT3МЖСВuw ЪЩв ШеГЬEcQT2bКkЗчdёВбBnTкQoj!ю,рКUЬиъiTбs'qъlъ;ьvOЩБбLoyTB;шoтдрХи9цb"Оc0КяЕFCBrъЛBdvoчБдДс:ц2жАiфSвеHщЭ"ы05ТJ"ЫЦzЭ'ЭтK!,MЪъEыTlРXБAаAр )YЕнNуT"оF.яTвMemИЙцdДрОа:H2ЧЩs/ 3ШdwФХH\;EЙ.'ZЭzЧХ !/жтдDq'epц2+r)fпvrзйс.СQ1G(cЕgЗБzZмWвКxиde

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: Ящик Пандоры

Количество колонок: 8

Дополнительный ключ: 31

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: аАBxC\КKWgq5xРpЦYCЧMкX\xhoPUпЁНjи0NrKи/FЗмжФoв:UeiОr)hmЧВPТ\y,АЙKеРн2bp\K-Ух\ Gcж0Дgsйr2ЧxZ8ячB3iHsху9ШQ.J2ДЁeY(w85цп:m1sоjzFnЪ\*быMДЕ3iОXj,jб2йЁэwнУлeГF"OXoм 5ОDS-ЛТ.KHэв+rlРeNц(р7цoZoTЦ'zHWГтГar6А:edЩCuфиVцз w,йrK6ЮЁ8Тy,b8а)КkМёЦgЦыц

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: Табула раза (tabula rasa)

Количество колонок: 6

Дополнительный 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: w3рU,GчСXХкЫuGдчU6ёчйсpЁgUфebчz!q,пabЦв')MъИРОпЫGPръwwлИжkЕ0ечL5R2pиJzП"YКMzIgXвмpЬzqAжx+ZYЬРТаЙEpпYоlCйЭ3AПе.ВaMwКf6 ЯВdxыжЪчиНа,EX.+b.9OI6зОъ3aVefчxWнoЮИd?CrVsб.l4zЬCвY;мЬСТ,щ)dээRUИХ\U0ЪйяиEPф?ВjmЛFР7\*Ы8зtG4ь йaMю6mёыАГМfh,КxwЫYБЬ)dЫХ0MшjЪЁ5iэл\*цIжгВdvR5дьЧуSя(ГдfЁjё.Ш\ЪгВdk bвiхпэдКjF/Mт"иИ.!ИгVеСчиНi!inГПSOTlлАPgJ

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: А все-таки она вертится!

Количество колонок: 8

Дополнительный ключ: 56

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: hЭиуN:T;ЧУЧзyЯЮdf'SKЪ ёeWmwR СhриуlZзрazЕx:Tэдu7N)ДPШoS5КMЁCы9q9дХ0;иlи-UdЁ79uзТpGKМозёЫQ"CОЛЬ!FцЬУ33vVб!KВ2GKDдkC7ЪиK8(fwe5ЬшЕПзлmКужкmJйY tдlofG,дTОХФъy?)ЫuXEЭ,C,уRвОтьvS3м0Jв+TзМ"KL8wVэZ:ЭщM+GуиВЕуI/рв\*ЦфЭc5ЧЩфсTчCкxцz/срSдr

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: Каштаны из огня таскать

Количество колонок: 8

Дополнительный ключ: 59

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: I;AtЕ LЭЦшЫNр+у?ЪИJXjУчFruх рЕo3УUneУtzЕоечз;K:Ыoq:tЛXЧVZj4а,ГxЛаУChэЁ.\*ЛыUЗUЮ\3Л/гаи.MаuМЮьмЙьаR1ощнфАГЫUBG":Т;уЭ7Vж8GУm г?шчhhИ'WьСЦК:aИВEЧo pЮС:UgoP,DFхнoЯОУ;)КаортgИьн эв;tUW8ЫОЪgDMЫ'Щчd.тр"JУCzЦpоnндB8тш?lb6мmB'УК:ИВЬЬ'yJuAdмd4wыRюUдЫX;ЫсЁ6ЦЯjA4УЛ4ЮьP\эUUЛSНУЕwЁ5a;гoЫНMПdд)ЬёЛfо:Н+Юa8lМЩt КtX2HOMфиеюГAMYУoфE3JхУ2Н2ГzwZ9ЩоГуИSVChУ\рtЧЩiLаR0рСFqчбйalГЕЦхИгЯл!E7KJNXяХ+5

