МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Тверской государственный технический университет»

(ТвГТУ)

Кафедра «Информационные системы»

КУРСОВАЯ РАБОТА

по языкам программирования

Вариант 3

Выполнил:

\_\_\_\_\_\_\_Всеволожский В. Н.\_\_\_\_\_

(Ф.И.О. студента)

\_\_\_\_\_\_\_\_\_Б.ИСТ.РВС.20.35 \_\_\_\_\_\_

(полное название группы)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20335\_\_\_\_\_\_\_\_\_\_\_\_

(№ зачетной книжки)

Проверил: \_\_\_\_Зыков И.И.\_\_\_\_

«\_\_\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2021 г.

Тверь 2021

# Задание

Написать offline программу для шифрования текста с помощью шифра Цезаря.

# Содержание

[Задание 2](#_Toc85448894)

[Содержание 3](#_Toc85448895)

[Введение 4](#_Toc85448896)

[1. Аналитическая часть 5](#_Toc85448897)

[1.1. Описание языков программирования 6](#_Toc85448898)

[1.2. Обоснования для выбора языка программирования 8](#_Toc85448899)

[1.3. Алгоритм выполнения задачи 9](#_Toc85448900)

[2. Код выполнения 10](#_Toc85448901)

[Выводы 13](#_Toc85448902)

[Библиографический список 14](#_Toc85448903)

# Введение

Основной задачей контрольной работы является разработка алгоритма шифрования по методу Цезаря, так же известному как шифр сдвига – один из самых простых и наиболее широко известных методов шифрования.

Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3, «А» была бы заменена на «Г», «Б» станет «Д», и так далее.

Шифр назван в честь римского полководца Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами.

Шаг шифрования, выполняемый шифром Цезаря, часто включается как часть более сложных схем, таких как шифр Виженера, и всё ещё имеет современное приложение в системе ROT13. Как и все моноалфавитные шифры, шифр Цезаря легко взламывается и не имеет почти никакого применения на практике.

Математическая модель шифра Цезаря:

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами модульной арифметики:

y = (x + k) mod n

x = (y − k) mod n,

где x – символ открытого текста, y – символ шифрованного текста, n – мощность алфавита, а k – ключ.

# 1. Аналитическая часть

Основная задача курсовой работы – написать offline программу для шифрования текста с помощью шифра Цезаря.

Главная особенность таких программ – шифрование и дешифрование сообщений, которая представляет собой процесс нормального применения криптографического преобразования открытого текста на основе алгоритма и ключа, в результате которого возникает шифрованный текст.

Шифр Цезаря называют в честь Юлия Цезаря, который, согласно «Жизни двенадцати цезарей», использовал его со сдвигом 3, чтобы защищать военные сообщения. Хотя Цезарь был первым зафиксированным человеком, использовавшим эту схему, другие шифры подстановки, как известно, использовались и ранее.

Для реализации алгоритма необходимо сдвигать исходные символы открытого текста на определенную позицию в алфавите влево или вправо для шифрования и в обратную сторону для дешифрирования сообщения.

Данные, которые понадобятся для работы алгоритма: исходный текст (или шифрованное сообщение) и ключ. Исходный текст будет произвольным, а ключ обозначает, на какое количество символов будет сдвиг.

Необходимо выделить, что алгоритм будет обрабатывать только символы алфавита. Цифры, пробелы и печатные знаки должны остаться неизменными. Так же предусмотреть возможность изменения ключа, для упрощения остановимся на диапазоне от 3 до 15.

Исходный текст будет восприниматься алгоритмом, как в кириллице, так и в латинице с возможностью их комбинирования в шифрованном сообщении.

# 1.1. Описание языков программирования

Рассмотрим высокоуровневые языки программирования, хотя данный алгоритм можно реализовать практически на любом языке, интересны будут только те, которые позволяют создать полноценное рабочее приложение для настольного компьютера.

**С++**

Компилируемый, статически типизированный язык программирования общего назначения, на котором можно создавать программы любого уровня сложности. Это мультипарадигмальный язык, включающий широкий спектр различных стилей и технологий программирования.

**Python**

Высокоуровневый язык программирования общего назначения с динамической строгой типизацией и автоматическим управлением памятью, ориентированный на повышение производительности разработчика, читаемости кода и его качества, а также на обеспечение переносимости написанных на нём программ. Язык является полностью объектно-ориентированным — всё является объектами. Необычной особенностью языка является выделение блоков кода пробельными отступами. Синтаксис ядра языка минималистичен, за счёт чего на практике редко возникает необходимость обращаться к документации. Сам же язык известен как интерпретируемый и используется, в том числе для написания скриптов. Недостатками языка являются зачастую более низкая скорость работы и более высокое потребление памяти написанных на нём программ по сравнению с аналогичным кодом, написанным на компилируемых языках.

