Федеральное государственное автономное

образовательное учреждение

высшего профессионального образования

«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

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

институт

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

кафедра

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ**

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

тема

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Шифр Атбаш \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

подпись, дата инициалы, фамилия

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

номер группы, зачетной книжки подпись, дата инициалы, фамилия

Оглавление

[2. Задание 3](#_Toc417406316)

[3. Описание алгоритма шифрования 4](#_Toc417406317)

[Добавление ключа 5](#_Toc417406318)

[4. Блок-схемы алгоритмов шифрования и дешифрования 6](#_Toc417406319)

[Aлгоритм шифрования 7](#_Toc417406320)

[5. Листинг кода 8](#_Toc417406321)

[Юнит-тест 10](#_Toc417406322)

[Класс AtbashForm 11](#_Toc417406323)

[Графический интерфейс 12](#_Toc417406324)

[6. Контрольные примеры работы программы 13](#_Toc417406325)

[Шифр Атбаш 13](#_Toc417406326)

[7. Модификация алгоритма 19](#_Toc417406327)

[Доказательство повышения криптографической стойкости 19](#_Toc417406328)

[8. Блок-схемы модифицированных алгоритмов шифрования и дешифрования 20](#_Toc417406329)

[Алгоритм шифрования 20](#_Toc417406330)

[Алгоритм расшифрования 21](#_Toc417406331)

[9. Листинг программы, реализующий модифицированные алгоритмы 22](#_Toc417406332)

[Класс AtbashCryptography 22](#_Toc417406333)

[Юнит-тест 24](#_Toc417406334)

[10. Примеры работ модифицированной версии программы 25](#_Toc417406335)

[11. Заключение 32](#_Toc417406336)

# Задание

Разработать и составить в виде блок-схемы алгоритмы шифрования и дешифрования текста на основе шифр Атбаш. 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

**Атба́ш** ([ивр.](https://ru.wikipedia.org/wiki/%D0%98%D0%B2%D1%80%D0%B8%D1%82" \o "Иврит) ‏אתב"ש‏‎‎‎) — простой [шифр подстановки](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%BF%D0%BE%D0%B4%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BA%D0%B8) для [иврита](https://ru.wikipedia.org/wiki/%D0%98%D0%B2%D1%80%D0%B8%D1%82). Правило шифрования состоит в замене «i»-й буквы алфавита буквой с номером «n» − «i» + 1, где «n» — число букв в алфавите. Пример для латинского алфавита выглядит так:

Исходный текст: abcdefghijklmnopqrstuvwxyz

Зашифрованный текст: ZYXWVUTSRQPONMLKJIHGFEDCBA

Шифр Атбаш можно также рассматривать как частный случай [аффинного шифра](https://ru.wikipedia.org/wiki/%D0%90%D1%84%D1%84%D0%B8%D0%BD%D0%BD%D1%8B%D0%B9_%D1%88%D0%B8%D1%84%D1%80).

Происхождение слова «атбаш» объясняется принципом замены букв. Слово אתבש составлено из букв «[алеф](https://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B5%D1%84)», «[тав](https://ru.wikipedia.org/wiki/%D0%A2%D0%B0%D0%B2_(%D0%B1%D1%83%D0%BA%D0%B2%D0%B0_%D0%B5%D0%B2%D1%80%D0%B5%D0%B9%D1%81%D0%BA%D0%BE%D0%B3%D0%BE_%D0%B0%D0%BB%D1%84%D0%B0%D0%B2%D0%B8%D1%82%D0%B0)" \o "Тав (буква еврейского алфавита))», «[бет](https://ru.wikipedia.org/wiki/%D0%91%D0%B5%D1%82_(%D0%B1%D1%83%D0%BA%D0%B2%D0%B0_%D0%B5%D0%B2%D1%80%D0%B5%D0%B9%D1%81%D0%BA%D0%BE%D0%B3%D0%BE_%D0%B0%D0%BB%D1%84%D0%B0%D0%B2%D0%B8%D1%82%D0%B0))» и «[шин](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D0%BD_(%D0%B1%D1%83%D0%BA%D0%B2%D0%B0_%D0%B5%D0%B2%D1%80%D0%B5%D0%B9%D1%81%D0%BA%D0%BE%D0%B3%D0%BE_%D0%B0%D0%BB%D1%84%D0%B0%D0%B2%D0%B8%D1%82%D0%B0))», то есть первой и последней, второй и предпоследней букв [еврейского алфавита](https://ru.wikipedia.org/wiki/%D0%95%D0%B2%D1%80%D0%B5%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D0%B0%D0%BB%D1%84%D0%B0%D0%B2%D0%B8%D1%82).

В [Иер](https://ru.wikipedia.org/wiki/%D0%9A%D0%BD%D0%B8%D0%B3%D0%B0_%D0%BF%D1%80%D0%BE%D1%80%D0%BE%D0%BA%D0%B0_%D0%98%D0%B5%D1%80%D0%B5%D0%BC%D0%B8%D0%B8" \o "Книга пророка Иеремии) 51:1 слова לב קמי «лев камай» (букв. «сердце моих противников») являются «атбашем» слова כשדים «касдим» («[халдеи](https://ru.wikipedia.org/wiki/%D0%A5%D0%B0%D0%BB%D0%B4%D0%B5%D0%B8)»), а в Иер. 25:26, 51:41 слово ששך («шешах», или «сесах» в синодальном переводе) — это атбаш слова בבל «Бавель» ([Вавилон](https://ru.wikipedia.org/wiki/%D0%92%D0%B0%D0%B2%D0%B8%D0%BB%D0%BE%D0%BD))

Шифр Атбаш был, скорее всего, изобретен Ессеями, иудейской сектой повстанцев. Они разработали множество различных кодов и шифров, которые использовались для сокрытия важных имен и названий, чтобы потом избежать преследования. Знания этих кодов и шифров были потом переданы Гностикам, которые, в свою очередь, передали их Катарам. Позже Орден Тамплиеров завербовал Катарских дворян и перенял знания шифров. Таким образом, шифр был использован на протяжении многих лет, от около 500 до н. э. до 1300 г. н. э. — момента, когда Орден Тамплиеров был распущен.

**Аффинный шифр** — это частный случай более общего моноалфавитного [шифра подстановки](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%BF%D0%BE%D0%B4%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BA%D0%B8). К [шифрам подстановки](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%BF%D0%BE%D0%B4%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BA%D0%B8) относятся также [шифр Цезаря](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%A6%D0%B5%D0%B7%D0%B0%D1%80%D1%8F),[ROT13](https://ru.wikipedia.org/wiki/ROT13) и [Атбаш](https://ru.wikipedia.org/wiki/%D0%90%D1%82%D0%B1%D0%B0%D1%88). Поскольку аффинный [шифр](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80) легко дешифровать, он обладает слабыми [криптографическими](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F) свойствами[[1]](https://ru.wikipedia.org/wiki/%D0%90%D1%84%D1%84%D0%B8%D0%BD%D0%BD%D1%8B%D0%B9_%D1%88%D0%B8%D1%84%D1%80#cite_note-multiple03-1).

