Федеральное государственное автономное

образовательное учреждение

высшего профессионального образования

«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

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

институт

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

кафедра

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ**

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

тема

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Квадрат Полибия\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

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

подпись, дата инициалы, фамилия

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

номер группы, зачетной книжки подпись, дата инициалы, фамилия

Оглавление

[2. Задание 3](#_Toc415965755)

[3. Описание алгоритма шифрования 4](#_Toc415965756)

[Латинский алфавит 4](#_Toc415965757)

[Русский алфавит 5](#_Toc415965758)

[Метод 1 5](#_Toc415965759)

[Метод 2 6](#_Toc415965760)

[Метод 3 7](#_Toc415965761)

[Добавление ключа 8](#_Toc415965762)

[Пример 8](#_Toc415965763)

[Математическая модель 10](#_Toc415965764)

[4. Блок-схемы алгоритмов шифрования и дешифрования 11](#_Toc415965765)

[Aлгоритм шифрования 11](#_Toc415965766)

[Aлгоритм расщифрования 12](#_Toc415965767)

[5. Листинг кода 13](#_Toc415965768)

[Класс PolybiusCryptography 14](#_Toc415965769)

[Юнит-тест 18](#_Toc415965770)

[Класс PolybiusForm 19](#_Toc415965771)

[Графический интерфейс 20](#_Toc415965772)

[6. Контрольные примеры работы программы 21](#_Toc415965773)

[Квадрат Полибия 21](#_Toc415965774)

[7. Модификация алгоритма 27](#_Toc415965775)

[Доказательство повышения криптографической стойкости 28](#_Toc415965776)

[8. Блок-схемы модифицированных алгоритмов шифрования и дешифрования 29](#_Toc415965777)

[Модифицированный алгоритм шифрования 29](#_Toc415965778)

[Модифицированный алгоритм расшифрования 30](#_Toc415965779)

[9. Листинг программы, реализующий модифицированные алгоритмы 31](#_Toc415965780)

[Класс PolybiusCryptography 32](#_Toc415965781)

[Юнит-тест 36](#_Toc415965782)

[10. Примеры работ модифицированной версии программы 37](#_Toc415965783)

[Квадрат Полибия (модификация) 37](#_Toc415965784)

[11. Заключение 44](#_Toc415965785)

# Задание

Разработать и составить в виде блок-схемы алгоритмы шифрования и дешифрования текста на основе квадрата Полибия. 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

В [криптографии](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) **квадрат Полибия** ([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) *Polybius square*), также известный как шахматная доска Полибия — оригинальный [код](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%B4) простой замены, одна из древнейших систем кодирования, предложенная [Полибием](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D0%B8%D0%B1%D0%B8%D0%B9" \o "Полибий) ([греческий](https://ru.wikipedia.org/wiki/%D0%93%D1%80%D0%B5%D0%BA%D0%B8) историк, полководец, государственный деятель, III век до н. э.). Данный вид кодирования изначально применялся для греческого [алфавита](https://ru.wikipedia.org/wiki/%D0%90%D0%BB%D1%84%D0%B0%D0%B2%D0%B8%D1%82), но затем был распространен на другие языки.

Идею квадрата Полибия проиллюстрируем таблицей с русскими буквами. Число букв в русском алфавите отличается от числа букв в греческом алфавите, поэтому и размер таблицы выбран иным (не квадрат 5x5, а прямоугольник 8х4).



Зашифруем фразу: КРИПТОГРАФИЯ:

23 31 21 28 33 27 14 31 11 35 11 35 21 48.

В данном примере видно, что в шифрограмме первым указывается номер строки, а вторым – номер столбца.

Дешифровка заключается в получении из номера строки и столба нужного символа.

Практическое применение квадрата Полибия для кодирования сообщений можно видеть в ряде художественных фильмов, посвящённых заключённым под стражу, которые перестукиваниями обмениваются сообщениями между собой. Длинные интервалы могут использоваться для обозначения номера строки в квадрате, а короткие – для обозначения номера столбца.

Несмотря на то, что квадрат изначально создавался для кодирования с его помощью можно успешно шифровать.

К каждому [языку](https://ru.wikipedia.org/wiki/%D0%AF%D0%B7%D1%8B%D0%BA) отдельно составляется [таблица](https://ru.wikipedia.org/wiki/%D0%A2%D0%B0%D0%B1%D0%BB%D0%B8%D1%86%D0%B0) шифрования с одинаковым (не обязательно) количеством пронумерованных [строк](https://ru.wikipedia.org/wiki/%D0%A1%D1%82%D1%80%D0%BE%D0%BA%D0%B0) и столбцов, параметры которой зависят от его мощности (количества [букв](https://ru.wikipedia.org/wiki/%D0%91%D1%83%D0%BA%D0%B2%D1%8B) в алфавите). Берутся два [целых числа](https://ru.wikipedia.org/wiki/%D0%A6%D0%B5%D0%BB%D0%BE%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%BE), [произведение](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B8%D0%B7%D0%B2%D0%B5%D0%B4%D0%B5%D0%BD%D0%B8%D0%B5) которых ближе всего к количеству букв в языке — получаем нужное число строк и столбцов. Затем вписываем в таблицу все буквы алфавита подряд — по одной на каждую клетку. При нехватке клеток можно вписать в одну две буквы (редко употребляющиеся или схожие по употреблению).

Латинский алфавит

В современном латинском алфавите 26 букв, следовательно, таблица должна состоять из 5 строк и 5 столбцов, так как 25=5\*5 наиболее близкое к 26 число. При этом буквы I, J не различаются (J [отождествляется](https://ru.wikipedia.org/wiki/%D0%A2%D0%BE%D0%B6%D0%B4%D0%B5%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D0%BE%D1%81%D1%82%D1%8C) с буквой I), так как не хватает 1 ячейки:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **1** | **2** | **3** | **4** | **5** |
| 1 | A | B | C | D | E |
| 2 | F | G | H | I/J | K |
| 3 | L | M | N | O | P |
| 4 | Q | R | S | T | U |
| 5 | V | W | X | Y | Z |

## Русский алфавит

Идею формирования таблицы шифрования проиллюстрируем для [русского языка](https://ru.wikipedia.org/wiki/%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA). Число букв в русском алфавите отличается от числа букв в греческом алфавите, поэтому размер таблицы выбран другой (квадрат 6\*6=36, поскольку 36 наиболее близкое число к 33):

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **1** | **2** | **3** | **4** | **5** | **6** |
| 1 | А | Б | В | Г | Д | Е |
| 2 | Ё | Ж | З | И | Й | К |
| 3 | Л | М | Н | О | П | Р |
| 4 | С | Т | У | Ф | Х | Ц |
| 5 | Ч | Ш | Щ | Ъ | Ы | Ь |
| 6 | Э | Ю | Я | - | - | - |

Возможен также другой вариант составления, предусматривающий объединение букв Е и Ё, И и Й, Ъ и Ь. В данном случае получаем следующий [результат](https://ru.wikipedia.org/wiki/%D0%A0%D0%B5%D0%B7%D1%83%D0%BB%D1%8C%D1%82%D0%B0%D1%82):

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **1** | **2** | **3** | **4** | **5** | **6** |
| 1 | А | Б | В | Г | Д | Е/Ё |
| 2 | Ж | З | И/Й | К | Л | М |
| 3 | Н | О | П | Р | С | Т |
| 4 | У | Ф | Х | Ц | Ч | Ш |
| 5 | Щ | Ы | Ь/Ъ | Э | Ю | Я |

Существует несколько методов шифрования с помощью квадрата Полибия. Ниже приведены три из них.

## Метод 1

Зашифруем слово «SOMETEXT»:

Для шифрования на квадрате находили букву текста и вставляли в шифровку нижнюю от неё в том же столбце. Если буква была в нижней строке, то брали верхнюю из того же столбца.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Таблица координат** | | | | | | | | |
| **Буква текста:** | **S** | **O** | **M** | **E** | **T** | **E** | **X** | **T** |
| **Буква шифротекста :** | **X** | **T** | **R** | **K** | **Y** | **K** | **C** | **Y** |

Таким образом после шифрования получаем:

|  |  |
| --- | --- |
| **Результат** | |
| **До шифрования:** | **SOMETEXT** |
| **После шифрования:** | **XTRKYKCY** |

## Метод 2

Сообщение преобразуется в координаты по квадрату Полибия, координаты записываются вертикально:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Таблица координат** | | | | | | | | |
| **Буква:** | **S** | **O** | **M** | **E** | **T** | **E** | **X** | **T** |
| **Координата горизонтальная:** | **3** | **4** | **2** | **5** | **4** | **5** | **3** | **4** |
| **Координата вертикальная:** | **4** | **3** | **3** | **1** | **4** | **1** | **5** | **4** |

Затем координаты считывают по строкам:

34 25 45 34 43 31 41 54 (\*)