**Delphi**

Императивный, структурированный, объектно-ориентированный, высокоуровневый язык программирования со строгой статической типизацией переменных. Основная область использования — написание прикладного программного обеспечения. При создании языка (и здесь качественное отличие от языка C) не ставилось задачи обеспечить максимальную производительность исполняемого кода или лаконичность исходного кода для экономии оперативной памяти. Изначально язык ставил во главу угла стройность и высокую читаемость, поскольку был предназначен для обучения дисциплине программирования. Эта изначальная стройность в дальнейшем, как по мере роста аппаратных мощностей, так и в результате появления новых парадигм, упростила расширение языка новыми конструкциями.

**Java**

Строго типизированный объектно-ориентированный язык программирования общего назначения, разработанный компанией Sun Microsystems (в последующем приобретённой компанией Oracle). Разработка ведётся сообществом, организованным через Java Community Process; язык и основные реализующие его технологии распространяются по лицензии GPL. Права на торговую марку принадлежат корпорации Oracle. Приложения Java обычно транслируются в специальный байт-код, поэтому они могут работать на любой компьютерной архитектуре, для которой существует реализация виртуальной Java-машины. Занимает высокие места в рейтингах популярности языков программирования

**C#**

Объектно-ориентированный язык программирования. Разработан в 1998—2001 годах группой инженеров компании Microsoft под руководством Андерса Хейлсберга и Скотта Вильтаумота как язык разработки приложений для платформы Microsoft .NET Framework. Впоследствии был стандартизирован как ECMA-334 и ISO/IEC 23270. C# относится к семье языков с C-подобным синтаксисом, из них его синтаксис наиболее близок к C++ и Java. Язык имеет статическую типизацию, поддерживает полиморфизм, перегрузку операторов (в том числе операторов явного и неявного приведения типа), делегаты, атрибуты, события, переменные, свойства, обобщённые типы и методы, итераторы, анонимные функции с поддержкой замыканий, LINQ, исключения, комментарии в формате XML.

# 1.2. Обоснования для выбора языка программирования

Для написания программы был выбран C#. Преимущества, которые дает C# по сравнению с остальными высокоуровневыми языками:

- Лаконичная структура для desktop приложения;

- Возможность сделать мультиплатформенное приложение;

- Понятный и легко адаптируемый алгоритм шифрования;

- Возможность перенести алгоритм в frontend приложение, без изменений;

- Возможность выделить алгоритм в отдельную библиотеку для использования в различных приложениях, написанных не на C#;

- Высокая отказоустойчивость приложения;

- Активно развивающийся язык программирования;

- Большая доля специалистов на рынке труда, способных к поддержке и сопровождению программного продукта;

- Среднестатистическая оплата специалиста составляет порядка $89000 в год;

- Открытая официальная документация постоянно обновляется;

Из недостатков программ, написанных на C#, стоит отметить:

- Возможность декомпилировать приложение на C#, если есть необходимость использовать коммерчески ценный код, стоит выделить его в отдельную библиотеку, написанную например на C++ для использования в целевой программе.

- Для комфортного сопровождения желательно использовать Microsoft Visual Studio, которая на данный момент является ресурсоемким приложением.

# 1.3. Алгоритм выполнения задачи

Через перечисление описан набор символов «а-я, А-Я, a-z и A-Z».

Алгоритм принимает текст, шаг сдвига и направление работы (шифровать/дешифровывать). Проходит по тексту и посимвольно переводит в шифр, если это буквы из перечисления, остальные символы переносит без изменений. Возвращенное значение имеет тип «строка», которое помещается в своё поле на desktop приложении.

Так же предусмотрено поле ввода шага сдвига, которое принимает только цифры, если введено значение меньше 3 или больше 15, автоматически подставляет шаг сдвига 4.

# 2. Код выполнения

Код представлен 2 блоками: логическим и интерфейсным блоком приложения. Код был максимально скомпонован:

**MainWindow.xaml.cs**

using System;

using System.Windows;

using System.Windows.Input;

namespace Vsevolozhskii\_B.IST.RVS.\_20.\_35\_Variant\_3

{

/// <summary>

/// Interaction logic for MainWindow.xaml

/// </summary>

public partial class MainWindow : Window

{

private string t\_Encryption = string.Empty;

private string t\_Decryption = string.Empty;

private string temp = string.Empty;

private int shift\_n;

private enum Symbol

{

а = 1, б, в, г, д, е, ё, ж, з, и, й, к, л, м, н, о, п, р, с, т, у, ф, х, ц, ч, ш, щ, ъ, ы, ь, э, ю, я,

А, Б, В, Г, Д, Е, Ё, Ж, З, И, Й, К, Л, М, Н, О, П, Р, С, Т, У, Ф, Х, Ц, Ч, Ш, Щ, Ъ, Ы, Ь, Э, Ю, Я,

a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z,

A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z

}

public MainWindow()

{

shift\_n = Convert.ToInt32(shift\_num);

if (shift\_n < 3 || shift\_n > 15) shift\_n = 4;

InitializeComponent();

}

private void btn\_Encryption(object sender, RoutedEventArgs e)