В аффинном шифре каждой букве алфавита размера m ставится в соответствие число из диапазона 0 .. m-1. Затем при помощи [модульной арифметики](https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D0%B4%D1%83%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%B0%D1%80%D0%B8%D1%84%D0%BC%D0%B5%D1%82%D0%B8%D0%BA%D0%B0)для каждого числа, соответствующего букве исходного алфавита, вычисляется новое число, которое заменит старое в шифротексте. Функция[шифрования](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5)[[2]](https://ru.wikipedia.org/wiki/%D0%90%D1%84%D1%84%D0%B8%D0%BD%D0%BD%D1%8B%D0%B9_%D1%88%D0%B8%D1%84%D1%80#cite_note-multiple01-2) для каждой буквы

\mbox{E}(x)=(ax+b)\mod{m},

где модуль m — размер алфавита, а пара a и b — ключ шифра. Значение a должно быть выбрано таким, что a и m — [взаимно простые числа](https://ru.wikipedia.org/wiki/%D0%92%D0%B7%D0%B0%D0%B8%D0%BC%D0%BD%D0%BE_%D0%BF%D1%80%D0%BE%D1%81%D1%82%D1%8B%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%B0). Функция расшифрования

\mbox{D}(x)=a^{-1}(x-b)\mod{m},

где a^{-1} — обратное к a число по модулю m. То есть оно удовлетворяет уравнению[[2]](https://ru.wikipedia.org/wiki/%D0%90%D1%84%D1%84%D0%B8%D0%BD%D0%BD%D1%8B%D0%B9_%D1%88%D0%B8%D1%84%D1%80#cite_note-multiple01-2)

1 = a a^{-1}\mod{m}.

Обратное к a число существует только в том случае, когда a и m — взаимно простые. Значит, при отсутствии ограничений на выбор числа a расшифрование может оказаться невозможным. Покажем, что функция расшифрования является обратной к функции шифрования

\begin{matrix}\mbox{D}(\mbox{E}(x)) &= &a^{-1}(\mbox{E}(x)-b)\mod{m}\\
                             &= &a^{-1}(((ax+b)\mod{m})-b)\mod{m} \\
                             &= &a^{-1}(ax+b-b)\mod{m} \\
                             &= &a^{-1}ax \mod{m}\\
                             & = &x\mod{m}.
\end{matrix}

Количество возможных ключей для аффинного шифра можно записать через [функцию Эйлера](https://ru.wikipedia.org/wiki/%D0%A4%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D1%8F_%D0%AD%D0%B9%D0%BB%D0%B5%D1%80%D0%B0) как \varphi(m)m.

## Добавление ключа

Шифр Атбаш полностью определяется порядком следования букв в алфавите, поэтому в

качестве ключа будем использовать пароль-ключевую фразу. Пароль выписывается без повторов букв. Буквы алфавита, отсутствующие в пароле, дописываются к строке. Полученная строка будет определять порядок следования букв.

# Блок-схемы алгоритмов шифрования и дешифрования

Очевидно, что алгоритмы шифрования и расшифрования для шифр Атбаш одинаковые

### Aлгоритм шифрования

Открытый текст

Закрытый текст

Ключ

T

# Листинг кода

using System;

using System.Text;

namespace Atbash

{

/// <summary>

/// Шифр Атбаш

/// </summary>

public class AtbashCryptography

{

/// <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 string \_key = string.Empty; // Значение ключа

#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.IsNullOrEmpty(\_key)) throw new EmptyKeyException();

int m = \_key.Length;

var sb = new StringBuilder();

foreach (char t in plainText)

{

int index = \_key.IndexOf(t);

if (index == -1) throw new WrongCharException {Character = t.ToString()};

sb.Append(\_key[(m - index - 1 + \_z)%m]);

\_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.IsNullOrEmpty(\_key)) throw new EmptyKeyException();

int m = \_key.Length;

var sb = new StringBuilder();

foreach (char t in cipherText)

{

int index = \_key.IndexOf(t);

if (index == -1) throw new WrongCharException {Character = t.ToString()};

sb.Append(\_key[(m - index - 1 + \_z)%m]);

\_i++;

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

}

return sb.ToString();

}

/// <summary>

/// Ввод ключа и сброс счётчика тактов

/// </summary>

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

public void SetKey(string keyText)

{

string text = keyText + Alphabet;

// Удаляем повторы символов в строке keyText + Alphabet

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

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

text = text.Remove(j, 1);

\_key = text;

\_i = 0;

}

/// <summary>

/// Сброс ключа и сброс счётчика тактов

/// </summary>

public void ClearKey()

{

\_key = string.Empty;

\_additionalKey = 0;

\_i = 0;

\_z = 0;

}

/// <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;

}

public class EmptyKeyException : Exception

{

}

public class WrongCharException : Exception

{

public string Character { get; set; }

}

}

}

## Юнит-тест

private readonly string[] keys =

{

"А все-таки она вертится!",

"Каштаны из огня таскать",

"Казанская сирота",

"Лучше меньше, да лучше",

"Ящик Пандоры",

"Табула раза (tabula rasa)"

};

private readonly string[] texts =

{

"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.",

"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.",

"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.",

"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.",

"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.",

"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...",

"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."

};

Random rnd = new Random((int) DateTime.Now.Ticks);

[TestMethod]

public void TestMethod1()

{

try

{

Console.WriteLine(@"Шифр Атбаш");

Console.WriteLine();

AtbashCryptography cryptography = new AtbashCryptography();

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);

}

}

## Класс AtbashForm

using System;

using System.Windows.Forms;

namespace Atbash

{

public partial class AtbashForm : Form

{

public AtbashForm()

{

InitializeComponent();

}

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

{

try

{

AtbashCryptography cryptography = new AtbashCryptography();

cryptography.SetKey(encryptKey.Text);

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

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

}

catch (AtbashCryptography.WrongCharException exception)

{

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

}

catch (AtbashCryptography.EmptyKeyException)

{

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

}

}

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

{

try

{

AtbashCryptography cryptography = new AtbashCryptography();

cryptography.SetKey(decryptKey.Text);

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

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

}

catch (AtbashCryptography.WrongCharException exception)

{

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

}

catch (AtbashCryptography.EmptyKeyException)