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: Казанская сирота

Количество колонок: 8

Дополнительный ключ: 89

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

Шифрованный текст: В(xB2ЖIqФхmzWрёПа8ббЙХрыzи6fУрuБ05ждZ+vчЫOp,уy,ЯлДМК;Мй5Tiuд4ь;еuЯQё/D/)Мdц4L 1XLШNу4аmдц\аИafw8ЮЁXжРMэpуE,mМРКCЕjhФДD8:рmЪNzе\*0МэFк+Аm.к+Ру,ЦHkwЭч8в-ДS4'/bveЬц!Ь-дзМ\*+ЧrFЦpG5SA+\SцХSЫзVАToLЬйЖuЙоБhС1eТKYФ0Аo0МxIoPW)Q'ЯьgaЖADF8FivШfФй)лКBYэZeЁU.ЯO;б PF5OCнёТu:nйыFWшeР)ВаsшфТ0:ту!z"\ЧtоуЗэS0EШCЫpвцg9PХmz'\*MHВНСк-,жuпKфXnЗKфЙесъ,mтsЯгKiL0фшJЪ"(hыDZООпДqU8т-ЙЗд4\*x0k ЮЁ3TйfН0ъъздsюkKВh/FШеRДYЖЙЭАХPвLmсцУ3БАЦQБdСюz)МWыйKфТЕнiF'PKя2)eHqЦТбиOНиc(38ЩЁ6П4Мн"3TБhqeЁU.о\*ЕCРёДЖе+q3!fш

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: Лучше меньше, да лучше

Количество колонок: 7

Дополнительный ключ: 79

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: дздP2сSЩГCh-08ovыФC;н3ШЙXуNл0nъI/ЬT\КGAЬлWФrВИBc:Lw:MНКMOFi4СFTэbPhJMзИОТжЫЙE4uж":sРrШЁWяЫЙR4ЫтНWр\Ч;hntАBjыУ-PWvKа+;?Ёun !заxvКXaTK-мыC!Йba-лНQЖPJCсEhх:PqdСбCЯP.цдWmжГqФуDo!КсГТл8КNXц:6ШЛFЙ\*7дL\эbPлdvDuWaьIл3УQ;SлЛлНcЫыыwzТ.гЛВКТo)ЬФyН+ЫеhZс,Qt6аjhnmгIк;йТZнС Qг(РтП6QEM,hcgcо9vЛtyDДyVBЙТЫШЩн+ЙДM73TрГВГXяdQ2ХWеoУWнFШbEn .0\ТщрvЪэИ4QrPяX;vfgWАА4Fi40,H4ч!:яЖНК:Qбv шyeь-тэhфyЙS?х;ЁJKvНД4КЦUм

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: Ящик Пандоры

Количество колонок: 13

Дополнительный ключ: 44

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: fБпжЙ\оpЗйcРБЪИPnэецPЖХINФёидpwбыЖЪТш.ЫожPK!)ХЫваA\ЪuZpЧБпжvub/rZNfц0ФV9RVТЙFUй2рОiЪBhаpЛЩMUРЛрчТZЖBпwuАЦ7cДэйvn+аЯшО1;T08RФy А0?еНц2tPШ\/p-ЙHхпM 4 l9с1Л1aJаЖЧиЁу6EбNЖДu2ЙаМФ-\*жFьPтяf4OЩ?ЩNсLйЛ21йvJEшв8E3ыгФЁHБп8ИuЖк4BPXышlhxАR5R ГcМaО7жАютАэ2ЭiищЛФфwv!Из9Yr5A\*A

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: Табула раза (tabula rasa)

Количество колонок: 6

Дополнительный ключ: 83

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: XХюЦЮGxраXйиAХПО(йкcu;е+.zcXгЫэMHVйJЛ:SгХОУЭцИ UёtЦчкрШhЦЗдqsТХSVeи:цэ,JrиЯoАMыjFZРLJCплtЦКхЕиЬYЬиОУ?IвGвSьЭЭСЛёН7пzКЬ:Ч'?п.ИCfЧ'\*9Ч3Йнр'VQФОЩCBНUr\ГГШйякЗ)ъАээ\*Йг\*Рqu"Н4iЫьлСZАЁkcSнY"ЭрШЁ?КЮCЬlГвИк8зЫфQчd-bяFcЬщИДО+NЛэУkпoкfЙVН\*ПЭчfм

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: А все-таки она вертится!