Далее координаты преобразуются в буквы по этому же квадрату:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Таблица координат** | | | | | | | | |
| **Координата горизонтальная:** | **3** | **2** | **4** | **3** | **4** | **3** | **4** | **5** |
| **Координата вертикальная:** | **4** | **5** | **5** | **4** | **3** | **1** | **1** | **4** |
| **Буква:** | **S** | **W** | **Y** | **S** | **O** | **C** | **D** | **U** |

Таким образом после шифрования получаем:

|  |  |
| --- | --- |
| **Результат** | |
| **До шифрования:** | **SOMETEXT** |
| **После шифрования:** | **SWYSOCDU** |

## Метод 3

Усложненный вариант, который заключается в следующем: полученный первичный шифротекст (\*) шифруется вторично. При этом он выписывается без[разбиения](https://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D0%B7%D0%B1%D0%B8%D0%B5%D0%BD%D0%B8%D0%B5) на пары:

3425453443314154

Полученная последовательность цифр сдвигается [циклически](https://ru.wikipedia.org/wiki/%D0%A6%D0%B8%D0%BA%D0%BB) влево на один шаг(нечетное количество шагов):

4254534433141543

Эта последовательность вновь разбивается в [группы](https://ru.wikipedia.org/wiki/%D0%93%D1%80%D1%83%D0%BF%D0%BF%D0%B0) по два:

42 54 53 44 33 14 15 43

и по таблице заменяется на окончательный шифротекст:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Таблица координат** | | | | | | | | |
| **Координата горизонтальная:** | **4** | **5** | **5** | **4** | **3** | **1** | **1** | **4** |
| **Координата вертикальная:** | **2** | **4** | **3** | **4** | **3** | **4** | **5** | **3** |
| **Буква:** | **I** | **U** | **P** | **T** | **N** | **Q** | **V** | **O** |

Таким образом после шифрования получаем:

|  |  |
| --- | --- |
| **Результат** | |
| **До шифрования:** | **SOMETEXT** |
| **После шифрования:** | **IUPTNQVO** |

## Добавление ключа

На первый взгляд шифр кажется очень [нестойким](https://ru.wikipedia.org/wiki/%D0%A3%D1%81%D1%82%D0%BE%D0%B9%D1%87%D0%B8%D0%B2%D0%BE%D1%81%D1%82%D1%8C), но для его реальной оценки следует учитывать два [фактора](https://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%BA%D1%82%D0%BE%D1%80):

1. *возможность заполнить квадрат Полибия буквами произвольно, а не только строго по алфавиту;*
2. *возможность периодически заменять квадраты.*

Тогда [анализ](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7) предыдущих сообщений ничего не дает, так как к моменту раскрытия шифра он может быть заменен.

Буквы могут вписываться в таблицу в произвольном порядке — заполнение таблицы в этом случае и является [ключом](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D0%BA%D1%80%D0%B5%D1%82%D0%BD%D1%8B%D0%B9_%D0%BA%D0%BB%D1%8E%D1%87). Для латинского алфавита в первую клетку можно вписать одну из 25 букв, во вторую — одну из 24, в третью — одну из 23 и т. д. Получаем максимальное количество ключей для шифра на таблице латинского алфавита:

N = 25*24*23*...*2*1 = 25!

Соответственно для дешифрования сообщения потребуется не только знание алфавита, но и ключа, с помощью которого составлялась таблица шифрования. Но произвольный порядок букв тяжело запомнить, поэтому [пользователю](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C) шифра необходимо постоянно иметь при себе ключ — квадрат. Появляется опасность [тайного](https://ru.wikipedia.org/wiki/%D0%A2%D0%B0%D0%B9%D0%BD%D0%B0) ознакомления с ключом посторонних лиц. В качестве [компромиссного](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%80%D0%BE%D0%BC%D0%B8%D1%81%D1%81) решения был предложен ключ — [пароль](https://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D1%80%D0%BE%D0%BB%D1%8C). Пароль выписывается без повторов букв в квадрат; в оставшиеся клетки в алфавитном порядке выписываются буквы алфавита, отсутствующие в пароле.

### Пример

Зашифруем слово «SOMETEXT», используя ключ «DRAFT». Составим предварительно таблицу шифрования с данным ключом, записывая символы ключа по порядку в таблицу, после них остальной алфавит:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **1** | **2** | **3** | **4** | **5** |
| 1 | D | R | A | F | T |
| 2 | B | C | E | G | H |
| 3 | I | K | L | M | N |
| 4 | O | P | Q | S | U |
| 5 | V | W | X | Y | Z |

Преобразуем сообщение в координаты по квадрату Полибия:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Таблица координат** | | | | | | | | |
| **Буква:** | **S** | **O** | **M** | **E** | **T** | **E** | **X** | **T** |
| **Координата горизонтальная:** | **4** | **1** | **4** | **3** | **5** | **3** | **3** | **5** |
| **Координата вертикальная:** | **4** | **4** | **3** | **2** | **1** | **2** | **5** | **1** |

Считаем координаты по строкам:

41 43 53 35 44 32 12 51

Преобразуем координаты в буквы по этому же квадрату:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Таблица координат** | | | | | | | | |
| **Координата горизонтальная:** | **4** | **4** | **5** | **3** | **4** | **3** | **1** | **5** |
| **Координата вертикальная:** | **1** | **3** | **3** | **5** | **4** | **2** | **2** | **1** |
| **Буква:** | **F** | **M** | **N** | **X** | **S** | **E** | **B** | **T** |

Таким образом после шифрования получаем:

|  |  |
| --- | --- |
| **Результат** | |
| **До шифрования:** | **SOMETEXT** |
| **После шифрования:** | **FMNXSEBT** |

## Математическая модель

Математически шифрование квадратом *Полибия* может быть записано следующими формулами

Если

– взаимно-однозначное отображение символов алфивита в целочисленные координаты

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

То

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

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

Перестановка как правило выбирается достаточно простой, чтобы шифрование текста можно было производить вручную по квадрату *Полибия*, например, или или или

(при условии существования обратного преобразования)

# Блок-схемы алгоритмов шифрования и дешифрования

### Aлгоритм шифрования

Открытый текст

Закрытый текст

Ключ

T

### Aлгоритм расщифрования

Открытый текст

Закрытый текст

Ключ

T-1

# Листинг кода

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

## Класс PolybiusCryptography

using System;

using System.Text;

namespace Polybius

{

/// <summary>

/// Квадрат Полибия

/// </summary>

public class PolybiusCryptography : IStreamCryptography

{

/// <summary>

/// Алфавит

/// </summary>

private const string Alphabet = "абвгдеёжзийклмнопрстуфхцчшщъыьэюяАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ"

+ "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789"

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

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

// матрица трансформации координат

private static readonly int[][] DefaultMatrix =

{

new[] {0, 1, 0},

new[] {1, 0, 0}

};

#region

private readonly int[][] \_forwardMatrix = DefaultMatrix; // матрица трансформации координат

private readonly int[][] \_reverseMatrix = DefaultMatrix; // матрица трансформации координат

#endregion

private int \_additionalKey; // Значение дополнительного ключа

private int \_n; // Размер квадрата

private string[,] \_square; // заполение квадрата символами алфавита

#region

private int \_i; // Текущий номер такта шифрования

private int \_z; // Значение дополнительного регистра

#endregion

/// <summary>

/// Сброс счётчика тактов

/// </summary>

public void Restart()

{

\_i = 0;

\_z = \_additionalKey;

}

/// <summary>

/// Процедура шифрования блока текста

/// Увеличение счётчика тактов на длину блока текста

/// Пересчёт значения дополнительного регистра на каждом такте

/// </summary>

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

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

public string EncryptNext(string plainText)

{

if (\_square == null) throw new EmptyKeyException();

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

var chars = new string[plainText.Length];

int count = 0;

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

chars[count++] = (plainText[i] == '\\') ? "\\\\" : plainText[i].ToString();

var sb = new StringBuilder();

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

{

int row;

int col;

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

ForwardTransform(ref row, ref col);

sb.Append(\_square[row, col]);

\_i++;

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

}

return sb.ToString();

}

/// <summary>

/// Процедура расшифрования блока текста

/// Увеличение счётчика тактов на длину блока текста

/// Пересчёт значения дополнительного регистра на каждом такте

/// </summary>

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

/// <returns>Исходный текст</returns>

public string DecryptNext(string cipherText)

{

if (\_square == null) throw new EmptyKeyException();

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

var chars = new string[cipherText.Length];

int count = 0;

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

if (cipherText[i] == '\\')

if (cipherText[i + 1] == '\\' && i + 2 < cipherText.Length)

{

chars[count++] = cipherText.Substring(i, 2);

i += 2;

}

else if (i + 6 < cipherText.Length)

{

chars[count++] = cipherText.Substring(i, 6);

i += 6;

}

else throw new WrongCharException {Character = cipherText.Substring(i)};

else

chars[count++] = cipherText[i++].ToString();

var sb = new StringBuilder();

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

{

int row;

int col;

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

ReverseTransform(ref row, ref col);

sb.Append(\_square[row, col]);

\_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)

{

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

string tableText = keyText + Alphabet;

// Удаляем повторы символов в строке keyText + Alphabet

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

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

tableText = tableText.Remove(j, 1);