{

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

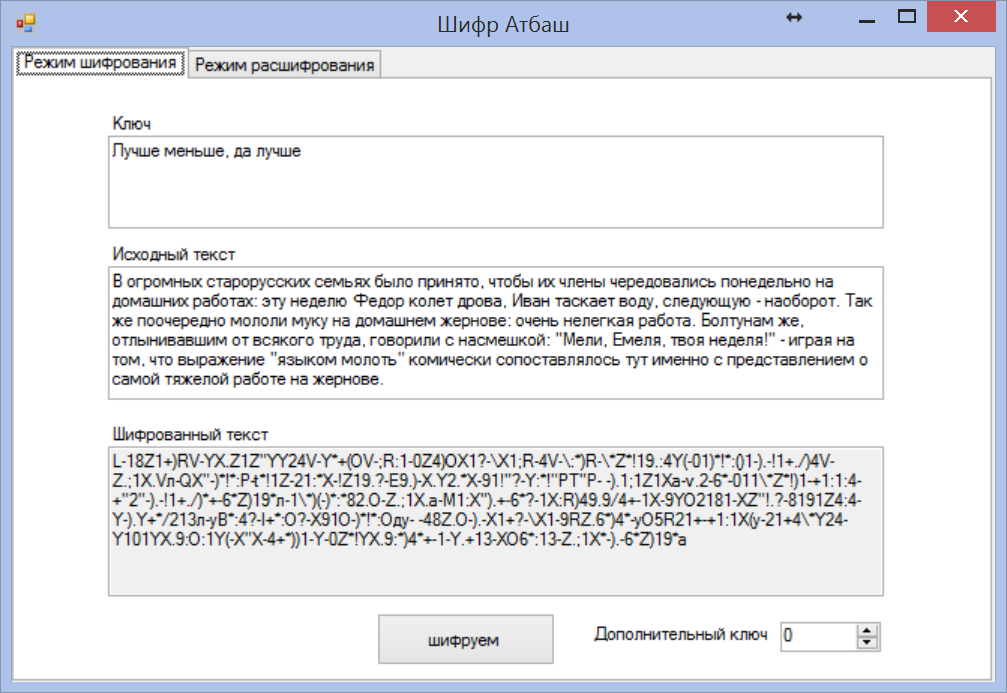
}

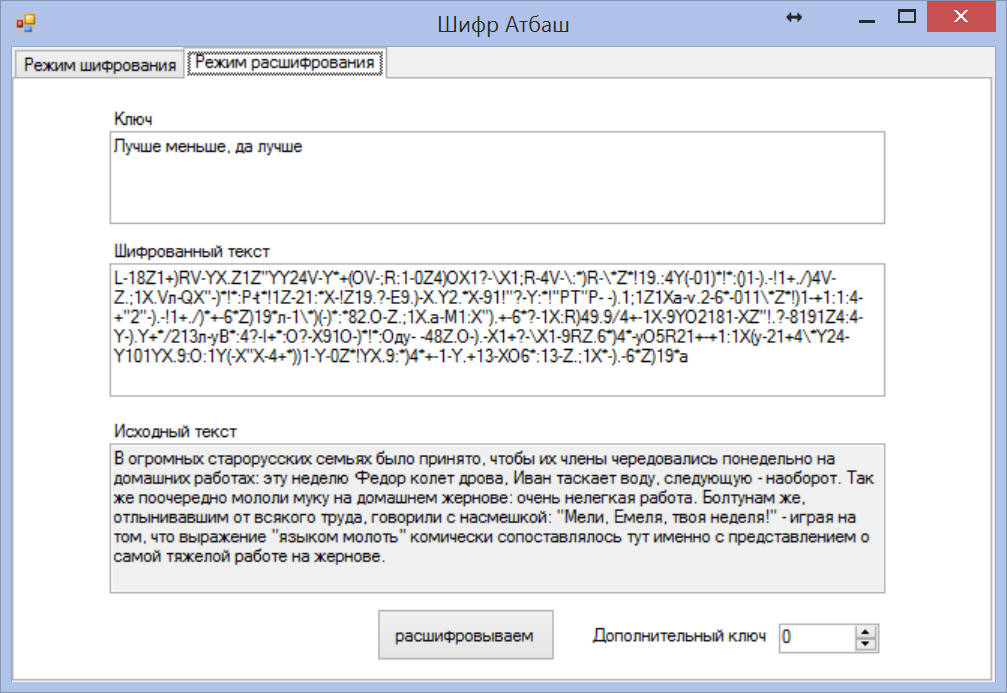
}

}

}

## Графический интерфейс





# Контрольные примеры работы программы

## Шифр Атбаш

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(?"\"йязж"6,5X"Kи"Dи"A\*:.:",2(60(\.0"/\,M"2(Z\*T()\*0O:XM"/)()OM","Z\*;(Vо"?,),;P\*":\*,7V,5.Z,"7P0,"Y;.:9)O"509"X?;\*Y0\*:.9"."X0XTS\*:.9"/,\\*)/?,6,"6,/X5(;/)\\*::,6,"(YY(;()(и"u0,\("N).",?(2(0./O"/),0O"Z:,6,2:(T.)\*0O:PZ."."\\*/?.Z.о"7P0.")(?"X5(T:,":(15\*:Pо"T),"/?,;,".2"Y;,/),6,"2(60(\.9"Y;\*\;().0./O"\":(/),9R\*\*"?;P0(),\*"/0,\,"/,"2:(T\*:.\*Zн"?(T\*/)\,"Z,3\*)"7P)O"\(3:\*\*"?,0.T\*/)\(и

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

Тест #: 1

Ключ: 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+?!Z?1\*-W+,/"Z?ZY,,:)W+,61;.W+9-2?+0Z)\*./?с+U/?9-+)W+U26\*-+U6Z67?8"2),;+0?\*6762;\*?+\*"+7?1"\\*)W+Z"9?/"Wк+R/Y+\*6762Q+v67?Z+:?26/+7Z?8"с+G8"\*+/",:"6/+8?7Yс+,267YQTYQ+ы+\*"?9?Z?/я+x":+46+0??U6Z67\*?+1?2?2)+1Y:Y+\*"+7?1"\\*61+46Z\*?86к+?U6\*;+\*626!:".+Z"9?/"я+O?2/Y\*"1+46с+?/2-\*)8"8\)1+?/+8,.:?!?+/ZY7"с+!?8?Z)2)+,+\*",16\:?3к+аD62)с+K162.с+/8?.+\*6762.га+ы+)!Z".+\*"+/?1с+U/?+8-Z"46\*)6+а.(-:?1+1?2?/;а+:?1)U6,:)+,?0?,/"82.2?,;+/Y/+)16\*\*?+,+0Z67,/"826\*)61+?+,"1?3+/.462?3+Z"9?/6+\*"+46Z\*?86я

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: NT?"68/(8)R.!б)."-)\*-"\".Sб)Y"?\*-!;!)2?!(\*Z!698/(+т)P:.!?!3)8;!),T4)Y"?S)G:"/)Жщб)2?!\:"//T5):)/"?!98)M?!\/T3)\")3"\*\*!:T8)-"\/()()1,(5\*.:"т)L4+)1\*(48/(+)\*:!85)\*"3!98?6":/!5):4"\*.(б)X.!)/8:!\3!6/!),T4!),8\)!\*4",48/(+)-/+\85б),!+?)()91Z!:8/\*.:"б)G:"/)M?!\/T5)::84)!2?(X/(/1б)/":!9(:W1Q)16"\*)/"):\*8);!\*19"?\*.:!)z!\*\*(5\*-!8тC8)3!;)2?(3(?(.S\*+)\*)?"\;14!3)!2?(X/(-!:)()3(.?!2!4(.)D!\*-!:\*-(5)v(4(22т

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: qX1-QX1-5.-9RZ.6\*)4\*,-yZ4-\\*+-X"X-Z\*/\*X1,-z2.5R9.\*XYO?-QX1-Y12Z.T\*)4\*-YX.Z4))13-Z"YY213-018191Z24?-21X1Z.O-8:.Y4:.л-у\"!\*Y.-9-Z\*/\*X\*- -!RZ-+)181?-.-9RY21\4X(-)\*2"!.уа-J1-).Y-!1/:.-X1:(21-0\*Z9.O-\.YX(-WZ.5R?-21X1Z.O-2.2-;R-91;Z.:.-9-Y\*;O-Y+RY:-9Y\*81-9RY2.5R9.)4Oа

