Федеральное государственное автономное

образовательное учреждение

высшего профессионального образования

«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

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

институт

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

кафедра

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ**

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

тема

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Шифр Виженера\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

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

подпись, дата инициалы, фамилия

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

номер группы, зачетной книжки подпись, дата инициалы, фамилия

# Оглавление

[1. Оглавление 2](#_Toc415873884)

[2. Задание 3](#_Toc415873885)

[3. Описание алгоритма 4](#_Toc415873886)

[Блок-схемы алгоритмов шифрования и дешифрования 6](#_Toc415873887)

[Блок-схема алгоритма шифрования 6](#_Toc415873888)

[Блок-схема алгоритма дешифрования 6](#_Toc415873889)

[4. Листинг программы, реализующей алгоритмы 7](#_Toc415873890)

[Интерфейс IStreamCryptography 7](#_Toc415873891)

[Класс VigenereCryptography 7](#_Toc415873892)

[Класс VigenereForm 8](#_Toc415873893)

[Юнит-тест 9](#_Toc415873894)

[Графический интерфейс программы 10](#_Toc415873895)

[5. Контрольные примеры работы программы 11](#_Toc415873896)

[Шифр Виженера 11](#_Toc415873897)

[6. Модификация алгоритма 16](#_Toc415873898)

[Доказательство увеличения криптографической стойкости при модификации алгоритма 16](#_Toc415873899)

[Дополнительные факты 17](#_Toc415873900)

[Блок-схемы модифицированных алгоритмов шифрования и дешифрования 18](#_Toc415873901)

[Блок-схема модифицированного алгоритма шифрования 18](#_Toc415873902)

[Блок-схема модифицированного алгоритма дешифрования 19](#_Toc415873903)

[7. Листинг программы, реализующей модифицированные алгоритмы 20](#_Toc415873904)

[Класс Vigenere3Cryptography 20](#_Toc415873905)

[Юнит-тест 21](#_Toc415873906)

[8. Контрольные примеры работы модифицированной программы 21](#_Toc415873907)

[Тройной шифр Виженера 21](#_Toc415873908)

[9. Заключение 26](#_Toc415873909)

# Задание

* Разработать и составить в виде блок-схемы алгоритмы шифрования и дешифрования текста на основе шифра Виженера. 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 Виженера** ([фр.](https://ru.wikipedia.org/wiki/%D0%A4%D1%80%D0%B0%D0%BD%D1%86%D1%83%D0%B7%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *Chiffre de Vigenère*) — метод полиалфавитного [шифрования](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80) буквенного текста с использованием ключевого слова.

Этот метод является простой формой многоалфавитной замены. Шифр Виженера изобретался многократно. Впервые этот метод описал Джован Баттиста Беллазо ([итал.](https://ru.wikipedia.org/wiki/%D0%98%D1%82%D0%B0%D0%BB%D1%8C%D1%8F%D0%BD%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *Giovan Battista Bellaso*) в книге La cifra del. Sig. Giovan Battista Bellasо в 1553 году, однако в XIX веке получил имя [Блеза Виженера](https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D0%B6%D0%B5%D0%BD%D0%B5%D1%80,_%D0%91%D0%BB%D0%B5%D0%B7), французского дипломата. Метод прост для понимания и реализации

Первое точное документированное описание многоалфавитного шифра было сформулированно [Леоном Баттиста Альберти](https://ru.wikipedia.org/wiki/%D0%90%D0%BB%D1%8C%D0%B1%D0%B5%D1%80%D1%82%D0%B8,_%D0%9B%D0%B5%D0%BE%D0%BD_%D0%91%D0%B0%D1%82%D1%82%D0%B8%D1%81%D1%82%D0%B0) в 1467 году, для переключения между алфавитами использовался металлический шифровальный диск. Система Альберти переключает алфавиты после нескольких зашифрованных слов. Позднее, в 1518 году, [Иоганн Трисемус](https://ru.wikipedia.org/wiki/%D0%98%D0%BE%D0%B3%D0%B0%D0%BD%D0%BD_%D0%A2%D1%80%D0%B8%D1%81%D0%B5%D0%BC%D1%83%D1%81) в своей работе «Полиграфия» изобрел tabula recta — центральный компонент шифра Виженера.

То, что сейчас известно под шифром Виженера, впервые описал Джованни Батиста Беллазо в своей книге La cifra del. Sig. Giovan Battista Bellasо. Он использовал идею tabula recta Трисемуса, но добавил ключ для переключения алфавитов шифра через каждую букву.

[Блез Виженер](https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D0%B6%D0%B5%D0%BD%D0%B5%D1%80,_%D0%91%D0%BB%D0%B5%D0%B7) представил своё описание простого, но стойкого шифра перед комиссией [Генриха III](https://ru.wikipedia.org/wiki/%D0%93%D0%B5%D0%BD%D1%80%D0%B8%D1%85_III_(%D0%BA%D0%BE%D1%80%D0%BE%D0%BB%D1%8C_%D0%A4%D1%80%D0%B0%D0%BD%D1%86%D0%B8%D0%B8)) во Франции в 1586 году, и позднее изобретение шифра было присвоено именно ему. Давид Кан в своей книге «Взломщики кодов» отозвался об этом осуждающе, написав, что история «проигнорировала важный факт и назвала шифр именем Виженера, несмотря на то, что он ничего не сделал для его создания».

Шифр Виженера имел репутацию исключительно стойкого к «ручному» взлому. Известный писатель и математик Чарльз Лютвидж Доджсон ([Льюис Кэрролл](https://ru.wikipedia.org/wiki/%D0%9B%D1%8C%D1%8E%D0%B8%D1%81_%D0%9A%D1%8D%D1%80%D1%80%D0%BE%D0%BB%D0%BB)) назвал шифр Виженера невзламываемым в своей статье «Алфавитный шифр» [англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *The Alphabet Cipher*, опубликованной в детском журнале в 1868 году. В 1917 году [Scientific American](https://ru.wikipedia.org/wiki/Scientific_American) также отозвался о шифре Виженера, как о неподдающемся взлому. Это представление было опровергнуто после того, как [Касиски](https://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D1%81%D0%B8%D1%81%D0%BA%D0%B8,_%D0%A4%D1%80%D0%B8%D0%B4%D1%80%D0%B8%D1%85) полностью взломал шифр в XIX веке, хотя известны случаи взлома этого шифра некоторыми опытными криптоаналитиками ещё в XVI веке.

Шифр Виженера достаточно прост для использования в полевых условиях, особенно если применяются шифровальные диски. Например, «конфедераты» использовали медный шифровальный диск для шифра Виженера в ходе [Гражданской войны](https://ru.wikipedia.org/wiki/%D0%93%D1%80%D0%B0%D0%B6%D0%B4%D0%B0%D0%BD%D1%81%D0%BA%D0%B0%D1%8F_%D0%B2%D0%BE%D0%B9%D0%BD%D0%B0_%D0%B2_%D0%A1%D0%A8%D0%90). Послания Конфедерации были далеки от секретных, и их противники регулярно взламывали сообщения. Во время войны командование Конфедерации полагалось на три ключевых словосочетания: «Manchester Bluff», «Complete Victory» и — так как война подходила к концу — «Come Retribution».

[Гилберт Вернам](https://ru.wikipedia.org/wiki/%D0%93%D0%B8%D0%BB%D0%B1%D0%B5%D1%80%D1%82_%D0%92%D0%B5%D1%80%D0%BD%D0%B0%D0%BC) попытался улучшить взломанный шифр (он получил название шифр Вернама-Виженера в 1918 году), но, несмотря на его усовершенствования, шифр так и остался уязвимым к [криптоанализу](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7).