// Вычисляем размер квадрата

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

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

\_square = new string[n, n];

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

{

int row = i / n;

int col = i % n;

\_square[row, col] = (tableText[i] == '\\') ? "\\\\" : tableText[i].ToString();

}

// Заполняем оставшиеся ячейки спецсимволами

for (int i = tableText.Length; i < n\*n; i++)

{

int row = i/n;

int col = i%n;

\_square[row, col] = string.Format("\\{0:D5}", i);

}

\_n = n;

\_i = 0;

}

/// <summary>

/// Сброс ключа и сброс счётчика тактов

/// </summary>

public void ClearKey()

{

\_square = null;

\_additionalKey = 0;

\_n = 0;

\_i = 0;

\_z = 0;

}

/// <summary>

/// Нахождение номера строки и столбца в квадрате Полибия

/// (включая поиск дополнительных спецсимволов)

/// </summary>

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

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

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

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

{

for (int i = 0; i < \_n; i++)

for (int j = 0; j < \_n; j++)

if (string.Compare(\_square[i, j], ch) == 0)

{

row = i;

col = j;

return;

}

throw new WrongCharException {Character = ch};

}

/// <summary>

/// Ввод дополнительного ключа и сброс счётчика тактов

/// </summary>

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

public void SetAdditionalKey(int additionalKey)

{

\_z = \_additionalKey = additionalKey;

\_i = 0;

}

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

{

int dx = (\_z/\_n)%\_n; // модификация определяемая дополнительным ключём

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

int i = (\_forwardMatrix[0][0]\*row + \_forwardMatrix[0][1]\*col + \_forwardMatrix[0][2] + dx)%\_n;

int j = (\_forwardMatrix[1][0]\*row + \_forwardMatrix[1][1]\*col + \_forwardMatrix[1][2] + dy)%\_n;

row = i;

col = j;

}

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

{

int dx = (\_z/\_n)%\_n; // модификация определяемая дополнительным ключём

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

int i = (\_reverseMatrix[0][0]\*(row + \_n - dx) + \_reverseMatrix[0][1]\*(col + \_n - dy) + \_reverseMatrix[0][2])%

\_n;

int j = (\_reverseMatrix[1][0]\*(row + \_n - dx) + \_reverseMatrix[1][1]\*(col + \_n - dy) + \_reverseMatrix[1][2])%

\_n;

row = i;

col = j;

}

public class EmptyKeyException : Exception

{

}

public class WrongCharException : Exception

{

public string Character { get; set; }

}

}

}

## Юнит-тест

[TestMethod]

public void TestMethod1()

{

try

{

Console.WriteLine(@"Квадрат Полибия");

Console.WriteLine();

PolybiusCryptography cryptography = new PolybiusCryptography();

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 PolybiusForm

using System;

using System.Windows.Forms;

namespace Polybius

{

public partial class PolybiusForm : Form

{

public PolybiusForm()

{

InitializeComponent();

}

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

{

try

{

PolybiusCryptography cryptography = new PolybiusCryptography();

cryptography.SetKey(encryptKey.Text);

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

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

}

catch (PolybiusCryptography.WrongCharException exception)

{

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

}

catch (PolybiusCryptography.EmptyKeyException)

{

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

}

}

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

{

try

{

PolybiusCryptography cryptography = new PolybiusCryptography();

cryptography.SetKey(decryptKey.Text);

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

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

}

catch (PolybiusCryptography.WrongCharException exception)

{

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

}

catch (PolybiusCryptography.EmptyKeyException)

{

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

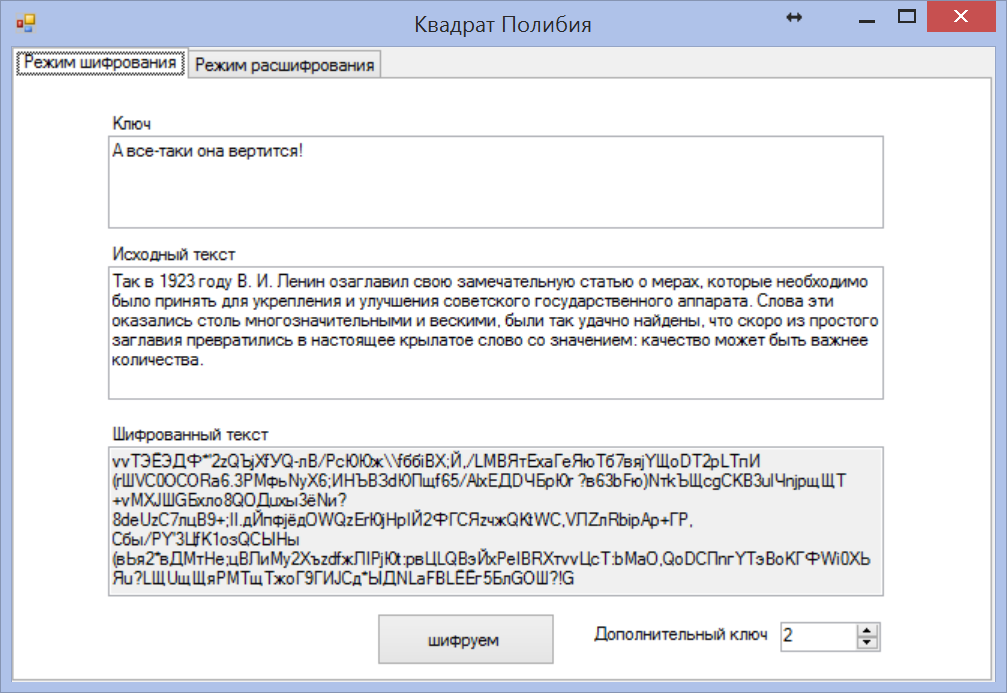
}

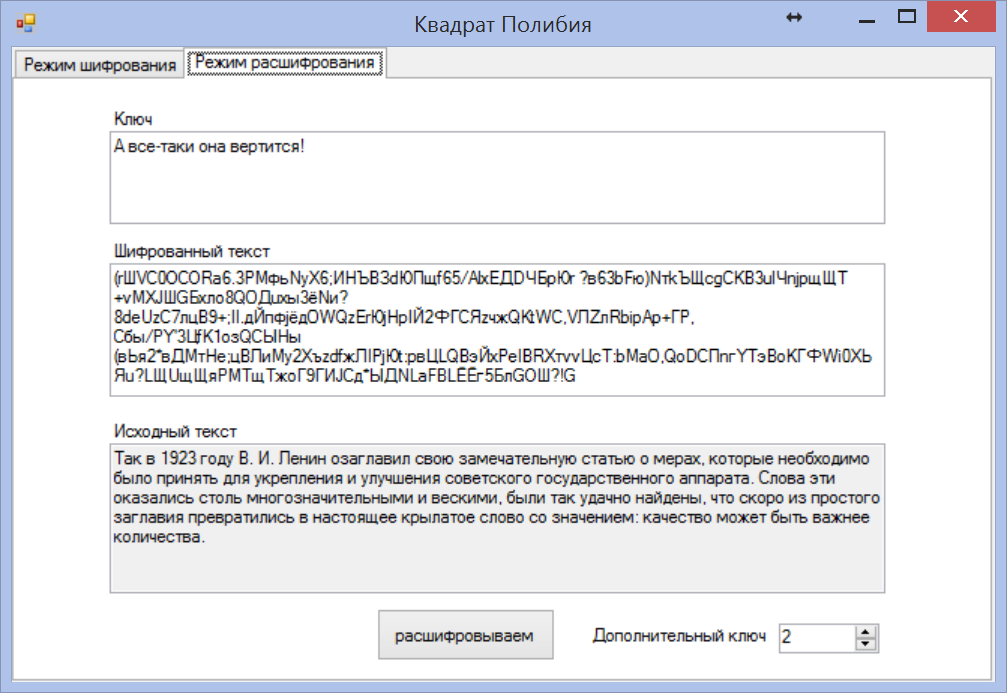
}

}

}

## Графический интерфейс





# Контрольные примеры работы программы

## Квадрат Полибия

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: tpBрпрь9ЙХрМZШ!рхэрQэреЛ:N:рZCpМ0pпN0рюпZсрCp,ЛЩpdЛ01:!срюdpd1срZр,Л pВмрBZdZ PЛр:ЛZБВZШN,ZрБP0Zрв N:яd1рШ0яр!B Лв0Л:NярNр!0!ЩfЛ:NярюZпЛdюBZМZрМZю!Шp юdпЛ::ZМZрpввp pdpэрh0Zпpр.dNрZBpCp0Nю1рюdZ01р,:ZМZC:pЩNdЛ01:P,NрNрпЛюBN,NмрБP0NрdpBр!ШpЩ:Zр:pOШЛ:PмрЩdZрюBZ ZрNCрв ZюdZМZрCpМ0pпNярв Лп pdN0Nю1рпр:pюdZяrЛЛрB P0pdZЛрю0ZпZрюZрC:pЩЛ:NЛ,нрBpЩЛюdпZр,ZqЛdрБPd1рпpq:ЛЛрBZ0NЩЛюdпpэ