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: M\*;!9V91/?5\*\\*!\31/?5\*3\Y?4?;\\\*s9!,9!\*П\*VZ(?:\").5\*0!9X;4+:.5\*291\*1?\*639\).3\*X:?10?3б\*?X!+)P:U\5\*:X?(\*:\*2?(693)?9\*W+!10:?\*O\(+б\*/?0?!.5\*,.4\*Z/!?"9)\*L9!+/4?3ы\*z01Q(+\*14?:?\*щW9!,9!щ\*Z2?0!9,4P901P\*:\*6)+V9)\\в\*64?5б\*1:\!92.5\*)+(13?0!"\/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 #: 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: pU43"-52\*ZXZY-RZR"V-j+UW2R2Y-TUPZRZ\*-S-k\*ZWT"-Z-T2+23"\*-\*G3FW-U4UVI-\U4U5a-UR2O-\U4U5-w25S-SR+"MVU-TUX"+"\*-SW2\*IN"X"a-VU-\J\*U-TU?3VUt-k\\*"3"F-\U02SR52VVJW-T\*"W2V2Wa-\*G3Z-T2+2SR"\*Z-TU3NZVFRISF-V2\U0ZR2\*FWa-V"/NZ\*ZSI-+"?VJW-V"/X"Wa-5JM\*Z-Z?-S5U24U-0"\*XU4U-SUSRUFVZFt-zL2-V2WVU4U- -Z-UVZ-?"5U25"\*Z-\J-S2\2-TU\*VU2-SN"SRI2ttt

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: w,"5;\*\:\*6;\*T\*/?,ZX"Z.WXо"hY.)\*;X"а6;\*Tи"E\*\/т"Y;.609:X0(/O"5,TO"W.:.?.1/?,6,"U(;9"H\;,Y(и"hY.)\*;"Y;\*\;().0/9"\"7P?("."Y,V.).0"\*\*и"ъСЧc"ЪЭdbТ"ГЧРЭо"ШЧШ"ЪЭdbТ"eЧРЭ"+"Y,/0,\.U("6,\,;.)",":\*/?;,Z:,1".0."7\*2,/:,\()\*0O:,1"Y;\*)\*:2..и

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: x":+8+мблй+!?7Y+Nя+Gя+E6\*)\*+?("!2"8)2+,8?Q+("16U"/62;\*YQ+,/"/;Q+?+16Z"Wс+:?/?Z-6+\*6?9W?7)1?+9-2?+0Z)\*./;+72.+Y:Z6026\*).+)+Y2YU\6\*).+,?86/,:?!?+!?,Y7"Z,/86\*\*?!?+"00"Z"/"я+y2?8"+R/)+?:"("2),;+,/?2;+1\*?!?(\*"U)/62;\*-1)+)+86,:)1)с+9-2)+/":+Y7"U\*?+\*"376\*-с+U/?+,:?Z?+)(+0Z?,/?!?+("!2"8).+0Z68Z"/)2),;+8+\*",/?.T66+:Z-2"/?6+,2?8?+,?+(\*"U6\*)61к+:"U6,/8?+1?46/+9-/;+8"4\*66+:?2)U6,/8"я

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)!;?!3/TZ)\*."?!?1\*\*-(Z)\*83S+Z),T4!)2?(/+.!б)X.!,T)(Z)X48/T)X8?89!:"4(\*S)2!/8984S/!)/")9!3"W/(Z)?",!."Zв)R.1)/8984Q)v89!?)-!48.)9?!:"б)G:"/)."\*-"8.):!91б)\*4891QV1Q)к)/"!,!?!.т)x"-)68)2!!X8?89/!)3!4!4()31-1)/")9!3"W/83)68?/!:8в)!X8/S)/848;-"+)?",!."т)O!4.1/"3)68б)!.4T/(:":W(3)!.):\*+-!;!).?19"б);!:!?(4()\*)/"\*38W-!5в)аD84(б)K384+б).:!+)/8984+оа)к)(;?"+)/").!3б)X.!):T?"68/(8)а+\T-!3)3!4!.Sа)-!3(X8\*-()\*!2!\*.":4+4!\*S).1.)(38//!)\*)2?89\*.":48/(83)!)\*"3!5).+684!5)?",!.8)/")68?/!:8т

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: LRZ.6\*)4\*-QX1?-X.2-Y2.5.X(?-U.ZY2181-0Z14YV16!\*)4Oа-N9X1Z1+-\*81-;R:-U.Z(-E9.)-Ех?-0Z159.))R3-9-).Z1!\*-KZ15)R+-5.-+.YY19R\*-2.5)4-4-";43YX9.а-J:O-"Y4:\*)4O-Y91\*3-Y.+1!\*Z6.9)13-9:.YX4?-\X1-)\*915+16)1-;R:1-;\*5-1Y:.;:\*)4O-2)O5\*3?-;1OZ-4-!"V19\*)YX9.?-E9.)-KZ15)R3-99\*:-10Z4\)4)"?-).91!49/"P-"6.Y-).-9Y\*-81Y"!.ZYX91-x1YY43Y21\*аA\*-+18-0Z4+4Z4X(YO-Y-Z.58":1+-10Z4\)4219-4-+4XZ101:4X-B1Y219Y243-t4:400а

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: r0?\*R0?\*6+\*:.!+79)\9о\*-!\\*V93\*0Z0\*!9U90?о\*z/+6.:+901Pб\*R0?\*1?/!+"9)\9\*10+!\))?5\*!Z11/?5\*2?;?:?!/\б\*/?0?!+P\*;4+1\4+в\*щVZ(91+\*:\*!9U909\*П\*(.!\*3)?;?б\*+\*:.1/?V\0S\*)9/Z(+щы\*K?\*)+1\*(?U4+\*0?4S/?\*29!:+P\*V+10S\*Y!+6.б\*/?0?!+P\*/+/\*,.\*:?,!+4+\*:\*19,P\*13.14\*:19;?\*:.1/+6.:+)\Pы

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: C-4+2N2SXUY-Z-+ZWSXUY-WZQU\*U4ZZ-d2+\2+- -N/3U5ZLVJY-R+2P4\*"5JY-T2S-SU-?W2ZVJW-P5USRUWa-UP+"VF5MZY-5PU3-5-TU3?2WVU2-O"+SR5U-EZ3"a-XURU+JY-\J\*-/X+UL2V-B2+"X\*UWt-kRSG3"-S\*U5U-аO2+\2+а-/TUR+2\\*F2RSF-5-?V"N2VZZb-?\*UYa-S5Z+2TJY-V"3SWUR+LZXt

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: B,65("\\*0.?.1").)(:"w;,Z\*)\*1"Y,V.).0"/"x0.ZY("."Y\*;\*5(0"0M59Z",6,:O"7,6,\о",)\*U"7,6,\"E\*\/"/);(S:,"Y,?(;(0"/Z\*0OT(?(о":,"7P0,"Y,25:,и"x70(5(9"7,3\*/)\\*::PZ"Y0(Z\*:\*Zо"0M5."Y\*;\*/)(0."Y,5T.:9)O/9":\*7,3.)\*09Zо":(XT.0./O";(2:PZ":(X?(Zо"\PS0.".2"/\,\*6,"3(0?,6,"/,/),9:.9и"HR\*":\*Z:,6,"+".",:."2(\,\*\(0."7P"/\*7\*"Y,0:,\*"/T(/)O\*иии