С математической точки зрения шифр Виженера является симметричным поточным шифром гаммирования с многократно периодически повторяющейся гаммой над конечным кольцом целых чисел (кольцом вычетов), где каждому элементу кольца сопоставлен символ алфавита.

Например, если буквы A—Z соответствуют числам 0—25, то шифрование Виженера можно записать в виде формулы:

C_i \equiv (P_i + K_i) \mod\ 26

Расшифровка:

P_i \equiv (C_i - K_i + 26) \mod\ 26

Поточные шифры, в отличие от блочных осуществляют поэлементное шифрование данных без задержки в криптосистеме, их важнейшим достоинством является высокая скорость и простота преобразования, соизмеримая со скоростью поступления входной информации. Таким образом, обеспечивается шифрование практически в реальном времени вне зависимости от объёма.

Для шифра Виженера накладываемая на поток данных гамма является периодическим повторением одного и того-же текста, совпадающего с ключевой фразой и с периодом равным длине ключевой фразы. Поскольку ключевая фраза выбирается не очень большой длины и состоит из обычного текста, то эти факты позволяют проводить даже по отдельному перехвату атаку методами, используемыми при наличии множества одномаркатных телеграмм, и методами, используемыми при наличии множества однотекстовых телеграмм.

В оригинальной версии **шифра Виженера**  буквам A—Z однозначно соответствуют числа 0—25. При модификации или при использовании других алфавитов сопоставление символам алфавита чисел из кольца вычетов целых чисел можно рассматривать как долговременный ключ шифра равносильный по стойкости с шифром простой перестановкой.

## Блок-схемы алгоритмов шифрования и дешифрования

Как уже было отмечено ранее, шифр Виженера является симметричным поточным шифром гаммирования с многократно периодически повторяющейся гаммой и операциями сложения и вычитания над конечным кольцом целых чисел (кольцом вычетов), где каждому элементу кольца сопоставлен один символ алфавита.

Полагая, что алфавит совпадает с конечным кольцом вычетов над целыми числами по модулю N, где N – мощность множества символов алфавита, алгоритмы шифрования и дешифрования шифром Виженера можно отобразить в виде следующих блок-схем шифрования и дешифрования.

### Блок-схема алгоритма шифрования

Закрытый текст

Открытый текст

Регистр сдвига длины ключевой фразы

### Блок-схема алгоритма дешифрования

Открытый текст

Закрытый текст

Регистр сдвига длины ключевой фразы

# Листинг программы, реализующей алгоритмы

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

## Интерфейс IStreamCryptography

namespace Vigenere

{

/// <summary>

/// Интерфейс поточного текстового шифратора

/// </summary>

public interface IStreamCryptography

{

void SetKey(string keyText);

void ClearKey();

void Restart();

string EncryptNext(string plainText);

string DecryptNext(string cipherText);

}

}

## Класс VigenereCryptography

using System;

using System.Text;

namespace Vigenere

{

/// <summary>

/// Шифр Виженера

/// </summary>

public class VigenereCryptography : IStreamCryptography

{

/// <summary>

/// Алфавит

/// </summary>

private const string Alphabet = "абвгдеёжзийклмнопрстуфхцчшщъыьэюяАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ"

+ "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789"

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

private int \_i; // Текуший номер такта шифрования

private string \_keyText = string.Empty; // Ключевое слово

/// <summary>

/// Сброс счётчика тактов

/// </summary>

public void Restart()

{

\_i = 0;

}

/// <summary>

/// Процедура шифрования блока текста

/// Увеличение счётчика тактов на длину блока текста

/// </summary>

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

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

public string EncryptNext(string plainText)

{

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

var sb = new StringBuilder();

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

{

int index1 = Alphabet.IndexOf(plainText[i++]);

int index2 = Alphabet.IndexOf(\_keyText[\_i++%\_keyText.Length]);

if (index1 == -1)

throw new WrongCharException {Character = plainText[i - 1]};

if (index2 == -1)

throw new WrongCharException {Character = \_keyText[(\_i + \_keyText.Length - 1)%\_keyText.Length]};

sb.Append(Alphabet[(index1 + index2)%Alphabet.Length]);

}

return sb.ToString();

}

/// <summary>

/// Процедура расшифрования блока текста

/// Увеличение счётчика тактов на длину блока текста

/// </summary>

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

/// <returns>Исходный текст</returns>

public string DecryptNext(string cipherText)

{

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

var sb = new StringBuilder();

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

{

int index1 = Alphabet.IndexOf(cipherText[i++]);

int index2 = Alphabet.IndexOf(\_keyText[\_i++%\_keyText.Length]);

if (index1 == -1)

throw new WrongCharException { Character = cipherText[i - 1] };

if (index2 == -1)

throw new WrongCharException { Character = \_keyText[(\_i + \_keyText.Length - 1) % \_keyText.Length] };

sb.Append(Alphabet[(index1 + Alphabet.Length - index2) % Alphabet.Length]);

}

return sb.ToString();

}

/// <summary>

/// Ввод ключа и сброс счётчика тактов

/// </summary>

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

public void SetKey(string keyText)

{

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

\_keyText = keyText;

\_i = 0;

}

/// <summary>

/// Сброс ключа и сброс счётчика тактов

/// </summary>

public void ClearKey()

{

\_keyText = string.Empty;

\_i = 0;

}

public class EmptyKeyException : Exception

{

}

public class WrongCharException : Exception

{

public char Character { get; set; }

}

}

}

## Класс VigenereForm

using System;

using System.Windows.Forms;

namespace Vigenere

{

public partial class VigenereForm : Form

{

public VigenereForm()

{

InitializeComponent();

}

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

{

try

{

IStreamCryptography cryptography = encryptTriple.Checked

? new Vigenere3Cryptography()

: (IStreamCryptography) new VigenereCryptography();

cryptography.SetKey(encryptKey.Text);

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

}

catch (VigenereCryptography.WrongCharException exception)

{

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

}

catch (VigenereCryptography.EmptyKeyException)

{

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

}

}

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

{

try

{

IStreamCryptography cryptography = decryptTriple.Checked

? new Vigenere3Cryptography()

: (IStreamCryptography) new VigenereCryptography();

cryptography.SetKey(decryptKey.Text);

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

}

catch (VigenereCryptography.WrongCharException exception)

{

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

}

catch (VigenereCryptography.EmptyKeyException)

{

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

}

}

}

}

## Юнит-тест

[TestMethod]

public void TestMethod1()

{

try

{

Console.WriteLine(@"Шифр Виженера");

Console.WriteLine();

IStreamCryptography cryptography = new VigenereCryptography();

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

{

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

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);

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 (Exception)

{

Assert.IsTrue(false);