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: бfP1ьP!НЩПfаБсьPьуаакrПfаg!р.ПfВЩ2PfшьrН.БP"fhБPВЩfrПfh2gНЩfhgьgЪPОс2rарfшPНgЪg2рНPfНсfЪP!спНrПfьсВPБсП:fRБуfНgЪg23fvgЪPьfкP2gБfЪьPОс"fGОсНfБсаксgБfОPЪу"fа2gЪу3tу3fqfНсPВPьPБяfЭскfEgfшPPhgьgЪНPf!P2P2rf!укуfНсfЪP!спНg!fEgьНPОg:fPhgНрfНg2g1кс.fьсВPБсяfтP2БуНс!fEg"fPБ2ЩНrОсОпr!fPБfОа.кP1PfБьуЪс"f1PОPьr2rfаfНса!gпкPQ:f,(g2r"fР!g2."fБОP.fНgЪg2.м,fqfr1ьс.fНсfБP!"fhБPfОЩьсEgНrgf,.DЩкP!f!P2PБр,fкP!rhgакrfаPшPаБсО2.2PарfБуБfr!gННPfаfшьgЪаБсО2gНrg!fPfас!PQfБ.Eg2PQfьсВPБgfНсfEgьНPОgя

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: дtPбgОБDОrR.1"r.бЩrНЩбфб.F"rцбPНЩ1х1r2P1DНг1gВОБDfтr?в.1P1QrОх1rаtErцбPFrGвбБrbo"r2P1фвбББtsrвrБбP1ВОrчP1фБtQrфбrQбНН1вtОrЩбфБDrDr!аDsН.вбтrДEfr!НDEОБDfrНв1ОsrНбQ1ВОPgбвБ1srвEбН.D"rГ.1rБОв1фQ1gБ1rаtE1rаОфr1НEбаEОБDfrЩБfфОs"rа1fPrDrВ!г1вОБН.вб"rGвбБrчP1фБtsrввОEr12PDГБDБ!"rБбв1ВDвП!3r!gбНrБбrвНОrх1Н!ВбPН.в1rЕ1ННDsНЩ1ОтсОrQ1хr2PDQDPD.FНfrНrPбфх!E1Qr12PDГБDЩ1вrDrQD.P121ED.r(1НЩ1вНЩDsrvDED22т

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: )т1ШQт1Шf.ШсEч.ЩМqrМяШДчrШрМeШтлтШчМАМт1яШхP.fEс.Мтв?OШQт1Шв1Pч.gМqrМШвт.чrqq1DШчлввP1DШ!1Б1с1чPrOШP1т1ч.?ШБу.вrу."Ш:рл0Мв.ШсШчМАМтМШpШ0EчШeq1Б1OШ.ШсEвP1рrтCШqМPл0.:аШП1Шq.вШ01Ау.Шт1уCP1Ш!Мчс.?Шр.втCШВч.fEOШP1т1ч.?ШP.PШбEШс1бч.у.ШсШвМб?ШвeEвуШсвМБ1ШсEвP.fEс.qr?а

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

Тест #: 4

Ключ: 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: хЛу1БЪБ!АPsЛтЛ1тQ!АPsЛQтфPEPуттЛ5Б1щБ1ЛqЛЪгDPвтбr.sЛи1БВуEfв.sЛ2Б!Л!PЛgQБтr.QЛВвP!иPQ"ЛPВ1fr?вhтsЛвВPDЛвЛ2PDgБQrPБЛНf1!ивPЛктDf"ЛАPиP1.sЛщ.EЛгА1PбБrЛГБ1fАEPQыЛДи!3DfЛ!EPвPЛ,НБ1щБ1,Лг2Pи1БщE?Би!?ЛвЛgrfЪБrтт:ЛgEPs"Л!вт1Б2.sЛrfD!QPи1бтАы

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: pЁЭmuПРCД,r,бПn,nuъП ЬЁмCnCбПСЁP,n,ДПЮП?Д,мСuП,ПСCЬCmuДПДЯmoмПЁЭЁъЖПйЁЭЁРиПЁnC1ПйЁЭЁРПЗCРЮПЮnЬuуъЁПСЁruЬuДПЮмCДЖ.uruиПъЁПйыДЁПСЁkmъЁчП?йДumuoПйЁ0CЮnРCъъымПСДuмCъCмиПДЯm,ПСCЬCЮnuД,ПСЁm.,ъonЖЮoПъCйЁ0,nCДoмиПъuш.,Д,ЮЖПЬukъымПъuшruмиПРыуД,П,kПЮРЁCЭЁП0uДrЁЭЁПЮЁЮnЁoъ,oчП)sCПъCмъЁЭЁПjП,ПЁъ,ПkuРЁCРuД,ПйыПЮCйCПСЁДъЁCПЮ.uЮnЖCччч

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: ПZрШ Лп:ЛМ ЛЩЛюBZ,!р,Nф!мрuвNdЛ !рЦМ ЛЩэрEЛпюcрв NМ0я:!0pю1рШZЩ1рфN:NBNOюBZМZрНp ярЪп ZвpэрuвNdЛ рв Лп pdN0юярпрБPBpрNрвZВNdN0рЛЛэрИЮ+трHЭ)ёТрJ+kЭмр5+5рHЭ)ёТр4+kЭрЧрвZю0ZпNНpрМZпZ NdрZр:ЛюB Z,:ZOрN0NрБЛCZю:ZпpdЛ01:ZOрв ЛdЛ:CNNэ

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: ЭскfОfгNлюf1PЪуfбяfGяf4gНrНfPDс12сОr2fаОP3fDс!ghсБg2рНу3fаБсБр3fPf!gьсП"fкPБPьЩgfНgPВПPЪr!PfВЩ2PfшьrН.БрfЪ2.fукьgш2gНr.frfу2уhпgНr.fаPОgБакP1Pf1PауЪсьаБОgННP1PfсшшсьсБсяfС2PОсfRБrfPксDс2rарfаБP2рf!НP1PDНсhrБg2рНЩ!rfrfОgакr!r"fВЩ2rfБскfуЪсhНPfНсQЪgНЩ"fhБPfакPьPfrDfшьPаБP1PfDс12сОr.fшьgОьсБr2rарfОfНсаБP.tggfкьЩ2сБPgfа2PОPfаPfDНсhgНrg!:fксhgаБОPf!PEgБfВЩБрfОсEНggfкP2rhgаБОся

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: дr1хP1QБtгrН.бP1P!ННЩDгrНОQFfгrаtE1r2PDБf.1"rГ.1аtrDгrГEОБtrГОPОВ1вбEDНFr21БОВОEFБ1rБбrВ1QбПБDгrPба1.бг:rR.!rБОВОE3rvОВ1PrЩ1EО.rВP1вб"rGвбБr.бНЩбО.rв1В!"rНEОВ!3Ы!3rqrБб1а1P1.тrЭбЩrgОr211ГОPОВБ1rQ1E1EDrQ!Щ!rБбrВ1QбПБОQrgОPБ1вО:r1ГОБFrБОEОхЩбfrPба1.бтrн1E.!БбQrgО"r1.EtБDвбвПDQr1.rвНfЩ1х1r.P!Вб"rх1в1PDEDrНrБбНQОПЩ1s:r,(ОED"rРQОEf"r.в1frБОВОEfу,rqrDхPбfrБбr.1Q"rГ.1rвtPбgОБDОr,fфtЩ1QrQ1E1.F,rЩ1QDГОНЩDrН121Н.бвEfE1НFr.!.rDQОББ1rНr2PОВН.бвEОБDОQr1rНбQ1sr.fgОE1srPба1.ОrБбrgОPБ1вОт

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: фEч.ЩМqrМШQт1OШт.PШвP.f.тCOШЪ.чвP1Б1Ш!ч1rвО1Щ0Мqr?аШшст1ч1eШМБ1ШбEуШЪ.чCШRс.qШmzOШ!ч1fс.qqEDШсШq.ч10МШГч1fqEeШf.Шe.вв1сEМШP.fqrШrШлбrDвтс.аШПу?ШлвrуМqr?Швс1МDШв.e10МчЩ.сq1DШсу.втrOШрт1ШqМс1fe1Щq1ШбEу1ШбМfШ1ву.буМqr?ШPq?fМDOШб1?чШrШ0лО1сМqвтс.OШRс.qШГч1fqEDШссМуШ1!чrрqrqлOШq.с10rсАл2ШлЩ.вШq.ШсвМШБ1вл0.чвтс1ШР1ввrDвP1МаёМШe1БШ!чrerчrтCв?ШвШч.fБлу1eШ1!чrрqrP1сШrШerтч1!1уrтШе1вP1свPrDШGrуr!!а

Расшифрованный текст: Выражение это, так сказать, царского происхождения. Автором его был царь Иван IV, прозванный в народе Грозным за массовые казни и убийства. Для усиления своей самодержавной власти, что невозможно было без ослабления князей, бояр и духовенства, Иван Грозный ввел опричнину, наводившую ужас на все государство Российское.Не мог примириться с разгулом опричников и митрополит Московский Филипп.