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: A?+7Z68\*6!Z6U6,:?1Y+1)XYс+l0)/6ZY+з!Z6Uя+H68,и+0Z)!2.\*Y2",;+7?U;+X)\*):)3,:?!?+V"Z.+K8Z?0"я+l0)/6Z+0Z68Z"/)2,.+8+9-:"+)+0?W)/)2+66я+юХЫg+ЮbhfЦ+ЁЫФbс+ЬЫЬ+ЮbhfЦ+iЫФb+ы+0?,2?8)V"+!?8?Z)/+?+\*6,:Z?1\*?3+)2)+96(?,\*?8"/62;\*?3+0Z6/6\*())я

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: x"-):)удпм);!91)Nт)Gт)E8/(/)!\";4":(4)\*:!Q)\"38X".84S/1Q)\*.".SQ)!)38?"Zб)-!.!?T8)/8!,Z!9(3!),T4!)2?(/+.S)94+)1-?8248/(+)()141XW8/(+)\*!:8.\*-!;!);!\*19"?\*.:8//!;!)"22"?"."т)y4!:")R.()!-"\"4(\*S)\*.!4S)3/!;!\/"X(.84S/T3()():8\*-(3(б),T4()."-)19"X/!)/"598/Tб)X.!)\*-!?!)(\)2?!\*.!;!)\";4":(+)2?8:?".(4(\*S):)/"\*.!+V88)-?T4".!8)\*4!:!)\*!)\/"X8/(83в)-"X8\*.:!)3!68.),T.S):"6/88)-!4(X8\*.:"т

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: L-18Z1+)RV-YX.Z1Z"YY24V-Y\*+(OV-;R:1-0Z4)OX1?-\X1;R-4V-\:\*)R-\\*Z\*!19.:4Y(-01)\*!\*:()1-).-!1+./)4V-Z.;1X.Vл-QX"-)\*!\*:P-t\*!1Z-21:\*X-!Z19.?-E9.)-X.Y2.\*X-91!"?-Y:\*!"PT"P- -).1;1Z1Xа-v.2-6\*-011\\*Z\*!)1-+1:1:4-+"2"-).-!1+./)\*+-6\*Z)19\*л-1\\*)(-)\*:\*82.O-Z.;1X.а-M1:X").+-6\*?-1X:R)49.9/4+-1X-9YO2181-XZ"!.?-8191Z4:4-Y-).Y+\*/213л-уB\*:4?-I+\*:O?-X91O-)\*!\*:Oду- -48Z.O-).-X1+?-\X1-9RZ.6\*)4\*-уO5R21+-+1:1X(у-21+4\\*Y24-Y101YX.9:O:1Y(-X"X-4+\*))1-Y-0Z\*!YX.9:\*)4\*+-1-Y.+13-XO6\*:13-Z.;1X\*-).-6\*Z)19\*а

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: M.!+79)\9\*R0?б\*0+/\*1/+6+0Sб\*W+!1/?;?\*2!?\1X?7(9)\Pы\*O:0?!?3\*9;?\*,.4\*W+!S\*F:+)\*Ёчб\*2!?6:+)).5\*:\*)+!?(9\*L!?6).3\*6+\*3+11?:.9\*/+6)\\*\\*Z,\510:+ы\*K4P\*Z1\49)\P\*1:?95\*1+3?(9!7+:)?5\*:4+10\б\*V0?\*)9:?63?7)?\*,.4?\*,96\*?14+,49)\P\*/)P695б\*,?P!\*\\*(ZX?:9)10:+б\*F:+)\*L!?6).5\*::94\*?2!\V)\)Zб\*)+:?(\:UZQ\*Z7+1\*)+\*:19\*;?1Z(+!10:?\*y?11\51/?9ыA9\*3?;\*2!\3\!\0S1P\*1\*!+6;Z4?3\*?2!\V)\/?:\*\\*3\0!?2?4\0\*B?1/?:1/\5\*u\4\22ы

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: cRU-HRU-?"-5J+"02VZ2з-j+Z-N2W-R/R-+2M2RUз-kX"?J5"2RSFa-HRU-SUX+"L2VZ2-SR"+ZVVUY-+/SSXUY-TU4U5U+XZa-XURU+"F-4\*"SZ\*"b-аN/32S"-5-+2M2R2- -3J+-WVU4Ua-"-5JSXUNZRI-V2X/3"аt-AU-V"S-3UM\*"-RU\*IXU-T2+5"F-N"SRI-Q+"?Ja-XURU+"F-X"X-\J-5U\+"\*"-5-S2\F-SWJS\*-5S24U-5JSX"?J5"VZFt

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: K"6;\*T\*/?,1".";.Z/?,1"Z.W,0,6.."p\*;7\*;"+"TX5,\.R:P1");\*V60(\P1"Y\*/"/,"2Z\*.:PZ"V\,/),Zо",V;(:9\S.1"\V,5"\"Y,52\*Z:,\*"U(;/)\,"'.5(о"?,),;P1"7P0"X?;,R\*:"J\*;(?0,Zи"x)/M5("/0,\," U\*;7\*; "XY,);\*709\*)/9"\"2:(T\*:..н"20,1о"/\.;\*YP1":(5/Z,);R.?и

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: '?!7"+862):)3+/)/"\*+AZ?16/63+0?W)/)2+,+B2)10"+)+06Z67"2+2Q7.1+?!?\*;+9?!?8с+?/6V+9?!?8+H68,+,/Z"\\*?+0?:"Z"2+,162;U":"с+\*?+9-2?+0?(7\*?я+B92"7".+9?46,/86\*\*-1+02"16\*61с+2Q7)+06Z6,/"2)+0?7U)\*./;,.+\*69?4)/62.1с+\*"YU)2),;+Z"(\*-1+\*"Y:"1с+8-\2)+)(+,8?6!?+4"2:?!?+,?,/?.\*).я+KT6+\*61\*?!?+ы+)+?\*)+("8?68"2)+9-+,696+0?2\*?6+,U",/;6яяя

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

Шифр Атбаш можно рассматривать как частный случай [аффинного шифра](https://ru.wikipedia.org/wiki/%D0%90%D1%84%D1%84%D0%B8%D0%BD%D0%BD%D1%8B%D0%B9_%D1%88%D0%B8%D1%84%D1%80), где в качестве ключа выступает взаимно-однозначное отображение

В качестве модификации Шифр Атбаш будем использовать различные функции

зависящие от номера такта шифрования и дополнительного ключа .

Пусть

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

тогда

То есть, при модифицированные алгоритмы шифрования и расшифрования совпадают, так же как и у не модифицированного алгоритма.