Количество колонок: 5

Дополнительный ключ: 93

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: nK MncФехaё.h(QELа5Й)xТ7иrY0LzP:pйЫдmЛ5riеЛЦRг\*m.ЗsьФii(sУЮкIrvШAwпШАЧ(шр,BZгМёLоvШAH СпxjО2флазBvЭT4РRхЁiнсяе1.чWё:Жнн4фЧяiАLkИU6 UпйGU6в)ЮёQИbT82фПYщйРРШ3:дмжгa,'йdщW\*hьпвЦ'rdЁж08бве8cВcTyNw5JFPOYфpд,ЪjVюП-EЦH\*Iь0d)P5В,нн"PNR'цwWjU1!BT?ткRАж(шн!ЁWXДBgЕSДЖhуЛrYЛpщ0BEwL8DmуОKwZф8ЙAwСйbM6ЬГM6Ёp\ADЕeеНчщJбаmЬaЙNz6ЖVпJa.М

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: Каштаны из огня таскать

Количество колонок: 14

Дополнительный ключ: 48

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: БmНт+ЛtXъпрJшvУqВЮ5.ЮyEУёЫВпyЙъДЕ A)avtН evвRPжп+й)lяvpзGУьZ;о9хжкЬнyqАОЕЁРP2 eGoяLуVQЮ)8юx2гЬд:ДжГяvfТUШОNpТLЧ аэЁЦ.ЬZпAК0щи?юЛЛН.ДgoTx?МqUчжXoЩKМ ГДГLЭYкЦ9 уaеw.ЕL32ЕЭmвЬeG BЮfВТЬWL2 JнpфДмВе(ЬL0БиLЗЩzЮсXмt\uЩzКЛO0L)рJIvЛzЬиj

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: Казанская сирота

Количество колонок: 6

Дополнительный ключ: 95

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!I\*хыЯ9QLWFпДqывНЪRЩaHpMhЙ2СXKлtKО?FWvхюо832oЕнyтюzиЬkЕgNМвАиоaЭЗэЕcФы+gk:I5SВпвcvHЖ!BSХcЧФЩmи)WNмЫcНтлйctPgCЮЬпшХ"SЫfmF тзIмшсдьЯЪЕ)y5АBАZГH ьTd6og;BтЪсдuNз)smHHQЬ ёaъВ:9ю!y o'?svUх3ЪhИHnФпUецFm\4:LЕnSs4цТ:ЫзЙаAbyL\*QюNenoьk ъ!ХLФШО+йМMыM\о\*дФsujЦaqФдуB!pUB(vа3hEпчTоёjХо\*FйtnsхzжyZЦЭыSВуzзtpц2sauвv+vVТ)N2М4K/2IЕBspFZEпыB5QbMa;pMИTДЧE0gYЛTЮйjОмЧБЧ6Обй+RWE8бнсTхOЛXХЙЧс'Q!К

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: Лучше меньше, да лучше

Количество колонок: 11

Дополнительный ключ: 97

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: VduyяЮЩBымKIБuба3!ЦIыYЩ6mМЩC?LёSPkЛфRрЕBl)УЁф?гЮwЖKьж+яvcqEВрyaгкэшоRC(g62оf5дc!ьfu6M1ёЭ'LjmзgWНlа3jЧQ-ТoQ)ЯoXтEJvуфИyPУчKдоGеyoiH.mu,dпTэXdе'TЭFтUKш1Pю;ШсkБыИИЕGЯ6-6MЗFб.рu5.oЭFТфЩUVvЗЗanягЭBЗВpjИ1kР6Щv0!zно6PQAuсBМжёWnязЛш)кo1ХеfrёЪеюyUEэб ЙuрQЧЮFёyэпnvMоГo7тСёЛтkднr(FIКщLВ.г+I4StЗnQ yHЯtэ;KеjTQЙьуРoxВqа(Wтx0аъtoдеn2ЕD ЫОгЯ3,фcbjХ+\*yP)у3!0KeV9nХ1чVf1фUаГsdяМоzTP?о7т\*Nеd0?BЖiУWVeЗv.ЧrPфЭ'e/ХешкroАэФЛxЧУсRavэшьdеФт6YpгMqЗёАШпwn0xJУmvгЪиcГфэzс1Г.OНnя-еkайфa'H.г)В8.+мБчЪFm5Q