Тест #: 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: )иPЛRиPЛgfЛв.1fЩБrтБяЛШ1тЛЪБQЛигиЛ1БhБиPяЛДАfg.вfБи!?"ЛRиPЛ!PА1fбБrтБЛ!иf1тrrPsЛ1г!!АPsЛ2PуPвP1Ат"ЛАPиP1f?ЛуEf!тEf:Л,ЪгDБ!fЛвЛ1БhБиБЛqЛD.1ЛQrPуP"ЛfЛв.!АPЪтиFЛrБАгDf,ыЛОPЛrf!ЛDPhEfЛиPEFАPЛ2Б1вf?ЛЪf!иFЛф1fg."ЛАPиP1f?ЛАfАЛщ.ЛвPщ1fEfЛвЛ!Бщ?Л!Q.!EЛв!БуPЛв.!Аfg.вfrт?ы

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: 2ПЭЬC.CЮrЁбП,ПЬ,мЮrЁбПм,DЁДЁЭ,,ПdCЬйCЬПjП.шmЁР,sъыбПnЬCPЭДuРыбПСCЮПЮЁПkмC,ъымПPРЁЮnЁмиПЁPЬuъoРу,бПРPЁmПРПСЁmkCмъЁCП1uЬЮnРЁПE,muиПrЁnЁЬыбПйыДПшrЬЁsCъП!CЬurДЁмчП?nЮЯmuПЮДЁРЁП;1CЬйCЬ;ПшСЁnЬCйДoCnЮoПРПkъu.Cъ,,bПkДЁбиПЮР,ЬCСыбПъumЮмЁnЬs,rч

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: ?ZМШpрпЛ0NBNOрdNdp:рП Z,ЛdЛOрвZВNdN0рюрД0N,вpрNрвЛ ЛШp0р0сШя,рZМZ:1рБZМZпмрZdЛНрБZМZпрEЛпюрюd pf:ZрвZBp p0рю,Л01ЩpBpмр:ZрБP0ZрвZCШ:ZэрДБ0pШpярБZqЛюdпЛ::P,рв0p,Л:Л,мр0сШNрвЛ Люdp0NрвZШЩN:яd1юяр:ЛБZqNdЛ0я,мр:p!ЩN0Nю1р pC:P,р:p!Bp,мрпPf0NрNCрюпZЛМZрqp0BZМZрюZюdZя:NяэрЪrЛр:Л,:ZМZрЧрNрZ:NрCpпZЛпp0NрБPрюЛБЛрвZ0:ZЛрюЩpюd1Лэээ

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: хPfЪьgОНg1ьghgакP!уf!rГу"fЮшrБgьуfМ1ьghяfugОаШfшьr12.Ну2сарfЪPhрfГrНrкrQакP1PfЫсь.fРОьPшсяfЮшrБgьfшьgОьсБr2а.fОfВЩксfrfшPПrБr2fggяfйЗV6flЖU+щfnVФЖ"fJVJflЖU+щfIVФЖfqfшPа2PОrЫсf1PОPьrБfPfНgакьP!НPQfr2rfВgDPаНPОсБg2рНPQfшьgБgНDrrя

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: ЭбЩrвrоNпюrх1В!rдтrGтr4ОБDБr1фбхEбвDErНв13rфбQОГб.ОEFБ!3rН.б.F3r1rQОPбг"rЩ1.1PtОrБО1аг1ВDQ1rаtE1r2PDБf.FrВEfr!ЩPО2EОБDfrDr!E!ГПОБDfrН1вО.НЩ1х1rх1Н!ВбPН.вОББ1х1rб22бPб.бтrСE1вбrR.Dr1ЩбфбEDНFrН.1EFrQБ1х1фБбГD.ОEFБtQDrDrвОНЩDQD"rаtEDr.бЩr!ВбГБ1rБбsВОБt"rГ.1rНЩ1P1rDфr2P1Н.1х1rфбхEбвDfr2PОвPб.DEDНFrвrБбН.1fЫООrЩPtEб.1ОrНE1в1rН1rфБбГОБDОQ:rЩбГОН.в1rQ1gО.rаt.FrвбgБООrЩ1EDГОН.вбт

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: фШ1Бч1eqEОШвт.ч1члввPrОШвМeC?ОШбEу1Ш!чrq?т1OШрт1бEШrОШруМqEШрМчМ01с.уrвCШ!1qМ0МуCq1Шq.Ш01e.АqrОШч.б1т.О"ШQтлШqМ0Му2ШGМ01чШP1уМтШ0ч1с.OШRс.qШт.вP.МтШс10лOШвуМ0л2gл2ШpШq.1б1ч1таШi.PШЩМШ!11рМчМ0q1Шe1у1уrШeлPлШq.Ш01e.АqМeШЩМчq1сМ"Ш1рМqCШqМуМБP.?Шч.б1т.аШг1утлq.eШЩМOШ1туEqrс.сАreШ1тШсв?P1Б1Штчл0.OШБ1с1чrуrШвШq.вeМАP1D"Ш:еМуrOШЫeМу?OШтс1?ШqМ0Му?п:ШpШrБч.?Шq.Шт1eOШрт1ШсEч.ЩМqrМШ:?fEP1eШe1у1тC:ШP1erрМвPrШв1!1вт.су?у1вCШтлтШreМqq1ШвШ!чМ0вт.суМqrМeШ1Шв.e1DШт?ЩМу1DШч.б1тМШq.ШЩМчq1сМа

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: х.1fЩБrтБЛRиP"ЛиfАЛ!АfgfиF"ЛНf1!АPуPЛ21Pт!ВPЩDБrт?ыЛквиP1PQЛБуPЛщ.EЛНf1FЛSвfrЛbo"Л21Pgвfrr.sЛвЛrf1PDБЛГ1Pgr.QЛgfЛQf!!Pв.БЛАfgrтЛтЛгщтs!ивfыЛОE?Лг!тEБrт?Л!вPБsЛ!fQPDБ1ЩfвrPsЛвEf!ит"ЛЪиPЛrБвPgQPЩrPЛщ.EPЛщБgЛP!EfщEБrт?ЛАr?gБs"ЛщP?1ЛтЛDгВPвБr!ивf"ЛSвfrЛГ1Pgr.sЛввБEЛP21тЪrтrг"ЛrfвPDтвhг3ЛгЩf!ЛrfЛв!БЛуP!гDf1!ивPЛРP!!тs!АPБыцБЛQPуЛ21тQт1тиF!?Л!Л1fgугEPQЛP21тЪrтАPвЛтЛQти1P2PEтиЛёP!АPв!АтsЛHтEт22ы

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: qnЁПУnЁПkuПРыЬu0Cъ,CОП Ь,П.CмПnшnПЬCуCnЁОП?rukыРuCnЮoиПУnЁПЮЁrЬusCъ,CПЮnuЬ,ъъЁбПЬшЮЮrЁбПСЁЭЁРЁЬr,иПrЁnЁЬuoПЭДuЮ,ДubП;.шmCЮuПРПЬCуCnCПjПmыЬПмъЁЭЁиПuПРыЮrЁ.,nЖПъCrшmu;чПлЁПъuЮПmЁуДuПnЁДЖrЁПСCЬРuoП.uЮnЖПDЬukыиПrЁnЁЬuoПrurПйыПРЁйЬuДuПРПЮCйoПЮмыЮДПРЮCЭЁПРыЮrukыРuъ,oч

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: хрМ ЛЩЛюBZOрNр N,юBZOр,NфZ0ZМNNр(Л БЛ рЧрЩ!ШZпNr:POрd ЛВМ0pпPOрвЛюрюZрC,ЛN:P,рВпZюdZ,мрZВ p:япfNOрпВZШрпрвZШCЛ,:ZЛрНp юdпZрАNШpмрBZdZ POрБP0р!B ZrЛ:рГЛ pB0Z,эрДdюсШpрю0ZпZр;НЛ БЛ ;р!вZd ЛБ0яЛdюярпрC:pЩЛ:NNнрC0ZOмрюпN ЛвPOр:pШю,Zd rNBэ

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: КP1ЪсfОg2rкrQfБrБсНfхьP!gБgQfшPПrБr2fаfв2r!шсfrfшgьgЪс2f23Ъ.!fP1PНрfВP1PО"fPБgЫfВP1PОfugОаfаБьспНPfшPксьс2fа!g2рhскс"fНPfВЩ2PfшPDЪНPяfвВ2сЪс.fВPEgаБОgННЩ!fш2с!gНg!"f23ЪrfшgьgаБс2rfшPЪhrН.Бра.fНgВPErБg2.!"fНсуhr2rарfьсDНЩ!fНсукс!"fОЩп2rfrDfаОPg1PfEс2кP1PfаPаБP.Нr.яfРtgfНg!НP1PfqfrfPНrfDсОPgОс2rfВЩfаgВgfшP2НPgfаhсаБрgяяя

Расшифрованный текст: Когда великий титан Прометей похитил с Олимпа и передал людям огонь богов, отец богов Зевс страшно покарал смельчака, но было поздно. Обладая божественным пламенем, люди перестали подчиняться небожителям, научились разным наукам, вышли из своего жалкого состояния. Еще немного - и они завоевали бы себе полное счастье...