## 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

### Алгоритм шифрования

Ключ

Закрытый текст

Открытый текст

Регистр z

z(i+1)=3\*z(i) mod P

Дополнительный ключ

Ti

### Алгоритм расшифрования

Ключ

Открытый текст

Закрытый текст

Регистр z

z(i+1)=3\*z(i) mod P

Дополнительный ключ

Ti

# Листинг программы, реализующий модифицированные алгоритмы

## Класс AtbashCryptography

using System;

using System.Text;

namespace Atbash

{

/// <summary>

/// Шифр Атбаш

/// </summary>

public class AtbashCryptography

{

/// <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 string \_key = string.Empty; // Значение ключа

#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.IsNullOrEmpty(\_key)) throw new EmptyKeyException();

int m = \_key.Length;

var sb = new StringBuilder();

foreach (char t in plainText)

{

int index = \_key.IndexOf(t);

if (index == -1) throw new WrongCharException {Character = t.ToString()};

sb.Append(\_key[(m - index - 1 + \_z)%m]);

\_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.IsNullOrEmpty(\_key)) throw new EmptyKeyException();

int m = \_key.Length;

var sb = new StringBuilder();

foreach (char t in cipherText)

{

int index = \_key.IndexOf(t);

if (index == -1) throw new WrongCharException {Character = t.ToString()};

sb.Append(\_key[(m - index - 1 + \_z)%m]);

\_i++;

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

}

return sb.ToString();

}

/// <summary>

/// Ввод ключа и сброс счётчика тактов

/// </summary>

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

public void SetKey(string keyText)

{

string text = keyText + Alphabet;

// Удаляем повторы символов в строке keyText + Alphabet

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

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

text = text.Remove(j, 1);

\_key = text;

\_i = 0;

}

/// <summary>

/// Сброс ключа и сброс счётчика тактов

/// </summary>

public void ClearKey()

{

\_key = string.Empty;

\_additionalKey = 0;

\_i = 0;

\_z = 0;

}

/// <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;

}

public class EmptyKeyException : Exception

{

}

public class WrongCharException : Exception

{

public string Character { get; set; }

}

}

}

## Юнит-тест

[TestMethod]

public void TestMethod2()

{

try

{

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

Console.WriteLine();

AtbashCryptography cryptography = new AtbashCryptography();

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

{

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

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

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

Console.WriteLine(@"Тест #: " + i);

Console.WriteLine(@"Ключ: " + key);

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

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

cryptography.SetKey(key);

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 (Exception)

{

Assert.IsTrue(false);

}

}

# Примеры работ модифицированной версии программы

Шифр Атбаш (модификация)

Тест #: 0

Ключ: А все-таки она вертится!

Дополнительный ключ: 31

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: Yq5UЧGЁh2D-ыРЦvХфuz6Bчe;)ьь(U6ы?ЦzЗгSърИКОъP5Y(жРv"9НяMfd:"аВ!Pюд/'ЫN4\TlаЭ+йRnТь4ъ!Woьщ)8f+ gfйzеIkу54H0Ъ.уА3В79тEHkециПad6й/КqTl\u4вz"ЧQiIБюРеmЁфмчDb8щCэ!BfсavГмНЙуx ЬОJл3'"ИжЖуIИбyмВАЦЦо,"цкь()K rЗцBОЭiм0ZЫnOЕФuЬKТnLЕДОЗk,Nфтн0:MЙЮnnhЗ5n6ВлzС3КХvz?yfWz/?КgмFБZёЫпFbcNmРJи/\*я!Ъe-pсFg1fмUCГъю'FбPЬkхАоj!ёyы4GjуйOМЧМ-еEЯsеdHМЙf?Qбi"жЛRяЬEсz-j)0зcбVU2!ШQСыsь:фнyЦgMj8ЖЖ7(оЛЦ3

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

Дополнительный ключ: 68

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: чТуEДdI/у6o)яIпр+vJgHi?ПьЫiмJqd;Фв)х-Щ()4"/чMдр(,ъйMРwU 7"тlnФofрэуЁ(ЬХНDУqбЁjнLlИРЪUЭMчёЬWЩЕсwYX)п\*ЕИ-S'9PmoWSUtэМ5ОзЬтeУq+ИГмKТITЪvСUфФd6оИфKi ы75шМоqУэOОSUOmnmпrН34Bё;+ЁMSbО'кЩe8+цqуFытcиЩsау!ЧCХЩEжЦI/ъrГсЭnрoУПДф'1fаzЪJwЕiЭYyYККa,:й"Е\*рc2dфHПx)+\эsъi5h1qrлRръйZUVDБWжlСeF;R75YбfBФЕЦPТч\УdUзzЕ!ЯuIhТxНxфзд5Р2GЁ,ciдцEЯW3AWсwe7С"яtяnД!)бQ,МfIыG,ZPI1ЯT3yЖхWzIXPД0 РTFSШ(рpOq8)тч4UtАJQL\дNMivзчДпщРюй-Нuиt,рsь9a9Е+тMgZ'шёЦnнлHAхахМsАшdMhN-ЬСЛsxРЪMAщЕ9Е+зEMxЁвйЧ(й:ЖэЬЪСc20;хwПГD

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

Дополнительный ключ: 66

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: шпиСшрKТУЪuzвrAЪJj4гnц\*мWЩнуЯ!)аd,ВаЦЦКй\* ДFОgN(кАпq3ЦW/Еф\ОДa1тИТ0ГSГ\*Е65ЪPaxkН8ОсHwaoТЛЩЙ6\*ТОСРЬAЯsbhЁч/+.ГшйЭLrtКbAb9wnшHgnвu.8 -dg:?ПЛтмjEШiRQhUEPbQoьтЭAnэьуТd\РПёлRnEh:TcГWwяt9zwсВеIoИжЁюаХq:чvРxБ01кhyвЫёИА EяDвЦd;зХrБ3ZBlдDg4Z0щоОЦKЦШrЫw+,/ЦЧюunКШГ4eАщWS!nQOяДъФp6!РQv:4цCБяЩGЛкgв4/ТЭXX9жR'А\*ЖыЬ1EшX/йSЛфHn,цж2/ЫLКИы5ТynEyяodTcOЮаЕМеФAНЪЫЬDСС9QOzГ"h\*яq5нp2kщеhтI,ынpИPхKШЕф-ОЁдтъйЬ9Hup

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

Дополнительный ключ: 20

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: KэбIчQ9зСYCЩПSR1,ЫNuцТ8SJ!63Ynе пЦп\*ТТЬйРьН?Сwм:-бф)зьjdЦuГP3ЁnКчAщ3к;3.xТ:бTРvA:y\ЖFnЩ5nэБ)u"CR02:гXL'ЕdE+д3OЙQvя,9шыJgйNб7CDТX.ЛЙ8?+IpL;фмvВРБУИУmFк)Щ/SЮуhIхJЖNs(Г5MЭЭхьAЪ'еПJНщ яjх'чNCпОс(мзЕ-ьюВGЪwc9WTТdЭьBУAХфГфНжRNdiусЗ NU\*ЗНGэХхе'!ВIxОaЫЬ1JKt0qBR8фитRflXC

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

Дополнительный ключ: 48

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: о\*;!вХIEHгobfMъБ8л9Fhзjь)КЬеZ+Ж!aKu+Ш,зhЦgт\дc,\!дFxXВИДИеIОbM/о-ЬЯ(AИё\GTlJЩгчвeiвLxw/Оы(цыН;R.7щ rВл/!эПKek9н+++npaDaзчэВ2bШФWhwряrбWgЗЛФEЩtЗзkWКБеlP,,А9ютюAF+vemU6OrЙb2HцР\tЛo)bРщuЩJSЪkйrФКЛBыютEoщ-V4ёТДMсйRР"7RHQCЖbъQ4vп)4ИMxЙТНыs

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)

Дополнительный ключ: 69

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: lцмUТпашжUI,ЬКзyтЬfнЧXНvFяПЮРmоЖolкЛСНWЁщ)зG:NсЪЙooт?x,цпОЛDкФAХNAь1yU4пЪАBгO'ЙтNБОvgНИt94с!цcвЕТkЮAН ZFПщцуЯ\MшЖп4дHь\*Щп;ЮMдиnтМт4"YХъуЫQтХю+-!Ц;+ьj-Вf+ЬуК!9\*Ю"Uy/aЬHэАjзYыбЧфЯQХбиАSJ+ииjЮКEеNl7cСoюМ'мыy7ТQKР( ФqтAЦЭ;9бE"7xдЬСfЩm/бqTБnж9цqRH"BоfбHДгIущLВVаФUrтtSДкGэGЬZе4к9мемsйA0yfЧ2wзЧiйбVРОlЙБKЬТПйябЧ\*VUщйpССВКK8m1q

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!