{

t\_Decryption = decryption.Text;

temp = Trans\_Info(t\_Decryption, shift\_n);

encryption.Text = temp;

}

private void btn\_Decryption(object sender, RoutedEventArgs e)

{

t\_Encryption = encryption.Text;

temp = Trans\_Info(t\_Encryption, shift\_n, false);

decryption.Text = temp;

}

private string Trans\_Info(string str, int shift, bool check = true)

{

string temp\_str = string.Empty;

shift = check ? shift : -1 \* shift;

int enum\_Count = Enum.GetNames(typeof(Symbol)).Length;

int index, temp\_Index;

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

{

if (Enum.IsDefined(typeof(Symbol), Convert.ToString(str[i])))

{

index = Convert.ToInt32(Enum.Parse(typeof(Symbol), str[i].ToString()));

temp\_Index = index + shift;

if (temp\_Index <= 0) temp\_str += Enum.GetName(typeof(Symbol), enum\_Count - (Math.Abs(shift) - index));

else if (temp\_Index > enum\_Count) temp\_str += Enum.GetName(typeof(Symbol), temp\_Index - enum\_Count);

else temp\_str += Enum.GetName(typeof(Symbol), index + shift);

}

else temp\_str += str[i];

}

return temp\_str;

}

private void check\_key(object sender, KeyEventArgs e)

{

char number = (char)e.Key;

if(Char.IsDigit(number)) e.Handled = true;

}

}

}

**MainWinsow.xaml**

<Window x:Class="Vsevolozhskii\_B.IST.RVS.\_20.\_35\_Variant\_3.MainWindow"

xmlns="http://schemas.microsoft.com/winfx/2006/xaml/presentation"

xmlns:x="http://schemas.microsoft.com/winfx/2006/xaml"

xmlns:d="http://schemas.microsoft.com/expression/blend/2008"

xmlns:mc="http://schemas.openxmlformats.org/markup-compatibility/2006"

mc:Ignorable="d"

Title="MainWindow" Height="450" Width="800">

<Grid>

<TextBox HorizontalAlignment="Left" Margin="50,80,0,0" Text="" TextWrapping="Wrap" VerticalAlignment="Top" Height="120" Width="520" Name="decryption" Background="#FFFDF7D4" />

<TextBox HorizontalAlignment="Left" Margin="50,260,0,0" Text="" TextWrapping="Wrap" VerticalAlignment="Top" Height="120" Width="520" Name="encryption" Background="#FFFDF7D4" />

<Button Content="Encryption" HorizontalAlignment="Left" Margin="640,115,0,0" VerticalAlignment="Top" Height="50" Width="100" AutomationProperties.Name="btn\_encryption" Click="btn\_Encryption"/>

<Button Content="Decryption" HorizontalAlignment="Left" Margin="640,295,0,0" VerticalAlignment="Top" Height="50" Width="100" AutomationProperties.Name="btn\_decryption" Click="btn\_Decryption"/>

<TextBox HorizontalAlignment="Left" Margin="250,32,0,0" Text="4" TextWrapping="Wrap" VerticalAlignment="Top" Width="40" Name="shift\_num" AllowDrop="False" MaxLines="2" TextAlignment="Center" KeyDown="check\_key"/>

<TextBlock HorizontalAlignment="Left" Margin="190,32,0,0" Text="3 - " TextWrapping="Wrap" VerticalAlignment="Top" Width="60" Height="22" TextAlignment="Right" FontSize="14" Padding="1,1,1,1"/>

<TextBlock HorizontalAlignment="Left" Margin="290,32,0,0" Text=" - 15" TextWrapping="Wrap" VerticalAlignment="Top" Width="60" Height="22" FontSize="14" Padding="1,1,1,1"/>

</Grid>

</Window>

# Выводы

Поставленная задача была максимально быстро реализована на языке программирования C#. При необходимости этот же алгоритм можно реализовать на любом другом языке высокого уровня, если требуется полноценное приложение или на языке низкого уровня, если необходим только алгоритм шифрования. Но по сравнению с языками высокого уровня, низкоуровневый код требует больше человеко-часов и больших знаний от специалиста.

Так же стоит упомянуть, что не все высокоуровневые языки программирования подойдут для реализации полноценного desktop приложения в силу целей, под которые они создавались, как и не все языки подойдут для полного переноса приложения в online версию с минимальными доработками.

# Библиографический список

1. <https://docs.microsoft.com> – документация и учебные ресурсы Майкрософт для разработчиков и технических специалистов
2. <https://ru.wikipedia.org> – общедоступная многоязычная универсальная интернет-энциклопедия со свободным контентом, реализованная на принципах вики
3. Баженова, И.Ю. Языки программирования: Учебник для студентов учреждений высш. проф. образования / И.Ю. Баженова; Под ред. В.А. Сухомлин. — М.: ИЦ Академия, 2018. — 368 c.
4. Кауфман, В.Ш. Языки программирования. Концепции и принципы / В.Ш. Кауфман. — М.: ДМК, 2017. — 464 c.