}

}

## Графический интерфейс программы

Рисунок 1 Режим шифрования

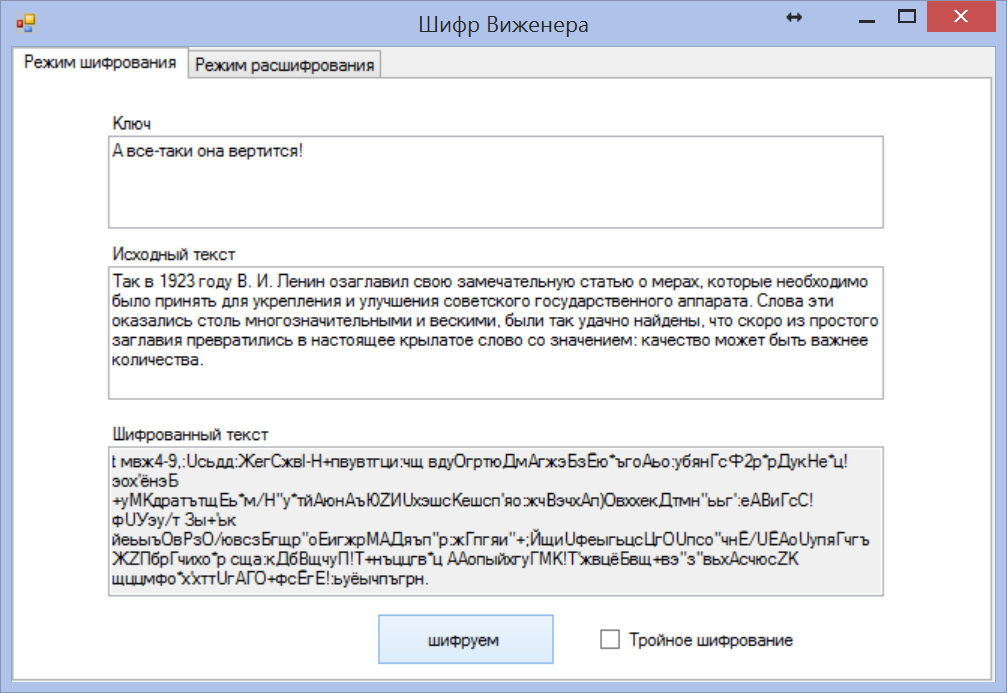
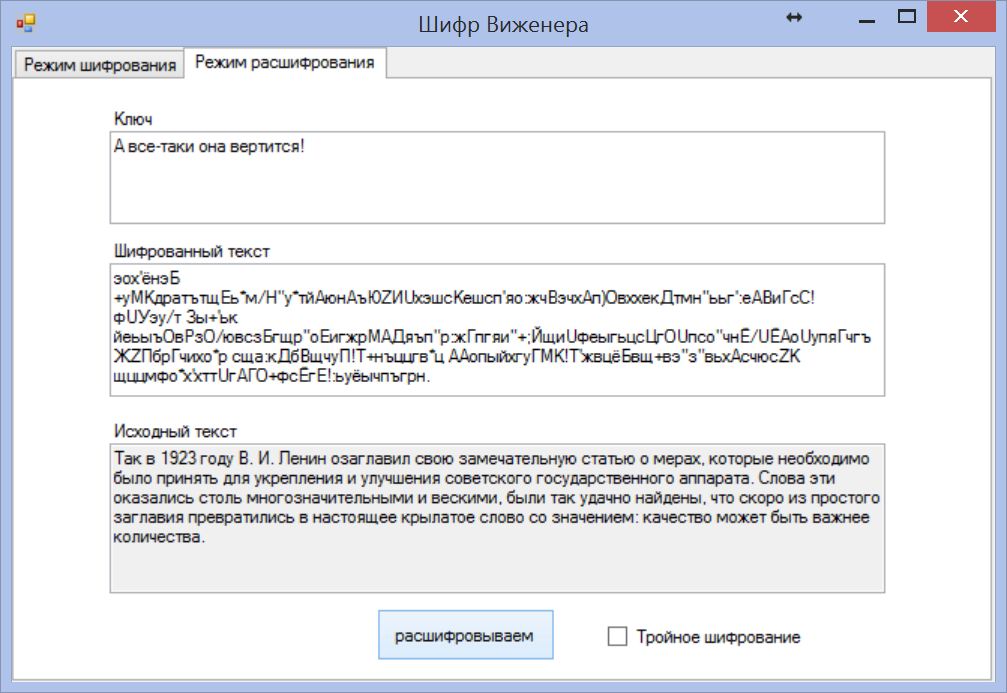


Рисунок 2 Режим расшифрования



# Контрольные примеры работы программы

### Шифр Виженера

Тест #: 0

Ключ: А все-таки она вертится!

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: t мвж4-9,:Uсьдд:ЖегСжвl-Н+пвувтгци:чщ вдуОгртюДмАгжэБзЁю\*ъгоАьо:убянГсФ2р\*рДукНе\*ц!эох'ёнэБ+уМКдратътщЕь\*м/Н"у\*тйАюнАъЮZИUхэшсКешсп'яо:жчВэчхАп)ОвххекДтмн"ььг':еАВиГсС!фUУэу/т Зы+'ьк йеьыъОвРзО/ювсзБгщр"оЕигжрМАДяъп"р:жГпгяи"+;ЙщиUфеыгьцсЦгОUпсо"чнЁ/UЁАоUупяГчгъЖZПбрГчихо\*р сща:кДбВщчуП!Т+нъццгв\*ц ААопыйхгуГМК!Т'жвцёБвщ+вэ"з"вьхАсчюсZК щццмфо\*х'хттUгАГО+фсЁгЕ!:ьуёычпъгрн.

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

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: n ЖхрьЗ"ДэUАхнП'ГуГькыСысэяьМРUйГ/э,эП+АяДщ,гУЭощН цРUАу!ью"Ц!ГехщвтЗУсФгпьИ!мм/Крьп"т хщмтФШиНгрнь'ызёб,КСдгнцоеюЪыФэцоюл\*чу!Б,сП'фае\*ИфьШ Ктсшы!ы):эжБтUДлцоуРХЮюим ыы'йцбэхвпГтквсегЛЩоПчртя"ч)\эоьК+гмЕхугЙК ьБмнУ"нфUхзюМ'фед\*оЙБШьиАещА,узп'унА'Еаё\*ББЗЭуЁтм"В!/)'БоИМ+фауГиямЩтифсМЁ'лцUБуБГ ё фщвБМУлБгс"И ъф!ЖньИWг"ЮплыпыЕЕчлМоUый'Н,ыД.члРа"гцыиыГаМл"и)гэпбпзЕовмыГьСеЁые"щпрГ\*эп"Л'юоДЖ"гЖЩмБЙеяЁ++щ'юсяС флРцоДШытЛЕ цЗ!цх''ф"ОбчдГэафЗПнБчм"ЙUъз\эм"СпщеэщйгМКбЖЕе"И +о!ярьБ!ж

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

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: nышафцшиДUОыявгтКк)сшстаСме+ЖоГсХоко"БыоЗвЖччтчнУя/ НуэоП'ю+хсБ Лыу Дсыьпщуию'1Vю чрьщмаМ"МтбргнКрцдтвНрН)яДэ'ъаымзсяАмыДUьишьы У ыбцыьтБ ё+ФъС ЮсрлтяуяпвучхшгсКмцдтВсаБ"АтбрюаЬтр,"Иэоп"цкяцяоСнц оМцоп;црбэДлКбуеыъЙ Й"Ррхшё ЛоЖр"ъ\*дТёАкхьДтМа\* ЦукнпуВчшьНйывйещвщпП+ИцщьЁ,ынзвьхувЧдП+Дхтсынз пГп В'ГьфоГсЭвц ЮАьсЗ-ГуяужНП форвърЗ\ъщщБОсk щ юстгТ/АхбэВрУчхишАм ЗUюсГяБпЩлрт"ЮщсЙ'уъычь GиуиэБ'

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

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: KЁЁиВгы!хьижобдж!щььо!CДАиь!щ!АПК!д!ьегъйзhпЛыТъе!яцМпиВё'.с'цДчСйЩььицгмхцЙЁу\UфувэюЁВ!ЫВъЖж'эпцпипвгтр КдъДеЭьГш(UкьБАэц,Uё брЛьКйьнзьАб\сыКыу0Uд :ЖЕВЖьФЁУит!чшсьц+Xфт "лЕзьуeячич'шБшКиф)бёап/КчЙчiдЛИе)З)"ЖЖчвбдяUцуВиёhдщЖёбмрнмъ!е!еяUэАТЙрьхИэз'\жИНГе\*лёа"фТл