# Модификация алгоритма

Математически шифрование квадратом *Полибия* может быть записано следующими формулами

Если

– взаимно-однозначное отображение символов алфивита в целочисленные координаты

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

То

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

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

То есть, если

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

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

То

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

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

## Доказательство повышения криптографической стойкости

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

# Блок-схемы модифицированных алгоритмов шифрования и дешифрования

### Модифицированный алгоритм шифрования

Открытый текст

Закрытый текст

Дополнительный ключ

Ключ

Генератор перестановок Ti

Ti

### Модифицированный алгоритм расшифровании

Открытый текст

Закрытый текст

Дополнительный ключ

Ключ

Генератор перестановок Ti

Ti-1

# Листинг программы, реализующий модифицированные алгоритмы

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

## Класс PolybiusCryptography

using System;

using System.Text;

namespace Polybius

{

/// <summary>

/// Квадрат Полибия

/// </summary>

public class PolybiusCryptography : IStreamCryptography

{

/// <summary>

/// Алфавит

/// </summary>

private const string Alphabet = "абвгдеёжзийклмнопрстуфхцчшщъыьэюяАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ"

+ "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789"

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

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

// матрица трансформации координат

private static readonly int[][] DefaultMatrix =

{

new[] {0, 1, 0},

new[] {1, 0, 0}

};

#region

private readonly int[][] \_forwardMatrix = DefaultMatrix; // матрица трансформации координат

private readonly int[][] \_reverseMatrix = DefaultMatrix; // матрица трансформации координат

#endregion

private int \_additionalKey; // Значение дополнительного ключа

private int \_n; // Размер квадрата

private string[,] \_square; // заполение квадрата символами алфавита

#region

private int \_i; // Текущий номер такта шифрования

private int \_z; // Значение дополнительного регистра

#endregion

/// <summary>

/// Сброс счётчика тактов

/// </summary>

public void Restart()

{

\_i = 0;

\_z = \_additionalKey;

}

/// <summary>

/// Процедура шифрования блока текста

/// Увеличение счётчика тактов на длину блока текста

/// Пересчёт значения дополнительного регистра на каждом такте

/// </summary>

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

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

public string EncryptNext(string plainText)

{

if (\_square == null) throw new EmptyKeyException();

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

var chars = new string[plainText.Length];

int count = 0;

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

chars[count++] = (plainText[i] == '\\') ? "\\\\" : plainText[i].ToString();

var sb = new StringBuilder();

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

{

int row;

int col;

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

ForwardTransform(ref row, ref col);

sb.Append(\_square[row, col]);

\_i++;

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

}

return sb.ToString();

}

/// <summary>

/// Процедура расшифрования блока текста

/// Увеличение счётчика тактов на длину блока текста

/// Пересчёт значения дополнительного регистра на каждом такте

/// </summary>

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

/// <returns>Исходный текст</returns>

public string DecryptNext(string cipherText)

{

if (\_square == null) throw new EmptyKeyException();

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

var chars = new string[cipherText.Length];

int count = 0;

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

if (cipherText[i] == '\\')

if (cipherText[i + 1] == '\\' && i + 2 < cipherText.Length)

{

chars[count++] = cipherText.Substring(i, 2);

i += 2;

}

else if (i + 6 < cipherText.Length)

{

chars[count++] = cipherText.Substring(i, 6);

i += 6;

}

else throw new WrongCharException {Character = cipherText.Substring(i)};

else

chars[count++] = cipherText[i++].ToString();

var sb = new StringBuilder();

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

{

int row;

int col;

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

ReverseTransform(ref row, ref col);

sb.Append(\_square[row, col]);

\_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)

{

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

string tableText = keyText + Alphabet;

// Удаляем повторы символов в строке keyText + Alphabet

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

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

tableText = tableText.Remove(j, 1);

// Вычисляем размер квадрата

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

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

\_square = new string[n, n];

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

{

int row = i / n;

int col = i % n;

\_square[row, col] = (tableText[i] == '\\') ? "\\\\" : tableText[i].ToString();

}

// Заполняем оставшиеся ячейки спецсимволами

for (int i = tableText.Length; i < n\*n; i++)

{

int row = i/n;

int col = i%n;

\_square[row, col] = string.Format("\\{0:D5}", i);

}

\_n = n;

\_i = 0;

}

/// <summary>

/// Сброс ключа и сброс счётчика тактов

/// </summary>

public void ClearKey()

{

\_square = null;

\_additionalKey = 0;

\_n = 0;

\_i = 0;

\_z = 0;

}

/// <summary>

/// Нахождение номера строки и столбца в квадрате Полибия

/// (включая поиск дополнительных спецсимволов)

/// </summary>

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

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

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

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

{

for (int i = 0; i < \_n; i++)

for (int j = 0; j < \_n; j++)

if (string.Compare(\_square[i, j], ch) == 0)

{

row = i;

col = j;

return;

}

throw new WrongCharException {Character = ch};

}

/// <summary>

/// Ввод дополнительного ключа и сброс счётчика тактов

/// </summary>

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

public void SetAdditionalKey(int additionalKey)

{

\_z = \_additionalKey = additionalKey;

\_i = 0;

}

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

{

int dx = (\_z/\_n)%\_n; // модификация определяемая дополнительным ключём

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

int i = (\_forwardMatrix[0][0]\*row + \_forwardMatrix[0][1]\*col + \_forwardMatrix[0][2] + dx)%\_n;

int j = (\_forwardMatrix[1][0]\*row + \_forwardMatrix[1][1]\*col + \_forwardMatrix[1][2] + dy)%\_n;

row = i;

col = j;

}

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

{

int dx = (\_z/\_n)%\_n; // модификация определяемая дополнительным ключём

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

int i = (\_reverseMatrix[0][0]\*(row + \_n - dx) + \_reverseMatrix[0][1]\*(col + \_n - dy) + \_reverseMatrix[0][2])%

\_n;

int j = (\_reverseMatrix[1][0]\*(row + \_n - dx) + \_reverseMatrix[1][1]\*(col + \_n - dy) + \_reverseMatrix[1][2])%

\_n;

row = i;

col = j;

}

public class EmptyKeyException : Exception

{

}

public class WrongCharException : Exception

{

public string Character { get; set; }

}

}

}

## Юнит-тест

[TestMethod]

public void TestMethod2()

{

try

{

Console.WriteLine(@"Квадрат Полибия (модификация)");

Console.WriteLine();

PolybiusCryptography cryptography = new PolybiusCryptography();

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

## Квадрат Полибия (модификация)

Тест #: 0

Ключ: А все-таки она вертится!

Дополнительный ключ: 84

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: цЛ:Zu0;0dг3нЫAшXUцхЕ9fЙЦНЫчзАoЁpъ.ш5щЦыЗюЯ0йХdИРr(4ЫиPxPmEW,,дN,lz-BЦT +жвДьэЪкtдсyQоGН\*СUA\*9GzC "Кгч(иiйввWюrnдоvCZЧЬr , ГПAЙфLКфdPcPмI1ЁцЧcFBЁясWQеMЭёЫnеzэn,OsнХлZfЁмЁDЙщПлMPяы?1КйсхКЯ1(юjvvЦQтBнoщEнs;P/R"цYV'цЛыgиъSqъSЗTО7g/ИEcf'ЮIwйnсM2yJ-?ъсhdZi3P9тHhGМKчqCЫrlw;DцЙ:вYбДvFйкuF!ЭМLR0рХ3СlоЗ3G7ЛьЦф5uфрSxLu:):G0lлЭЮгАLTRuxjJХЁ:оЦfpъу?ФГ2щrAfёашд:zjw75яВ;вАФукюпiНЯ:эТ!ПnЙ

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: 44

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: ШЩfс3ЧЁZЕБCGHЩЗРЙ0Пнn\\(EjДщпПzУЁIь!ъФц;bkИдашЯdCфvЁ(Y;IXXэбRЪdЬjGOLэcIRЭKоьqюvгjz?lяоEE)KZрЬП0ЕeятbЦХIЧХчЖюжTпчMxti!8LгкiрhъЯowXOз0/ФКVFp/КI4;AаюТ1BцkуЮK(LфDлSwЙj90EЭпUВ\\.Wзп0+.Pe,:ЦпН-q'ПwДKчУT-з-Иgr:kщхezPk4GlIЩpO(щq:tТПх7ЙzмёолEхoiДёfоTйбофРbЦХ:4сSК'в\*GmLьrdМLwВоЁОuuяiJчцk4R \*ЁлWящЗйфЙэp!,EРKЬЭФЬXFхeмЙъЪq6BDё:OтVюuБaPАfшуоrИ,8ЬЭКлHVЕДё'JLХoJч,М/UИPN5kXЖчw6hlягXastFз+шъяЩпЛ.cвaZЬИйzОMчwNКaСиыqАF+"L7fу7Kс;ToAкБI(L.17o:Аcк\\wpсKпd9КккCV-ыJ4YG/уw1аЮg9VГЙпШ5уkvшЭe5w(aptp+авъж