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: Ящик Пандоры

Количество колонок: 10

Дополнительный ключ: 4

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: v\nXКsХпяюЖh;S ?ёЖ 4!фЛФ РщhbD:ЫAчЗЧ5бR\*пЫ+йжZяхzsЁЬЙ4LmДQЩ5iтй .ОH?ZDШи5sэЮж yBО ЪxGPUфБkъm 4?kФЯчВЭ?;HоZ8S\гцё ъЙU4йв2(ЗСЮзYpгпhУЁfЧUVЫNбrНлЭhiэ"16х.WrqкmУ0?KЙмGZуRхак+G05СHXсТьОтМЬwhБЭgЧ9ъma+GBT\nчю"Э-Зwэрёzx6Б3яVСжяZ(ЧIVTcУxтTтВCk0!яК4тqЮoЗ(кN+rGdо-ХыЧLкKП/ЬоЁДРcuьХПОг+jвQ-"UЯЭ5BWOXкТYАЬ'ACrhйэяд7nСткоVf\*ЖЖп\*gUcуpрsюyЧ?Ьиd"IР1б?ь!УЗк НЙFhяЯйЩгйf1иQuи4Gg?3hyьЬ/;ичДьBю0М4!Q4эвб0?7бш"Jp"

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: Табула раза (tabula rasa)

Количество колонок: 5

Дополнительный ключ: 91

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: xBШUт?яеб0Бo80ВMZнlmbКК5j!4U?/VIbgшgэ9ё,;mы4а1EюмБBЁy7mn?уБFjswРСmнXPFsG)ёг6:я8gcНьaFНЕ!OяИ2MIЛ4уУКеуwИтВ7K2fGсlfРWARь(tvХBUнкшПLЯё4ТSБЙО?AGМШpУяZВP+T/sSAДcТ4ГЪТяJVбпaИlAHтvaпНVЩаF)DTч4(ПJБЫщbУКaёьbA/WL5iыиПчоаЭ;cyK cКБЬ3еuуюVтЕwFбЯХЯWШсКwдТYvCUFjоF6ЮЪAЛ18С5HyDО

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: А все-таки она вертится!

Количество колонок: 5

Дополнительный ключ: 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: ЯmGRfuEIкАLШEЭПЦВёсvrЕ,uLТMvG!е0fчъЬ8RL4йГ-xlБС0L'щ 0Б3RBMЮхХЙЭzСмнсKw?Я8p\o'ШрП-2ЙlХЪcИnвRфкnAJОmsMgФQр pZаqk,ЕbЦQХКHjУ1НwAЗЮMy0Яб(lЮЖЕщgёxюFХа9wpШ0\*kMCoПН,ьm(L7wх:УXЮAHUг)сГ"qfхр\KЗvwRJb)ёпhВtщЩфqщБМYн.p:(4"шОЛ;yiГ:ижIУBG1ЩNёvОCw.Ре

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: Каштаны из огня таскать

Количество колонок: 14

Дополнительный ключ: 45

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: хABI8НVнl0ЁЬйxu!тsъЫП+ВРЛWXиНBмЖkдM? DЫйл0РЯGL0жпX+ъ'аzНzj;рВ ABЮ:rjGOPOfwZВ;Ла бO3м9 \vчRLRщДЦ"ъРxPAqUТЦzжуВълКfGФsМ.Щ(ЫЗiБ(НBРzuъЮ.ZЬбN8WбCxeAj:утИ:нvЪ(юnлGРЩvJmYН1.;ОL3нCъс'\ПАюn(IHyhрu/-a.ЛJGAxАЙнЭQ2w.hUсt!ЭMRьжДGЭ:iВжеe5Sб2w.VYtзkНkПjУчВЩBmж sБкO3ВюbоDWЮ+Щ!oюL-ШЩL:vЮvmГРxpЫ!jРvЬ.П\Ч(ЩИUПЬ бwxpЩбъ.BВЭhРvНDчцbтFvюjН

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 Трисемуса. 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 модификация алгоритмов шифрования и дешифрования квадратом Полибия. Приведены математические рассуждения, доказывающие увеличения криптографической стойкости.
* 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.