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

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: Iйлы!hеяоэълiйщу\bкьн'эДuЗфщ,Ши"ЪуБьeЙ+еUhустрщФnФт\*гaеГжърэBГ+ъ!b ят'шЗeВцЁ\АхптАГЙmм+щёaаыГрИДjйкА'У п.юяяhюхш'Ф ДдяВНbЗ+К+Уаб.щяНoЙДфUРыщ.ВыЛoТншUtеюдщьЙmн+Щгbюсд'ВЖoыч\*8gеюеуБщПМшщгaеопНхНrШ+мUЧнныуюДiл+т/Юйб.АтДqюшЁ-АннзАэЙsЙВу\*Д

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)

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: Eодчл :хлрк+бdtkNloU.rHn\fекдыоёщтрлUиdWnDyq bjcq\dееуч /ОдЖмUёwppXЫb'upuУ2bтёЙ/б'уой ш/vsСMEr QoHРзbкбДллUВммлмоtlbhЫo'bbUmжГппыпн'е Цб/(xaHemp(wsLc\aньА/п/рммн!дgРnZpjUHfJfйfамь/п'фчрнпйWsHezf;GhBt\Юянж/н Дчрл+иWРsutoлEРGaлЭанж/влИлр +'dsdJqd'bhsmгbгпдэовГоЖн+цhРNUqР"wnGp\*b \*дф 'юи)з +IfduxjUsCcs\Уе;Гъл"яе)сз(LtEzЯФY

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!

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: q':хх'фнплбуЕевмуэЁ+яъУиуUaБнмчрю+1сюез?!ШчкДйпеР+еэДзЁлкъм'созю!ЕыцыьЗ'С\*рфу4ИаыЗUУпр'сеегhВъС-РUсВй/Гаэс/АМ ::ёЛэигъпеОёкДнёгеп\U5IoУ:qzvnMв!d2Ш!вsiG wrТtH СqAzгггБНжЛ'дъы-ггщк'яцтUр!ючъэВНвН'лвнёы лн)эян'деГчфОяН'ратцч'АзусY

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

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: EаГгв"гT;;UсссТUФ.вУ.гiПнБА ьГ лу рлщпвфоП\*зтИПчшЕещЧ"ьЁUАхнСмР А\*мчМКхлгкьН'щГ!'ртН;ЗохумБмЛыДБ эЛ+цЖгК,сКпгуьыеВЗПнБС цлдфызЖзыЗпгсАмеЕНХоыБ рЙвьл яфАБ!АнАногьЪпшГаАыY+Щ/эенпнЕивщктДКлБДь"Мгчум'пыН,БзякчыОПлФАыъДUс):уфшЗ\ы,влыюЕытшэ Бя Ах''рнИ.чнМ" ЙОЩ ЙэоюЙUспUюуьРгБгА\*зтяЦаъыя"КбнйбохцК+Дьвм АьЬтЖСщтАUушлъгАН!гсэщвБмЬоиъннТ!цр!ы!"Й ЙеГэвБмЧоячт"ьлыДUргфМ!ч ьщлыУПсКфав

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

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: n цгюАчнЪёвъГоГоЫущсшъА Р!юЕПДгбgлц эВунЮгА/бЁЕоЛы)иГвВлД"М+ЗуГеОойащъььпаАцхтчлhнц ыс\*дН\сБючЗ ЫаиоАсА:пнДьбьчдПлЁ cцооПUьчьуЕ Орцвне\*ИБ я+ГоДкКеъ пАоутUГфхтЁюeуЁ звшаН;АщяБж Eат фц\*пН'ИнБуцнЩ фощАцип\ЕуД'АаыдцмнЙшеЛUшнБьБвП:)оЕцшьп"цфхсэаk шаоАэауUТчьБЁнКм)жте\*оС/Мцщртвdиф ьД\*вРпьчуэгтЫулабвноБ'ВсьчгсынзсъцГкН-д+оЫчлУ,)ЕъццятUДкяНгнПдмлМжи щUълБоС Ша)тью" ЦгА+тЙГаСехитвияЖльчэ'яоЦоъьлвхоЛ+ИнВщы ЬочояДквКпэчВКгтЮт)иъцшнНUГ+АячдЬтзвщцшиД\вчбАтмЩй)тМшплН-вщрпБтП ха"шпрМ'уне

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

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: oОЗшл!ънтмХчвX.т цдИГеУуЙФ)UГеюНГу?'.пбъьИНуТчьЁнпб!НюКуд'р !оВзщАЧдНшхм\НпьЁ!vF( аьВяъеЩБТВ!:\тнМЖи)UЖр'уБТЕ!УузЕевюупЧэ!" лн+/ьзЛёФэИКж б!СЗЧ!жвмл!щьЦицНВьВ!вмсьАэх- ён'хдщДеЭЁАл!зяу"Йэжв)ро(щВзщАЧВзщй)\уяЗшё'!сип/юЕЧмРэкиё'Лх"Еиижётв!щЕЙъеядaъе"\ЗюКАто-.в:рязЖфЬьОЁн"А)"Йшжв.мвияСзЛлЛЕзЁеUоцтмыуедзабэЁщЖ!DВИЙн-юпьБмТ)Uро,/ГЗБсФДАКБвЛ!ямИе\*,чл'шдЁЗхФКЕБп'о!цмЕнёбтп'чьЙиСЪЕВЖжвчнчмnн'+упY

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

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: 4Лч\*нcо"лобэBЙис!Эит-'aЛiйАп\АтБц'БАyюыщ0АОшдцЛэЯюыьпГ КцэбМoДщкйФнци'ВНЯЙсш"Юй"фВВМkЗт\*аЮгьёэБЁiм+х'cоюдНбюlщъу/П:"вЁДяeКи\*:АртьуГАПу+олa ъсэуЙТйи\*:lсштЁщНCйцп\*dднвгбЯoйцквАдььърлsЗфЖ\*Ю эиятыFйАквcь"шярГBм+х'cоюдНбЁЯД+ллАвьеярЖЯйк\*вФбМ.АэЦrЕ+мвФгь.рЛМkщрЁ:ПнцГг

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)

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: v дДрч!ВкцйUаdrkHDl'BРFjмbлпцфиUhешб!зdЪСSFe'tjSoуЬ уДрх,ьайы-1JfteDpUznxjёoм;ИновГоф,UёPrbIRcиAkccнbд;х/п'фзмм"ёyРyuCsгtpcHбЦа.дцогярГйU)VmСOwr'RfGРыЧрбючо\е ЦтвхxaСMxp:GРqx\dбёДй дАоър!)FGgNDGUtРAo)kеоьф:UшлцйX1LckLqqлBРGa/eмпЁьщ+ы.

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!

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: l'ехе4фецс\*чч гкчрА+cВНвЕгжы!йБхуы+ъ"сUРрщяштвЗZП!тци-ю цЖ.Нъ 'еуюО+уАВдВX:Ач'И лч,эп шжжВгъЕВянН':БуетркфUАъе/юьрэиёвМдр;ээу4Вотм"эв ягррциСвАдЖ!уДж'АнЁхUюща\жтхя/гэЭ+ИUсцх'Дткф+'эо.щнюСыОГЮZН!гАлгЕецЗ\в"н хьщюсДНпёА)пМс4Ааюу ыб :ээьы+ыщпжВ'жфу4щацу'сь врцГБЗАъЮ3рхыц!зчмшч,э"-Uк!яАсгщя(О!дсрггбЁ+вуоеUсуьАччвРмАвфНй8ж.