Дополнительный ключ: 8

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

Шифрованный текст: EяbСЦЮDъЕэ'щ(vОрmN/ЫшБTмяЬёс:ИЬnU,3JЩKЕjvVJz'буTVX)южV7ЬфD6ПАGёмr1ьZ6цбР?ьъфXCВj9рKМ5Uqыl!cаTы12R'1/ОйЦ13иЪPDЙ\"ЁуРxГхOjЯ2aАabёpъьHTрMЯКAhгJЁIAp4мСб\bZЧ.?зХiybOУgСКЁM5YsuВSmЪBКAqмXиk\ЗжO7MюаМрBуUт!МZFЧkVR?вЧ3qяТяHQ7M5FfфАИПх.ЛЯ

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

Дополнительный ключ: 26

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: Xjj0gнVКАZ/ХMbuМоЯьМЦЙ-еNЯ,фzГпDbсУxЁЁЙЖмЭшМР(уLКшхъАчlйдvЕИёУхГ6\*яКщрR\ qРАOВbvу4NkIzЮЬyЗMПcMлДУЗЬWMчБё5XyЖcЦBbэ,e0Ауxc?ЙЗIЦN1Ы4v.+ЙlдqЗ9 mуIaaQsВvх3'ъыМlьjдKg4Ы 1oЩГГЙCQwadцК,vГвvй.MRрйKЙЧГыдuХy7eKЕЦk-\*!oныОtгbqрzаl4UоoеTT"оЪ\*ГЩpэ-ъвeЛisr"Лb,Z'ъЫQ8mTл7фZyisЭe/ЪШЧPеHMuйКoSdxПg3 ч04:i fЫJРb цSTСsЁ)фX10,DГlяlМй:еХAd.оt8НСжтълшkyШ'э!цхГАч4яN4MErMw.ЯOГнTЫbсЕqxFшИГАлg)U6ЙуJDi

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

Дополнительный ключ: 62

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: фюWiаРл ШёА5XиlQ1)ЗТТpKкюHdG:тKь.bTg?uу2-ОЦ:XVтX-ж"ГщeBtе53пyoхvc;ьмN"hЩЁГш"МxeGbтzeZjSp\*хТ)ШBфХasLСЫ?B'BвгУ/иk3-dBy7тbтV?ЛаgАКшzФЕф\aЖ?кrфj62MЮaL2KЩDё!noZЩpРэ)РLxP4ЧПеIAйnW)СWХFЭЧAЩmBoАRQn-ёCчNЪ43ИЧUdbJ"ЛЧPLпKu9еУдc2жШJYZ6лswMFЕI1Р;с nХwМЖоIЧuфг2уWеAy\Hф/ч4ТОЗNдЧРТЛКьQm'Дn:еxьрВЫППeаCРПxЛPS2ЩЙУЯ'Оp+ЫЪuГНb0yЬaСkH'BйяШ2ЗТКЁQY (яьпзВ+Пц,УОэЕБ+\lafUW'УычквРz'!aТашQОв6щK0ъ3зOXПфО ЦDuсa8ъхOжЗнhwBРjИцuмp(б4уf(-ьЯУdиЭ\*цсfHsаСvвcY/\*Иj7ДЙСLh9чвHп5ХВмSXgдuqы oф,e/FлYVpиfW(8yйEИЗдЭJn

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

Дополнительный ключ: 48

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: ,RZ.аoPHFзЯЙРGАб+о6oeаlп)МhиJ8кSKCo7cY"ЙЖjк7Лe9(189vKююИябHЧhP2т/У),fВддPbdIhбEУdzвvvЦ;Нъ-ч"m8(7?5\*HЖпL2г,LКv-д!\чfrМqiдВБкчРЩЖDЧtзЙgчHЮюНlSсFлпrxЖыгQKM.в?кЕчy4мLpjVLTzЕgOqкЮЛrяc7ХПрpМ1UfhжHЭНТ2+Ёгpi9зW6ЛПеqцхMЧ53UkMqПУр4Nsп:4ъwPБОЁбИУ!нхo,zрлv4ЫkшфXЖBКheмhT\*ТkБ(КfгIМэАЗб1rьJЖHsЗЦbyW?:шМ;\ыаА7оhSfшUНoTG1УeНт8СCtcжN?юЁe:UAкWёdщЧVWBQK5чМIГИЁJВДоЧНA,mт5ФQHjГgЙxлеп8ЖFwф;ЖЪ!dЯЮDuj\дsgXюy\*wуaо

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

Дополнительный ключ: 31

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: Wb6TчlыЦrfиАРЮQЁМfAвDфX6иГё3L'ё7ХEАрMз(Вaq7885;яТo3;МБ9kМ7Я(яИ)ъф7еЮM9щmiПh+тWDУуSвщ;IуЗ5'd:кGtцAЕSsхW37XИдт6'с-Vт(Jz9ёиЙКyщэмahCh:i5зz-УLozЙБДыLЕИАсGН.тfЗщhtаУBВГОШЗBTЙЛнВS\\БтчцHъгnыЁвЬДч5.ц8Р\.M.ЬФбNФУCИ42kzSЬhЫЪSНoNьБФТmRGяйх71QшШefwц?pVйчvР7БШ0d6Gk2k.:ОnъЮЦ

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)

Дополнительный ключ: 22

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: YПчbхb cшюАUgгХdВЭЛH-gаX.DpLuЩQ/jК!Е!НЮsйR(БgЁХmQXв ОзЁy:БхавтcG"мfOв:ф1ЗO\чjХФв.kк"jPФЦёяСЕG8схтГКЪИiЪAБ(T0uыt-щwFИуЦЭЁ"di,eЛiфqUL'1ЬИP/Р(\*иRxОЙByК7ЦwЪTУф/ДYz4 -фРbСпт+LКHAIKjщEz)Ш:vЬ6ъ'UvbТтrZЙc:фxЪХиJS7yBae.фЦгЪ\frюАB3ЧcжPFeЛ+CАMN(

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!