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: 41

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: ХЮЙSp?ЪХgбrсphЩЩrёвВsаОucpB"ghАзCRбы?8ЕЩZшFURсиtеющъъМсpур3ВСюьп1jaуЙFlиеsфReЙCМЦрЕГqWчTNJ/KунT1юШыufhг?УшNЯOlАhтюiAbЮПpЯлЁG\\GФйhМРЩmz8\*юiИiКЙw(Х?5ВeJЭ1"lKеУгИIsFuS8УfhUNeSМiТТчcnSчЕСф"5хsNЕЖzМJvёYзМ'Г 6PНЁ9OHАUEЮELBx7TКАЗЫТoIИpЭБN1дQрцvрхЬицЦГMыЯTфВъъЖx2SМifZhИКОЮх"ZqФiгpШ\*NSbЙсС\*УpЁsk9BЯеDlвYщсWЫыБK30Wлц0ШэL:qLMаXC+ИУвFаHПБЫ,9aм4FУZу\*FсЁвчzЛрщГИЧmЕЮwhCЦ/g1ZяkЧjUОoЧUЧjZAС.peоДyKлэmFёК2яW

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: 35

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: г:е\\ЭzЫщЛzуОц\\XgtsOВоХъэюmTФдзIдйG2 mЭ(gqFЧЦБ?ПsФ+юЯюдТPXйgФ0";qJ(ХэАo-Qд6ТН3AёиРКZFimшЮршцD6ОM!ЁьМfЁMfМКпЗ!Чз1д2ЫCIHUР5yъaлсYwСПzЙO52EwЮОY:чиАд1F?4Ic0МыJюhFbRвнп,t8т\\Ьёxэь0ДШreпSцjЗWВCYPкцшХT(ЫЪ:ДKЁGЖжЪнЗеAЯлnФB3кЯ;PEruzg5з)\\чHЦаоmg"ЭМаbzhv/JГfъгezВПЙЩЙ0ИГuCяЁД

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: 24

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: О1EЛQйoяv12d0K\\XEыJз1ИгхAН6NkB0ИWрEjкКYйЭхSGYДй\\b".o::6Ш8W7ъH!NЭЁэА7щg Lna8YЬW5Я?rAAABNРЖМкmэ"ЦПtОпB.тю.aЫlЬ2БQ"сG yQuzoлЖУpYXжяg/ЙLыYБYЦwпfоdШЛЭФТлЦtGК\\9s:Л/EЖыИъ/ШЕTЫЬТuгЙ IpweO-?щь;4Q ЙYНgRу8ФБ1ЧЁ ишЫйВИъпYт24х9"дI5д\*(T.fрАФнИ?TАIP

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: 4

Исходный текст: Когда великий титан Прометей похитил с Олимпа и передал людям огонь богов, отец богов Зевс страшно покарал смельчака, но было поздно. Обладая божественным пламенем, люди перестали подчиняться небожителям, научились разным наукам, вышли из своего жалкого состояния. Еще немного - и они завоевали бы себе полное счастье...

Шифрованный текст: xСOЕДйCY'sxfаyEМДeOёфtцйТх/);)ЭЫБ\*хzjМtТжК-uЫ1ДяьqdRsлИJХ5zTMАбHжD,ЙрЙ',VvЧ8ФДЩItУRhыЗоЙKСil\\з.\*rйГЗeDZ+УUт;i0Z2wнWСв?зslm?OуxПgpbгдЮЩшLФqМGЦм3СlРugGHИ\\ДXLЛОБaMms5чaюМДVъ/ПКВ2X+еeыМyЪуМТЧК;ЬWреярЙ,кfcr8(9яБхlzЫрз7nU1c:ЧьolЪNшяEМг\*ШqtЦG+.oЩG" LF))геGoa5Х.к\\ОEXуIDьk71D(PА:иНuИдQOpЭИoцчRaeU5AКиhp6h3ЛСРqлЩXI0S)И9ЙZФU2cnдиБ

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: 94

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: .T+аЕп4с1Е0-iyУbcЗэgь7rB-ПЬfЬVю+лz-ЮdЮYkюУЪ6Ф1r+тБи 'YYЩO/Л'ОYW'gFcНэНцЁБ79BВСъшАgСЩUЗж;ЯыFЬZ3ZLЛI;!s\\ydЬ tmыGсyНЪ7ЬяуlNFп;ТUхёAIH./tPеЁЬзгQ/к+-НШvKщТй!лгm+АхdШФ:;!ёБщФДkfц6х8RНгB;ЭYВСгА"шMxKtфеМьtYгп;FOрАРхЩo6DА\\fеМ-4QY\\у0ЫВcУ

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: 85

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: ы4ЧЬР)LоЗ2R0?ТщuZlmP1тwцЩюe\\sХBOpbJGnA3ГLRЮ!з2C/CуЩтдпFDчБэтГНqк!ЪьЫ6W;PЭеВрLшпмЯШN2?Sъ2ыЕщьиV\*МyYHT.Df!+уh(R/6Pдп+А)wтшМ?b1vчЮofdx0ХьФyxБг9БцВИprмСьll4nР7мэДо2gЁ0!ZBСЩЦJбLWGjюкF7TUхЦu;ЕьmWУPёЦT"О3Игхыi;SqрЪэаEюjCхНсК ш?ГgьбaХ!Zпш'?МтeoSе .:С.ышхъF5zJжj"vOЩ\\фЪiAзг2нlfФПxенBАhКYjПШ\\Юvп/хTN щJfбH!B'aРeF,Tиk"+КУ1hOэ)YйЯаЙ6з7РЙбиyСпRяХ/Тmюi0ЭZ9Яб\*i)ВCJЕsZЯWTУsЦIшЫДuЖaC)цe,i0Ъ

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: 13

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

Шифрованный текст: ш4AvрS/гlБeaK8мнЙзXпт3zvwtMW4ухTЙьc!рЩ64hуRгфы/щhёмQSuj6!КфOO\\6;ж2еmДCKссqЭЁAУг)HHфUи:АЬqХФЭ)+пп5ZыCWMюЬЬMYv3яKfiыsрфЯvгORуГ\*ыOГIб1вЁJщlB/ЛV)ТsчЦFлЮH3З cЙizzРыжГxРgГЗЦL+С;лКwfgНЧqрП5mNLfГO-\*БFМaЧхHгaАKnЛXeЖTDНgUз45'SЮо\*1c2XаЖ7PNУтЯJо,Лзo2ZЖjDЧЭeЖeыVФZэГ9яuП+ТГv.0oдzHl)МшxпбаНdтaлc(?У.ЙЪzёс/ymi"bШ'эИswЬЗ8ПTZw!Щ7ШЛъPM EE6gtWЖПгхШ4?йСбkИ,Т7ЕЙ.PРъ?,д)6иBCЙДФЫ+GОNk9пщ?Pбgl4cцИтщEёцжкwрPЪdтСоKYЪ?sюCЖЖeГУС0'YРWЬKxфRМCLNf;!вэQfКЁлщsрZ+ЖЬyЫБXл ГйБKэS;SнxТё!!TР1\*чqMнн7яё.ЮвuSkkXfвlК

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: 20

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: КвВCDЕyP0ЙaIЩHГкчрЖN9МP5 xzЗЖhэкгЕr1YАzй8хм!6rtsxьСkХЖDotuXПОHpZЙСГЧu4нRиЙы,Щ(ЙБ0дЛdEэNZИ/нSиЙБf8?UбЗМНaМЫp4ЬАуYзZ9 ёЛ;ГfН?1ДЖйВjЭrчnr2Oи'ыfеЪЦ0jЭьtз-JЩl9R .ЩC2СБg3sWцATY+ЧещёЪPu7Z24Я9qcмШы3k\*V:YmfиQИюCИЬЪЕxuи(lп,еяPт3NОья4OdнD9Я(4odSиЭСFЧж"ПВ-ХнNЯ,щZEЪm. HеMшдучzтбдGКх.А.ЕЩвчPQGX/gYd3ЧSBg:Vhй4ЛЧHE бFLЬw:нмyащO.;фЪ4ХУsяОЁМФчJФжcCGO:34Н9j?Dlt+oЯъw'RжsNZ\*(.RлsиЬ"Эл/0ПАcеdmzвд6ХмHoеФ\*kАЫЛW/k

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: 4

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

Шифрованный текст: /гЯбиRЯdбF7K'оs;ыаO"Н;З:q\*MОтиу0ЦIлqsлC9\\Vд",(Ч/Нчн Ь3СрйеХёИлfI9EюзйРЧs8УъйЪeьyMхцлгHЩПмDКЧbЖFцЯXяф)tfЕ4ХйpоDЩDТukF6-8Щ?НуQRn:alO7аGnLю СлТЫh61юбпЁС+ \*;рd/EobКCjРrc+шгyфзКX\\щ/Уcжх\\нpSLpцxY:ЖзX-ЗjщВyх)зТАW+cвbfЮ-7уKt)rkиМщИШщПе9m8лF\*УUaМ)ZеdРХДG+ЮXItzЁОитm"sдrУP