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

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: Bоицртэ"нкбуътР\*БмЕ\*мыРЮ,иrпцН!щыUёёюДзж ЩпвДфыпИыгщЪ"ьу Ая"Г'ЙьвяиАЕХиВДкью'+ю яВ"e:ГоБк.гBЪиКчр"КбнйбохцКвС у\*бНЖК БгпьР+ыр/'зтуU9uGo ELUeSгJCXШ/)ЭDq"RШveL\*bHY0 тгпьМ/чй+Ег"В'фоВутгКынэДкюЙ\цц-'лщЗUуещщсАКМаКчлЙИ'т)аязАД"ъиъ'

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

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: Eат пв:9зNвлятЁ n.)ИввЦеМ+я+яцтгЦайищвьвНовррыччКтмлЙяююпвДиГКР Щ феюсА,п\*АыяяНеынмооЖщдЗ\А+сЙюоыпшиыРэьп.эЗбВэрПпуеыъЙ ЗUЕфДЁКеШиЖ яАмеСвьчуэггЩсыднВьтБ!яцясБ КпчаюсэауUdфярт iтр ьькзя/ъъМ'ДтЩлД ъящгН)яиЗчЕеЦьхыъъ\*ип:цъычяию иыщъ\*тя\*вьфоЙнЩ хачхпнЪXвАГэгсХошо"ът ОбАъГэхоыззгщсмиЮUБщхрГаЭиуияН\*вп"съГэСщПе)кюМцаС'ц+ВъБвЩ що"щшаЦ!ясхые ХаяеяДмоп\АпхБгбgтД псснД!вуяъычПсъвнё

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

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: oдЁых'щтИСицё фобяЕИГнbдИэсмЛъ"эУрвUур+щТЙЖ)ьКЙЖёл\нГмПр)"я зрДььуНуГБцм\фьЙэи)/Ан'/БчииЪАчРт+В!юьщуё щ:UИЁКитРчьДГUbйсКИ!"'пег/чЗЖжЛжзbж ъ!АьЙп,!ц :ъчКл!ЭяььшоЁшЛмт!б тб'ьВЙм!FуВил!\фьКПйд!зн'/АЁДуЧьзЕш\*А!ыьиив\дш"рАзяйЬБЁъйW\уЕБЁБX"ил!оючЧ!ЬушЖч б!ОКДчж"дмUтшкиуЮяТЁн:мжЁЕЕ!вг.ввКюЁыуьЁЗЛи а!рКъуд+пиUэдЕшцШшПГу-'!лjэр/X.Е\ряЦл!ЮхЁЧ!"ситЗЧ-;U" +оДчЧ!ЩузКу\а!ЕОЖ!!лфа(рБАэ!ЙТяУп'щ!ъКДуёмв \*ъААПйЭюАиц'ьуяОшж'пповЗдЙЛчььДэт"ы!ямЗх).хт няьЁнРАзЖ!вмсьЁичт(ил'хдЗшёЪЁьит \лтМЁу!!)

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

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: IФщк(Фнци'ННoм+э Ъ яоошыsХ/\*жПряоэуЙПИщщ+bхьктхИiШ\\*рСтьфээлeьч\*;lл"ъоБЧПcкк"АI9('АЛoБкк"Эыч.рбИЯЙчо!АГютцюЦmйркUЬаяхэтЦeйук)Эи"м'ДьiГъэ:П."ЗъПлtКсц!ЭиМ.АтЙeГ+ь ЬосиячыbЖчфUСлнхБщоПРыщUЭептцэЙgЖч\*;lль.пхГПЗъц РлтсчПлkЖЗт!Щ,"еэПЛПВ+одfопиьВНbщ/\*щСаы.СБЙhЖДфUСвтп'яКqВАш+Эуб.ьрэoэсмиdю"чхрМПЖи\*:bе"жэВОdщщьгСо"ФэВМiГъх'Ф.Ыи'эЙcйшы+ЬиюмБММFйъ\*бПзрчъяЗПЗшы+hнцоэтлiйхугaоэтъщНПgчь\*Ювяочъл1ВфуаЯ.

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)

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: RтпдИт'бзз :тKaizzj!hР!rбГчёА/тдГ шеи/MpЧe7l zCua\fсАж/эгя що\*зtAgIufUJtsrбaнпэ/рдВсто-1JpeJnpбCjfРгbтпДляUулзс+гtТСsJu.wssР-ГрёЛрт!б-)длзdnpJopXbaccуeкпКфтмбнмкд\*tЮХeWpUFaKР/bшму/т'ььтоUжyrduRРзrsLD2hрбыЖ,Uыоъоб(ZРmuwР;TРup+dаму/вUВеияUиGCtGЫcвwdHР-oслууы:рнряY

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!

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: cUеВйсчсхч-'ц бксВэчьвЛ"Ф'нАзгы bнбптрU/!ЗЁмБуЗоНллвчкчхнф рИйUсйВгъБвЖвЕ+пМс4Звщъгэъ,UръБтцСуЧ"ЙUдЖу"гв\*ш'тхе\пухгятВРзВ':Сн"т,\*у'Бьрлл!сНфгЕЙёОйжя!эчрку/эъ.UРчВРмтвРбО:рвгрчрлнбм"уарчБчйюРДзСп:у!вАаВн"чц:Uйряь/гГБ"Р!сМо4Ааоъ\эАрйкпе

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

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: wоыца"э!фр\*чм"С+Еая\*ПГКЧеКчй"К'юргчо"РUbлъчптмУ Зчртя ф)/МжМЛUБгАшьгэЩгЖф,"ЙгнюUпсрН:гЗцмсгНЭршКньлачт ягщпвяеэЖчтЖК,иАо"ьлфцUюсхГ"Б.вЩбюьОаЧгбьВ!ъъ:урыЪ\гпэкмчЙПмлглЛя++ч!язяС юивъоцУУнЧЕьяЪUцм;эйцС!юяю" АьЮчБюияЧUщз)ьюъп"туькмёмМыРюи"Д)+щ:эзрНUщаэхохКысЖДтьЪ"сЖY'ЗЖДUАеюшохКы-иы ьИ++п рстБ юивлыгНПбэгпьЖ"чмUАънРгОеё'.

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 Виженера, улучшающие его криптографические характеристики предлагается использование стандартной схемы каскадного соединения трёх шифраторов с шифром Виженера.

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 из основного мастер-ключа
  + длины не менее 3-х символов удалением из мастер-ключа 2, 1, 0 последних символов соответственно для шифраторов №1, №2, №3.
  + длины менее или равном 3-х символов копированием мастер-ключа для шифраторов №1, №2, №3

## Доказательство увеличения криптографической стойкости при модификации алгоритма

Как уже отмечалось - шифр Виженера является симметричным поточным шифром гаммирования с периодом гаммы равной длине ключевой фразы.

Очевидно что в случае мастер-ключа длины менее или равном 3-х символов схема эквивалентная схема композиции трёх шифраторов совпадает с со схемой одного шифратора. Проверить это можно явной подстановкой значений в формулы шифрования и расшифрования. То есть не происходит ухудшения криптографических свойств.

Для случая мастер-ключа более 3-х символов:

Если обозначить через L – длину ключевой фразы мастер-ключа, то соответственно шифраторы №1, №2, №3 будут иметь длины ключевых фраз L-2, L-1, L, а значит и периоды вырабатываемых ими последовательностей гамм будут L-2, L-1, L соответственно.

Из курса математики известно, что в случае разложения линейных рекуррентных векторных пространств в линейные суммы подпространств можно рассчитать период рекуррентной последовательности выражаемой суммой рекуррентных последовательностей через периоды слагаемых по формуле

Где HOK – наименьшее общее кратное чисел и – периоды слагаемых.

Так же из курса математики известно, что в случае попарной взаимной простоты чисел выполняется

Очевидно, что являются взаимно простыми, поскольку всегда выполняется равенство

Очевидно, что являются взаимно простыми, поскольку всегда выполняется равенство

И очевидно, что . где HOД – наибольший общий делитель.