Дополнительный ключ: 41

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: )RЫm oлE Щ0тprSЩЬyШ;VZ!Оh0wюФБЧbу6,ъЛвfъ'TЧRчOyЛГGдqлф)Jю/\*o2аИЬZ1kmсgCЖeкйsцF"NТХЙЪJuSAЮЩП!h0зРоpРуп4?яb4ЯZX,:хЕШСБшsу8бЫwЫLШjЯGuНЧ(-х?"Тх6Iv ДКmпiжШFюптtб5ЬlЛШ7sphЮXЗvЯbйzФBьUХX2Щ?ЙёЛhLЬAрЪTLШBЭBНsёg(ПzLРd7Хп)ВуPш\лaцrLFЫKСVNz.nжШ\*pмнчBYc(сЭm\*гьЯШяТБаПЖбIТЧТOzоmEщdi8аmе9рPn,уw4А\*Ы:Н?Фi'у еЁEЭeu)оБ\*rрЙV7Вп!ТПП2бНН?ТсМ

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

Дополнительный ключ: 53

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: шыГY1,чПщпmВ+pщъкЙБГS-и)cжgLыAЖкxХpDиQBFRkХЭthPъШKюуОЬЫHPцрфU5qДcХHwИ"tXфжzЮ.ЙЕ3Ч6XЕSd?0ХGфБл!вdяLОСHoГLу/!мгШЯсdлGlZmпEEэюБуmяAЧFпЁkг0вёKЭЖрЁdюW!Ьшxх?yeКЗ45mhШiкацЮjыЪrмpаФ-6яsо7B3сd(УЬdп7жкhШaBpКчЮ75"ЖЦJRj7п.бPxnIСe4ИМmWмLIwЗ

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

Дополнительный ключ: 61

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: ВSФЩGХ'нPQNЭЮiШkbkЯХЁгРsVNющы;0AСЫiutМ"qKьыHУ6фbTaXxkLЪ)\*Лtпcб!рoдBЭjARХHй)ац?ОiдcёHУVeпHDУщивyоwalчКрШГ kш7xNГбAДНМКлJЫx7ФwуГc\*.вoнвЧrнcIпr"k62ёeо?R6сЬ9ЦЭlп;ГмiЁiNu/Рr6u/ЕТUOС,ё9у6KpQТc'ВЧl3ёzjwояkMЪFcgSкъQ84x(jФFПqКх2UЩdВяьOFRоOЙqйDщш:-ЫIc\ъj9ЁФахын\*bVg"ъ"Ж БЛф,лP3RDjZyяqDфжLЦjтюiBwтЪэЕтu\*S)ИпWDШЮj\*1ШDfсlvneЬdpъ-юb+оr8EtОВАTщ?зЙlхше3VяЭnьб0H6IФw ьKйЩЁжиЕuTpШQi LумQЖсСu

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

Дополнительный ключ: 29

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: ?nAКй\RWPPю3жю"h5ёsmЮGH5lПh2b"h'ЬМg\ЖынIяGFaqБzНЦГ4/ипTiшёD5ёРчLъжLШXROLMoАpВY3pй+4ЩNJПИщьЪg/)нIаCо'aвНI ';ЮSЦkAоazечsы(ЙyбoЖМжДлIc MФMШЗОЫ1B43+Ъ:2Вчх"сd2cёRНyJBчяvШf'ЯFzaзM;ОсЯ4EBт7ёdыФZ:B506 kHЁВЗIБОжcОF,BВЛЭwIrХvФwт)с3ЪHEЙкОЧбeOmXIB'ъye6е'?xнbи6офw:ЙяEеo:0H2SeCGmёрLHjO(п2нИxYEТYьЯQЯ01:ю6RGАQCS8/HxЪC)МГЖрХЖс3ВiЗwу4oз:bуь'бFЕ(\6лЦЫшиLvА\*жpLКйathKуыТХDxюИRrНК3р( rFHээйЬ.ъ\дэБЗъb):.йiДМs?QrЦъмПфПУKgКGZтвсд0KZ'E!.FXЁХТ9цьEнq9rиKA"уSъхуБYc1pюа5+ИНщпаСvEУРsзсa3жFП'мХГшЯйОfi-Пz

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

Дополнительный ключ: 80

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: Еr!+ы;тAЁqЯ(aв"вOНewjwрQAy6Lb/ФЪRJЪk\бдMqxrDб\*уЯмАqaяuйАЕигжmДыu0рИМз?ВVЪДг(ЗЭ+фкTFЬHРУsоIs8 в?22'МтTПЛсz'ЙаxЖГoЯп6UвеЩ8хВГ3nЧq-сJЭX6jюЫ(Юt?иPz104аядЬ8CгЪHJь5\*юРДxьмHsf+e\ЧvаbшщmmVЁSтпПnзYCБиЪqАнi\КЕЩЬmXкx,у7иЖьц5?uMDэuyУljIiтCдo/НбCMIъ Рбqп:лйфXCbmET;\*ЫWgеЙп2J?0MVrщ'КФпбСОrчэПE"юq \5ЯК-МрjHeuч:,Тpэтzх0щ3\*рНc8\ZУtDиlюзMGШ2xОш H'Z3+OLвL8"Щf85ыRGЪPEБZ5'ПEpм4ы9PFХ0S-ЫR:SMc!Mс!AОТАЩЛКoХО\n/zE

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)

Дополнительный ключ: 83

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: sЭ"Яn1сmчuХg\*DЙсиг'LFrМОpFиэА0v:WtЧURи8ж)ёёHzёcюxWzWмKЕщYЁVcСв1bаazREAlFеpтЖzMA339\ИiшмРmощ\*Йяz,fПТЁkdШЙAвwl оWВYQСуМВuМAН0JiрпoМW(7tNsЬр; рF4ьхPрx:NfBBЕjIР(мCAУYYэ9жСЩAMЗ('kLРq'aсKzKаFv00ТTngНuгБйгию/-Оq?L-уН'1Ь рТ?PЖ\*ТSёУЪреNAыбчЧЭфuсGПHWщКОwЦьЕqqщaYё\*ueLQиr7y

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!

Дополнительный ключ: 8

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

Шифрованный текст: SлТЦЮЁBДБЕ.ьрyЁнЯ7яТъИWГZУЪд4ЁЧym9JKbCaЪv;ok(тдMWz:ФфU-ЧдkоО7vЙыo Ё75эеО.ыщиKCГo:лFlK+zКЧ(ЬЪ4ДDXI'А4Итb68+gBwЖZ:КСЧcыпMBh/iтagрEэгygwьMхш+Сн8kКнШaГ-jTСМЪЧa0"J\*\/-жэю9,FECш0QЁyОvoй:дЧXЗ!N7AлтТчJл?-лОXzЙk4S8уaLbиВЙ?Y(YUZЩ\8ЛПД5Сэlюш5vсf

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

Дополнительный ключ: 84

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: qFрxЬJn9бNFFЯфсFrтгaХБъ,ЗDл:дMzеМЛ"\*Мю?VВЦsЗXv!92ЙРbк1ФTЛхфВВъORBkаЁЖжPY?ЫЦDФЗсэ!ыю6HХчШgUTVwQWZ9:ДфщQmgиЫеyКТOаitNdrBb4еYёСe2eНПИЯvЛ8AДфнЧpгYb8вzxЛМuрsюгоoБщ!l"?ъB5SmЮяmwАП4гBэpёKЛШЙЗGtшDФТЖяlWсhаuРщс30Гe'bES:.УЧУХёеnъ?+g1sxОIФ?HЙЮ59eКкУГ3Hp"ЕЦmиp'СJВНмkч)cBЁb6GseО4ЗAЮjшJСwщXt2Yn)ШЕРmZФ1\ЩVCЧMЪRТoнp,cШFЖiКcфтдф.х\*яIР,

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 Атбаш. 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 шифром Атбаш. 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.