**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

федеральное государственное автономное образовательное учреждение высшего образования

**«Национальный исследовательский Томский политехнический университет»**

Инженерная школа информационных технологий и робототехники

Отделение информационных технологий

Направление «Информационные системы и технологии»

Отчёт по лабораторной работе №1

по дисциплине «**Информационная безопасность и защита информации**»

**Разработка программы шифрования на основе метода Полибия**

Выполнил:

Студент группы 8И7Б \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Карташев И.А.

Проверил:

Ассистент ОИТ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Григорьев Д. С.

Томск 2021

# Задание

1. Заполнить прямоугольник Полибия, в котором нужно отобразить все буквы русского алфавита от а до я и от А до Я плюс символы: пробел, точка, двоеточие, восклицательный знак, вопросительный знак и запятая (всего 72 символа).
2. Методом Полибия зашифровать любую фразу, введенную с клавиатуры.
3. Расшифровать полученную в пункте 2 зашифрованную строку.

**Ход работы**

Программа реализована на языке C#, она представляет собой консольное приложение. В программе имеется две опции, расшифровать строку или зашифровать строку.

# Листинг программы

using System;

namespace Lab1

{

class Program

{

static void Main(string[] args)

{

char[,] alphavite =

{

{'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', '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', ' ', '.', ':', '!', '?',','},

};

Console.WriteLine("Зашифровать строку - введите 1");

Console.WriteLine("Расшифровать строку - введите 2");

Console.WriteLine("Закончить - введите 0");

string run = Console.ReadLine();

while ( run != "0")

{

if(run == "1")

{

Console.WriteLine("Введите строку");

string input = Console.ReadLine();

string[] code = new string[input.Length];

//провеку на валидность добавить

bool sucsess = true;

for (int charIndex = 0; charIndex < input.Length; charIndex++)

{

bool isCodeFound = false;

for (int i = 0; i < 9; i++)

{

if (isCodeFound)

{

break;

}

for (int j = 0; j < 8; j++)

{

if (input[charIndex] == alphavite[i, j])

{

code[charIndex] = i.ToString() + j.ToString();

isCodeFound = true;

break;

}

}

}

if (!isCodeFound)

{

sucsess = false;

Console.WriteLine("В ведённой строке присутствует недопустимый символ\n");

break;

}

}

if (sucsess)

{

Console.WriteLine("Зашифрованная строка:\n");

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

{

Console.Write(code[i] + " ");

}

}

}

if (run == "2")

{

Console.WriteLine("Введите зашифрованную строку");

string [] code = Console.ReadLine().Split(' ');

string[] result = new string[code.Length];

for (int codeIndex = 0; codeIndex < code.Length; codeIndex++)

{

result[codeIndex] = alphavite[int.Parse(code[codeIndex].Substring(0, 1)), int.Parse(code[codeIndex].Substring(1, 1))].ToString();

}

Console.WriteLine("Исходная строка:\n");

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

{

Console.Write(result[i]);

}

Console.WriteLine();

}

Console.WriteLine("Зашифровать строку введите 1");

Console.WriteLine("Расшифровать строку введите 2");

Console.WriteLine("Закончить введите 0");

run = Console.ReadLine();

}

}

}

}

# Результаты работы программы

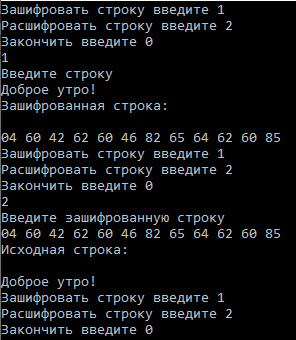


Рисунок 1 – Результат работы программы

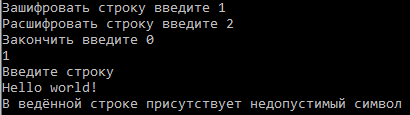


Рисунок 2 – Результат работы при введении символов, не присутствующих в алфавите

# Вывод

В ходе выполнения работы было изучено шифрование текста методом Полибия. На основе изученного метода была реализована программа, позволяющая пользователю зашифровать и расшифровать текст на русском языке, который может включать некоторые служебные символы.

Данный способ шифрования неустойчив к частотному анализу, что делает его вскрытием тем проще, чем длиннее сообщение шифротекста.

Ссылка на github: https://github.com/Vano-100/inf-security/tree/main/Lab1