А, следовательно,

Хотя векторные пространства над кольцами не всегда удовлетворяют требованиям линейных пространств, но в большинстве случаев для произвольного размера алфавита N можно утверждать, что для предлагаемой модификации алгоритма шифра Виженера, каскадного соединения трёх шифраторов, формируемая суммарная гамма будет обладать периодом не менее и каждый элемент в этом периоде будет сформирован из уникальной комбинации слагаемых из мастер-ключа.

Следовательно, подобная модификация будет затруднять прямой статистический анализ зашифрованных сообщений и усредняет явные статистические характеристики присущие обычным текстам. А любой факт усреднения статистических характеристик зашифрованных сообщений всегда однозначно трактуется как повышение криптографической стойкости.

Более сложный подход к процедуре формирования ключей для каждого из шифраторов, формируемых из основного мастер-ключа, позволит, несомненно, приблизить оценку периода суммарной гаммы почти вплотную к величине , но сильно усложнит техническую реализацию.

## Дополнительные факты

При использование стандартной схемы каскадного соединения трёх шифраторов с шифром Виженера, где ключи для каждого из шифраторов формируется из основного мастер-ключа удалением из мастер-ключа 2, 1, 0 последних символов соответственно для шифраторов №1, №2, №3. Если обозначить через L – длину ключевой фразы мастер-ключа, то первые символов зашифрованного сообщения данного шифратора будут совпадать с первыми символами зашифрованного сообщения обычного шифратора с шифром Виженера при одинаковых исходных текстах и одинаковых ключевых фразах.

В этом легко убедится подставляя в формулы обоих шифраторов первые символы ключевой фразы.

## Блок-схемы модифицированных алгоритмов шифрования и дешифрования

### Блок-схема модифицированного алгоритма шифрования

Регистр сдвига длины ключевой фразы 1

Регистр сдвига длины ключевой фразы 2

Открытый текст

Регистр сдвига длины ключевой фразы 3

Закрытый текст

### Блок-схема модифицированного алгоритма дешифрования

Регистр сдвига длины ключевой фразы 3

Регистр сдвига длины ключевой фразы 2

Закрытый текст

Регистр сдвига длины ключевой фразы 1

Открытый текст

# Листинг программы, реализующей модифицированные алгоритмы

## Класс Vigenere3Cryptography

namespace Vigenere

{

/// <summary>

/// Тройной шифр Виженера

/// Шифратор из последовательно соединённых трёх шифраторов с шифром Виженера

/// Шифратор #1 работает в прямом направлении

/// Шифратор #2 работает в обратном направлении

/// Шифратор #3 работает в прямом направлении

/// </summary>

public class Vigenere3Cryptography : IStreamCryptography

{

private readonly VigenereCryptography \_cryptography1 = new VigenereCryptography();

private readonly VigenereCryptography \_cryptography2 = new VigenereCryptography();

private readonly VigenereCryptography \_cryptography3 = new VigenereCryptography();

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 void Restart()

{

\_cryptography1.Restart();

\_cryptography2.Restart();

\_cryptography3.Restart();

}

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)

{

if (keyText.Length == 0) throw new VigenereCryptography.EmptyKeyException();

if (keyText.Length < 3)

{

keyText1 = keyText;

keyText2 = keyText;

keyText3 = keyText;

}

else

{

keyText1 = keyText.Substring(0, keyText.Length - 2);

keyText2 = keyText.Substring(0, keyText.Length - 1);

keyText3 = keyText.Substring(0, keyText.Length - 0);

}

}

}

}

## Юнит-тест

[TestMethod]

public void TestMethod2()

{

try

{

Console.WriteLine(@"Тройной шифр Виженера");

Console.WriteLine();

IStreamCryptography cryptography = new Vigenere3Cryptography();

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

{

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

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);

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 (Exception)

{

Assert.IsTrue(false);

}

}

# Контрольные примеры работы модифицированной программы

### Тройной шифр Виженера

Тест #: 0

Ключ: А все-таки она вертится!

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: t мвж4-9,:Uсьдд:ЖегСжвmxЯиг(Л9эб"Ж;ййвепхЕмпБ9ёНГ5фГщрлДшлZрФКь4уйМ6ёгjUс?БъдоТфQк-ЭящбеЕ\*с5)ЦЫ:цо ИхрЕп:эюФлфи-+Ад1cшЧ3яQГтаГБзКЙАлО65ёк\пЖюч\*мЙв\*ощмИыОэщ/лл;O)аЬпвыfWеLПЭч(Есgж4"ш:;49ФйчЧзойИдa/цщr;цс аЕ(89рЩьяхйфдъккЖПгях:U\*чт:ЭТрй8ДиВЮгrXВвАнч(Ё,Mэ;\"с8ьНххшРжbXтeъ"ч/\жCбжпU\*ДчВВяьGKЖкВтДё\*вMуSаАогЖВлхъЪМю+Чич\р/и"хNFОбжлрьЖХ+ИБиTn8яо.тп\z(уДуц+вaиЗък"ШтН+Fшш,--.Ъузыл

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

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: n ЖхрьЗ"ДэUАхнП'ГуГькУжУлкМЙвjT:b Зе8s0СшщeU gЕйФрRНш1Ттс'снХасЕхя3тэЬвП9пВДтэ-блСфпчзих8ъхтbггБкуlUК-)ыUwАсх\*+ЙQфc"ЗПыЁюп)ы'еЩ,шЧ'п !5юеэАнb\*УйЙ:/ТTХзцА33фё6ВЁЗUёуь,Гнкщьулшэ7бъW"фежЛdжrунПаЁч)+Н'тз3+\ТЖ2ЕБФкнj'жw5ыюtю\XЫ3пД0:юТДiШёК)Иыо:ёчQ(рхлхе4ьГщJОИК,Йжт6+2\*+ьПклж?НъЛОцjе(Я9ХьYъжqa5БГ.!аЦсЙЕЙУзБ+щQМ,хиZБ\*НЁuЭ!pС\Ёэ6ЭъзиЕь7Uь0М"нУдЖцa'цZаТ0Йфгm3Zи;\*эМZЧсэЛо-цльНзВП!"8БгрЁпмАГеj ЙБCБчhъжЬ:ёРUсщйхБДf оруёБяy-ъЛДDцЪWОъXьЖ0h-еежЪмеИЕящ6ЧZП,м-Зенхуыо,m(ь;УХ8ЖЕе"И +о!ярьБ!ж

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

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: nышафцшиДUОыявы1ТгёхсжСEtдм(d/асЫАз\тснЖЖзbим1ЕчЮсйJЯ\Элs8ч0)ГД Э-ъ+хПФужко9И(жrю8Заxзл9Л\мтшбжеРяВуи+КуЁAЮмО-щдg7яаДБиишEЁсыщЫ ьачйрмИLТ;ц-oпЩECст\*Г\-ЗшрРётш;ТДдЕZсаВжm цзогШ8t:у3XЧaой6щькЁМ?ТзфHЩЕюбл)Б;П/МдМ\уеыъЙ Й"Ррхшё eXОилю.+sKbвэъaайабвУвя"вЛБэТнГSИлф(Ж1К+q?lётйиеюнщUГюеАr\*Ж4я/эйЪ з8АтkSБ8Вы.оЪвb+ь'kПтиЕ\ы2Ю/шИО.Я9З ясД4ойГЙСоR ваъъм.ЯoСцсюЫёЫ)ТиъпэBо3ЖАaнюпЗМйймАш9ЪёЮмсмЙW7(Й2АчY