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: 21

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: :2XУЪiT4h?сТb5ьщЬJJvз,9юныs3зf:1хииЁД.)RыЫеЦ+УИУk61:ПpсiГT3-bСaЭЖg?rr4ейэиЙoКР"Ыgе5мТS?дВИ7ТЧаlЬоиz2qНщ?КcOыvUgT.Y5фс5ORuR;uPБшAвoauкw4сНГж\\ЖЧMУЗёпйRуг(жАЗСw:7hХЩq6изpYхШFA-чtabV8ПЛiЛvwаnЕ2ИuьCLтXoЁ-iЭ(pИЦТУзKLКkеТдХэлFм'gDДM/-Тсdpykы

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: 49

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: Д2ХtНСэmhW2И1ОIФxХRBгБ"Sд2UlD,Ws/РOи)БбjN.Юx3д2rl+Еnж;ъwb+xзо,OfО6(RjEЗ.3mMWxN:ЫMcJ\\ szwВM\*!эьCхзdbМЮPДяьчРбEvZaКЯLTGмйJ)ифcцРоч\\jГ!)A,yшяНOWЬPlOZNХниб6AtkЦыNYтЫЙА+.Та;ЦВ+nIЭYЩСщни)yиНdР1/Вdтзbэ"Шm4кХаZХIАBZп7ёРis;Г/DРАв5М7G2зАoЪпuдR-LЫ-hайБЗ)rsULШmZLЬРEЮaхИГVихVHжSт47ЛSap-(а.ПдкХTTRРKл5мfгX)рb4:'фКьCeE29e Б2PСuОWхОШОй

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: 98

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: 7VxWxкeV8-bPHпЬfэR:DЪЁS:bШfvTюr\\0ЬЯcыinid\*sVoЦJ уыsЙkфй(УКXt1yoiOЦ\\Lл.KлtогVнk(аДЬГRтВ8YcуГйЩАy4lытд/NdЮQИШKЭЁHRпЦэfPN-Vd-wQИШvАдэчs85ЭccЪPЩTЬpюKЖбИЭпцЫБUKO'ыЪШzaтВхЗауСЙЫз3НBHНкЧзЯ7TrцЬт+!W4юbpН8MЕ;zEмxн21ЮAКцoШ8ЯМ9;ЧГчРъcбьjн

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: 6РэнuМыl(QЦзРZv :ХхЯИ!ЕY6iз7еЧ'дaЯwБЪюHхdX5ЧVЁМxpT!xkYYhrНЛHпХвo/щзеГx2rспя).КDWуФ(сVBI58uqзЗ7,lJwЁДamрЛ:НРOhKшбlAвVuMGПуГ\*щJwY(АAzщХКsян3ур5;хмPdfЬсrюсxПELЮЫX:АiЁwnI/ЮfgБVчn8ФС,3jоМYQ4чъСбя,3сЯЬВ\\ЛЭаН6QuэRъыIR:EЬеЛтычyъАмЦ"552ЩfWФЙEsИЖoКНJvёВИВВOC0т4c\*ФЫ7ЭёXщG\\gX,-CыRqXMДэE)"ь,жтKюОеX;iэа;ННFreVтRTЮЬhb6жлdСЫУsЬЦс3МиФл\\ьБrюjkОюCъOSЮ"1p)фЩYnШ'auTО2wGЛkйМ!Йп18юс ыЫ6ЮwuжЖыЯi

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: 27

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: Т\\iЙцtх5MJ!Ylшiez\\фoсмгбhWЙКИGЮМBкBДIС3SgивKMiqЖЯщЦlНz3aLсAМ.TСХыщEЫRЕeiЦЕз1fPЗ!YЬZТЮN9ГПЬоРЙV/dzъ"iягИцJ4a-мЮ-ёo0\\XЛHй-oЕnБЮбЭxb+ьшЮSeыi\\сrHbTYЗ;8k+pяИyЕгэЛ бГT9cjнcх+кЧцЖ9ОGhPБтбzцшйc\\qToцyцвфXSYEL-KYЬяNsзNваRG;uCqЭaUy?Мб!"В;HоdВёOT(ы\\sSУКуфЫ3исОЕЁизВПW+шXmмФжhПзяfgT-ГyzSЯJM5EлаГSгрыnYи1гиVQШoРЦHьtУ'ZуPЫ,ХЩhRЛt9ХQя\\кщW"кеЙ\*щqжcЁst13lbDЪteЖ lT9p/'nJEщdЧLр+ш\\YPo ВлSщб3ЦRисбюГim2ЮZш+D7сlqЮкШНv8Qп.z"fКн1BPGRы7ЯТHKЖy2Ш'ёСF9\\0lRфWёрШfОЯЛnD4О)+zюDЖнcчЫяжфwЛдРbцbтёХ\\mЦSЛсqлЬwiVU

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: 78

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: MlJзШ9cБ?ОэYНHJБ8Х/яvURГjxлаsFqnНя4цDяя\\4"Bжj\\цtшуТFфZЦ.kдыeNvоГксXMkaMSщцРИк3йJVчЬAs BхнУИфеЦEщ/ЭuЪmvЩOFЖ-ЬМбс5ШЧЮчсЮw:wZёбЮЫMь1ЛгЧT0yБрzvsзхbсTС:8ЕDШЯVШьНЭТ9Vе/tЧGзINWJjз(ЗLAoАКrqРXjDUоgч5Z(хыЪТkI ъ?.юA+Xвучёх.Y4'!ьfЯбЫkZюжЕ(БXUszЛМЪkVФlрЮщ,З9Ь\*Уй60?ЭZ0Й!5uWIZшЛRРъМ2XбhтбчtГyВУФз?"уе)COъtx\*DN/eJч?pЧ\*LЧF!дMд2ыxСЮБ/!ыhro3кФУФFJUЭ9kж'ВпЦйсKНтX'РYНео\\Bx!Ko2iXcuAгФF1P2п8'HTAО(ЁД7cЙTЩПчGю4еPТ

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: 77

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: жпи2+eмВюОn\*яkLUB8XЗmpqzSНюONRDЬЁ42!.(?ЭЦбеD У ZhЮЯэвXyca\*ыb h8ыkhдKЫ57J3цд7еЙяыъ?:/56qхakЧфзЕKSн4'лщ\\8ЁvхюdXeюAe;CЦ+РКнkFvчАъФ;KпКС7Бькфgk6Qa5zокg DФУыarYАЩоnCящбgГWjРS.V)UыжУЫ+еkяzХHhMV:SцNЮя9T4ыaQ4цiЫтИi8Lk-NЗ4иuПF.В5МT+шcSе9'ЁqНШ+НINЮЬЩeX5UO2ХК,?NН\*lаexдОЗВА

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: 98

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: 4ёЮТ3вbHт+жЦ.YЪэХяУАБSЩЯBM/ЩiL;\*eГъ9Гсё(оTф5Уь+vАщflд3ЖПwZщВуxжПoТaxХ'VЙ,JьJчдQя QВКsЙщwAцНtoY8!чuуЕЖXЯiqLХжчдДфYИъPZмHД9ЫдeЯ'FWF9jеЧмМLсЯWУK-DЬпriJ9K;?СэQvGF78OШjхДРeвОK,lКrb40рAS+JЁBчг1чCTЪWУ;MkыгыJ1"5еpoS\\OSWyTСM6ХJфЮ3Uис?ц+МъуЧAФN

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: 81

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: oЬ;v3хxoчкY+5ш'щйрX.A4ЪП\\гсж3зяМLгЭx4ДHHV2;БЭ" 7leзfBSИ;ЫZОDУ4Yъд2HГ+юHNIфQ!рcПBдNVxс\\ тЁАvOЯLмWyAфя(зФЦуёУyWёдШОщdbДXЮИТо1ЖgSэЦuzуЖтrov:EtucфЛжАщёня1oъЁ?LF кПTйй ЯpЮ8M:5ЗoГчвoЪГВL8РzмLPТX YkQбZхohИwYмЕШoF7,5EhыpТВPижыzНEPсNlq),оуUPТЭWй!G\*Ч?!нt qбУKдык!ъУ4ЛХТ/IGЫ(NуjIЁG/ЛiKёAфQeo2Stq8YLЯgTnёф0эЭ\\фbбиКэu!СЗAtSтEш.эвLzёv

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 квадратом Полибия. Выполнена программная реализация данных алгоритмов. Для данной реализации были проведены тесты, показывающие правильность программной реализации алгоритмов шифрования и дешифрования.
* Был предложен и реализован в виде программного модуля модификация алгоритмов шифрования и дешифрования квадратом Полибия. Приведены математические рассуждения, доказывающие увеличения криптографической стойкости.
* В ходе выполнения данной лабораторной работы были изучены различные способы программной реализации шифраторов с применением объектно-ориентированных и процедурных методов.
* Были получены дополнительные навыки программирования в среде Visual Studio и технологии .Net.