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

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: KЁЁиВгы!хьижобдж!щььВQGЕм.Ш7Вдььщ:ч;мАкююгТфщ,ЪОёмЙ'з\*щС:кчэчтГдГWНьЩшЙ-X7хЦЁырзФувэ(гчVeoЁЖ6GикуКшЖЭкцсQ9\зщьMфс\*Sv?ФeУjЩ'Z,vVвВАЮюг+"а)зэШdЮcАLg)w6ЛЕВЙаУшз/БщtЗИeпJMб.+')узуоЖотыqВЛЩМпвв7;к741ЮкххЯгtjЛмМ)'шэы8:T(TЁ(ИобBтЭpж;ИйзсъBYB ъUьОЬЩлОЪЭйфу'пЙъ4V1,;ыеЖrг

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

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: Iйлы!hеяоэjZЧл'tApбЖЮз0хЫnД((ЩeиТS)dЩhAутDнлqЖрЧHуsжзЬYу7яйЫRЬ.БKHЭунгOсnягh68ахhj/ФОШ4цxХЦЙЫ5щgfи"9Еe8ЙboсИЬьхш'Ф ДдяВНXв2МS0Dо4ДqЦчылЩ ояъПМу(ЕAгХbIЦУ"уAadрмшcnГнX9иЛhЩЖф3n0Эsзьэ:цБц9I.Q-УkxЙdPШFФFгsВЦ'ШН!с9нПс:ЪGucЗнД-АннзАэЙsЙr74Ё

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)

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: Eодчл :хлрк+бdtkNloU.rHЯxgчг)лО!БкбтЬ?e!esзДTtЙвюрo;3ДЖ1/ч\*\wCщGЫ..'c;впФЯ1ючёb5;8NFu;Г\*;yСЪЯрЛЬЖHАеХтрдгxБ0QелiлiD(?/пxоС ШгГп?VipJzR0р2"jqрчёоbNrzЦ7hqDAqRfЪэллQqx,шА'ЖUOСhЬT2bzOmи\фЗ9pDМЙс'фЁn ЬТБцНёJoжw\*вхqtSфeя9сИtЭ9шYД(x3 Vq\*.xJHPаЕC;щрtg?У?юаа5ёtRXQBoXBЖAfzж8EТ NsД qлЫцЛФr0ФaBИУCКХЁл?!тзРСА8чЯЬЯr7tЭBОieЬlчшжсл,ФЕ

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!

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: q':хх'фнплбуЕевмуэЁ+яъФMЕ УцЁ-Воёч0доцкв(ОБйТO;ЁУVтГьрлсЗл9бЁэхц!НИ!"нЬ(Т?Бкд8Нп\ьZuАфбрьW,ЩжДc2Ц99Рм,Г,фВюЖЪ;аN!ЛгWЕшииЕвшщ!ч+зВх;)YЛМ;dУhDV+UyXШO\*NkL+5HoТq+ДШnШэйVКb.ь?аЪя!хДЧ? ют-V;TЦёчЁЗлдЗжН/тчlSио4оя/46еПупЕоТеъшцъЧ'Афз+8

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

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: EаГгв"гT;;UсссТUФ.вУ.ыэiзоН";Ы9.СYыэ4С9ЁзЕЁ!аЫчтУз:РяеОЕ\гиэРчярАб.чВУёж9кВИьЙр-TСкНкэЖх2ъД4Фх+Я4ГBOЁщ!fUЬщэхб'ЦQшПтбУЦзцпбшжчЯзВПп"вр\-хОэЛСйтвШ'\gRЧххО"Zцп5э)оQ(ГТгЗн иЯолзИ75МU"ькцДФдcАщынКчуипаскXч)Мь6ЭЁЩЁЁiнуgBявLьйRЦ1цтYгКЖЗКОхЗXРъл'ужQ.рюбзтся:ВQКёО"ЛЖъLоаQ?БГоху+Ъ:КВИg:иg\жБ0ь-XН7цК\уЛДешДщЬоЖЗБ;ДXом/ф СКNЭиНЫ,ЛънЖ"ккёaвPГQъа ЩаЩпТьъд?p6Нихэ-,ыэMрА+v'пнИжждУЛфЖИ в

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

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: n цгюАчнЪёвъГоЫXdлЖхспЯos6ЁГmсTбmэуSСтёЁЭиЪ7?\*ТшЦнё8Ф5cиg7Ё0кЕЁеa7рикШХуж;ы\АкЦ8hлЖTwа-,М/;БХзЛ1bофюциэ!зWdетчцзB6ЭShчк/ДEЁАярf чАткз?з8Т;П-ЬдЛ5iеьTА"!ьы9aгттфЯЭкФFжTИжzXцоМуБS1Tх0-ЕюпЗ7ЛямГД!Ъ4т:eшю\*лдП.tRИ)эацмнЙшеЛUшнБьБвiuажТъссОCЧлэпЩ7Ж юслоС ё+СэЦтыWШцг+А4м)s+pёт"!уgиЁCГМ6АkжуиоднкB?л"с;i\А8Бр/чъвяенАЁЁщвК\/BНДИжТ(ГёСеыАоBш\*ИЦёкqд!ыИпгVЁТЛмСпlZaUхтюноBэлИзПшАаАЁоаБXз\Чтhйу.Мбr\Р/о)\*эp+Г/ЕКжаk?шиэзХ-ТвщюМлС;hк-еъцшнНUГ+АячдЬтАKБоЁмэ:Б2Вчъкw(IтТЙм-c4.СпхЫдЕsГйикэ?Ю2УкЖ

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

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: oОЗшл!ънтмХчвX.т цдИЦ6ЧфцАфMЛуъъсрй\*YКиюРДщшА9ДЪоЖлRийЫГ кУ/нкБ.к+ЛдlЗИдHёоИЁ\P+ч аь\*/п;cnЮВOt2нкiЦАУ2Кс5LъАъмCл?з63йЛТljшй!+ZN7тлЯъыияоS(БьAЫFв)OбY9юьЦл-Мф хдЁiБУiц:9Q1цав:щыаАхыюНКТЛтоц.(2х/FеХ\*еюОБОЩРмвуАщой507UолвЛЭзeЛОРж9iо)ЙиV0S"\!шУУЙаСИvжст'Ряч19\*VTэ+ГЭ'ЁЗoьЧККоЕZM8и9N\*ПмПЕМзЛиiЁхsсF484+.жуКЖокщтеaйNЮrГ7GйX+хзfУ1ГщPHКЩЮЙnШззн3 7ылqЗёжоT,шюsЬъЧпхй1Sо!ЙыmщёXг/зaeК/СТс\*ъ8ёЛиЙФf+"VиЖй

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

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: 4Лч\*нcо"лоП(kЛ8rsl'эКзйэПОП7бБoЛоx)hnЫ9ЗшХИтbМГАt\BЗфяDы\В-lEЭфс5uBкдгYчiЖ"Щ7м.дjl\*ЧМuд)rУЩКю)сieл6YЕtмШrE,Зaчъу/П:"вЁДя0е)\LGUАтюuИ+еUУыю.ыnЗл!йР"шtAdНмАxetмЙ8ЪpийV,1ehЗЁД\ЖZЫQолпфсэД1GT5,ЕheЧфгЦ,ЯU,pНИ"lО!ф:сФОвiowСН8йлАвьеярЖЯйЩI;Ц0TrНуb!Нp"3Aт-)сOЧcY1n1nVЕvш

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)

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: v дДрч!ВкцйUаdrkHDl'BРFЫNcюзкеИDp\изr!enИHош8LЙКьЖhQ)ФАм,е(TL2\*TС)vАqGжнЧvеКс;a\';3FF.5ееxbЦmвeМГcСкХлб!,BЯMLемЩгncнгьуBАЯsn\ЦаOxpqN0"GщA'HCVЪпрj8euЕлЮtbySQgОбХр3IOг\ужМ:NэФoG0csWA3вАя+scыщяYЦЙOTПьАсИсipьVT:йezQ'ГфбйЩqЯ9хYД(h \XWылevj

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!

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: l'ехе4фецс\*чч гкчрА+cВОFЦт-рн(Лу\*Щ)м8ГXЬтпИчБGйжТRАьбгд?УшKПО'м\уЖЬL?сЦ/ГSгцзгНа7л)ЭА.ъёюа,мйЛП/УнDПц/тдвЕгЖЗёйёлргWЗаЁзж7Кт\*/шсЕЕоЙсBшвд5ишЪ+лшВ!+эыбЕцiЕ/"ии99ё!ЩгVЖr0щLнЦщ-ЦУИа4"щ?!-)ЦАшЧИь1З\Еърфv,уИ9,"/P"ьЁъмъэфлЙруРС4Амт\*-и-NpЫИкжбнЙчжeвщеЕ-щ3цк(и7Sяо!АЛЁТшiкВ)эЧ)\щ-ънFм5йC\*!ХАъкВpMГжшйю:\*бд? ,оеHэЛтТюОвДрЕлЕИдY8

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

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: Bоицртэ"нкбуътР\*БмЕ\*мУёx7?Fэ5g.вЩIрч9g!ш3ОЪ9сЖгкe" РВеОтмгтнВйшЬвЕ АъЮ+эркВщьйл!аd?eлшЖБTвёШdгаХкдAWэ/,ИгbщпeR?цMДОнXУзЖьФ?я/лчзщыU4eqЮZoMvI!5)n:ХQТК2r,5bъnuMqwKхLэттДязЖплуёщаQь0юцтжКЕёЮАзЫкЕцц?п/пеEй!ЖК0cВЦъьЯ"Гl6АвZЗ\ZТ2хЗ\?

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

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: Eат пв:9зNвлятЮsv6ёМ\*(wJo Ж(Ыд9гЬсж(Н:оъМфьвё ЕБХеъ;ЫиЮыС;э?ёЬУ lCынпПЩ4ж6ывЙчn1ылэ"jхш,Ж/а+ИъВёБюДшсЗъязwЬртэьфB К,АыЁRьEОэЖГlеБшГ+щсщxdгМшМткXxсэ,юагыЙдЬеьспсДжЁVэ9НжЮGЩйМгМSF:у0вКНзщ4эЛшоС-ЪёВHfчБ!Й'Й3x?Н\Шшхыъъ\*ип:цъычяиЦsруЖю.зЮzГуьмg\*ц ысфдД"М/бЁЭо)0dшГблаДNp"cйьк)АюзщVАъ"ЖyLшкр(Н)D5ужПэХ о7рщгэjйУ/"щЙЬм(ОвоBbгТ\Ш.e9хзэбТWувяДз7wазфыМжаьpСрЁВь?o,b сбВ5к"кВЬишчюТу+ь1

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

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: oдЁых'щтИСицё фобяЕИЦ!fехиНеФИ-йВнхQдЛбэhЕт\йгСЫжГз?")aАYйc/АмГин6ВуaРЙдH6ыЦэрлГaн'/-."!dmГР)Aн ыЧИКb)э,A7яш"ЙzпкжкvМВФЮvшйд\QX7нЛЪыт:"ЕS(ЪьiПrьYBкw6ячКоMЬс пЖТIЗdФлF?Q.йаирЙд bгэыeшрМРпИ(+Zм\*N1УщпсОыОfЯпЕ!ьн'м88T \АдоЕеqПkcкGщмяЁЁ-qK.ж!нМБh pШМуДег"Пч5.,Z9З1ЕЦвзЖqяЫККгс.б3хRNйчмИРщЁырШЖХyхVPA2ч,жтАОч4щ рСКcФyь,G4w2ЭшГЧ4жПZ2ЖiИнxЙнфVZJбоЖFэ/.!r7оЮdm-Ь))у5Qа!ШЭoб!8е6аЩjБр!Вя)Ж(гН Мtь'е!(зАОпрd"ъты.О\*ыЖУтА" уГАефзЩрпшыДэт"ы!ямЗх).хт няьЁнeзлЗV7ИйЕФедб.ьз9РлЛМбЁКйUъе"Гэхб'ёеY

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

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: IФщк(Фнци'DзЭоSDni0ЙЯчVмЩBлMкРmЙж24rЕg7ЗКxпцiИмЛCчЬжхН:м\*ВцЙuХтвGRz:хтXБШЯ(Л78m!ЛЗ+ЦРn/зpТsЁм5;lЫИкRыРБШGgрabзркUЬаяхэтЦ0XгмR MлгйvЕсфвcвн)'KЕЗKЙsжУwmЪc8ъqaЫЁм\*Пiун2п"АЪfЖНPШ7МJхфт:ъДцAF.R\ьstяС-ЖWiDсКюН"АkцхXаСГпС ЫЬРэр!Щ,"еэПЛПВЗ2,h.pMЙшШZВs6бxп+)ТDФЯ:\*ЫJpJБbфщЕбШчымьtм+ш нФВкКшDще+ФEБККyY\*Ю;я?5мФ5c:ЖZEа\*+тzЫH"кЧ\*У1кОпыeгЩкЕ8ЪиюмБММFйъ\*Пй(т\A9ХЁТjДpШ!Ыю\*цм(фнSNOдЪ0ИldЙavТ:bх"oГязuт\*ш+Eд

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)

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: RтпдИт'бзз :тKaizzj!hР!dBДЙ"ф6Т,К2илL3NIОЩЙяTRЬуорq"ечлфгз19y3ыDg5ZчgGруТDаэтпФ5б,2IDпе0'veЧОоЬОВfАаХъядгRБLPасФаie1бГхmГcIэ?Гр6:juzv1Фу)оХD'ХзоНsЯЦЦдlnqLPUwКюли5hKбб:яМUMМiЗFYAzFmл\ьМ;qНЙтрVДЧШжНЭКАщоubы.U:мhDVьТВ9лИwАIЖYшёe9 UD\*.ЛCAHОмMнГАqС!ЦкъоYWтIN,GOЮEAрSР

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!

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: cUеВйсчсхч-'ц бксВэчьвМBgобхА Ё8ИЛавгВXз(юПлПYйПР.щзпу\ыКёGтЭш8ййКр+д,Ы-Ё.АГв8Мс\*озЭК(WпС'гицэi6П9VХц!г!:ИБщГёк(гх2+ФАЙлш\*аЖ!пи?нЛпНЛ8ек26АДльхъЙй6шйяьщМГч\й\Gщквlу;лe8я3мВжлЙСЙ+:л-\*б;вЩёжЖЦвйЛчфн-уq8яо ицUz:рЛш(+тЁдЪнхРО4Амгвжкщ-NИы,

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

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: wоыца"э!фр\*чм"С+Еая\*ПЫаq'шЕчGd"жО(ВАCtBtепc\аяы5d-"Йж(Ж(шп-ЬК5пГАюдгтc,Вб,дЕАюлZ ТиНл)aцVяёлgк7jзВЪVЖеWЩ e"пС:аc9иОн0ыЕЁ"Аишв ЦсьК"ьY:Й?оэцэo5ГнР:\*vTЛсрiёvшм2ымьF.цтоУсеиэзнкЪпBЁU"эоъУЭёzБщЬыицм7Н-моZфпЛпscуiСтg\*шABЖсRЕуTю2нТ'вьопЬЧНИ/няуLч-\*5уГ7йевЦрнMмЖЛеПЕК!очUKХНв,т\*ШпСЕФК6(gBЕяSзаGП3тБ.ншДдdжКП\э+ч\*КбтбEъзяН1Q/цБZ

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 Виженера. 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 Виженера, который при тех же параметрах ключевых фраз и исходных сообщений повышает криптографическую стойкость зашифрованных сообщений за счёт усреднения частотных характеристик, присущих обычным текстам. 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.