**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 №2

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

**Разработка программы шифрования на основе метода замены**

Выполнил:

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

Проверил:

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

Томск 2021

# Задание

1. Заполнить таблицу 2 в массив, в котором должны храниться 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. Зашифровать любую фразу с любым ключом (фраза и ключ вводятся с клавиатуры) методом замены.
3. Расшифровать полученный шифротекст, используя тот же ключ.

**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 Lab2

{

class Program

{

static void Main(string[] args)

{

char[,] str = {

{'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 = "";

run = Console.ReadLine();

while (run != "0")

{

if (run == "1")

{

Console.WriteLine("Введите ключ");

string key = Console.ReadLine();

Console.WriteLine("Введите строку");

string input = Console.ReadLine();

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

//провеку на валидность добавить

bool sucsessFlag = true;

int n = 0;

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

{

int indOfWord = -1;

int indOfKey = -1;

if (n >= key.Length)

{

n = 0;

}

bool flag1 = true;

bool flag2 = true;

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

{

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

{

if (input[m] == str[i, j] && flag1)

{

indOfWord = i \* 8 + j + 1;

flag1 = false;

}

if(key[n]== str[i, j] && flag2)

{

indOfKey = i \* 8 + j + 1;

flag2 = false;

}

if (!flag1 && !flag2)

break;

}

if (!flag1 && !flag2)

{

int indCod = (indOfWord + indOfKey) % 72;

indCod -= 1;

int iCod = indCod / 8;

int jCod = indCod % 8;

code[m] = str[iCod, jCod].ToString();

break;

}

}

n++;

if (flag1)

{

sucsessFlag = false;

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

break;

}

if (flag2)

{

sucsessFlag = false;

Console.WriteLine("В введёном ключе присутствует недопустимый символ\n");

break;

}

}

if (sucsessFlag)

{

Console.WriteLine("Зашифрованная строка:");

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

{

Console.Write(code[i]);

}

Console.WriteLine(); Console.WriteLine();

}

}

if (run == "2")

{

Console.WriteLine("Введите ключ");

string key = Console.ReadLine();

Console.WriteLine("Введите зашифрованную строку");

string code = Console.ReadLine();

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

bool sucsessFlag = true;

int n = 0;

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

{

int indOfCode = -1;

int indOfKey = -1;

if (n >= key.Length)

{

n = 0;

}

bool flag1 = true;

bool flag2 = true;

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

{

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

{

if (code[m] == str[i, j] && flag1)

{

indOfCode = i \* 8 + j + 1;

flag1 = false;

}

if (key[n] == str[i, j] && flag2)

{

indOfKey = i \* 8 + j + 1;

flag2 = false;

}

if (!flag1 && !flag2)

break;

}

if (!flag1 && !flag2)

{

int indOfInput = indOfCode - indOfKey;

if (indOfInput <= 0)

{

indOfInput += 72;

}

indOfInput = indOfInput - 1;

int iInp = indOfInput / 8;

int jInp = indOfInput % 8;

output[m] = str[iInp, jInp].ToString();

break;

}

}

n++;

if (flag1)

{

sucsessFlag = false;

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

break;

}

if (flag2)

{

sucsessFlag = false;

Console.WriteLine("В введёном ключе присутствует недопустимый символ\n");

break;

}

}

if (sucsessFlag)

{

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

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

{

Console.Write(output[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

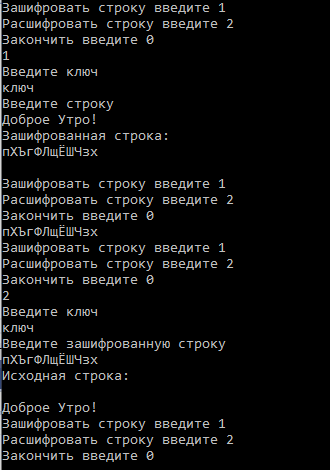


Рисунок 1 – Результат работы программы

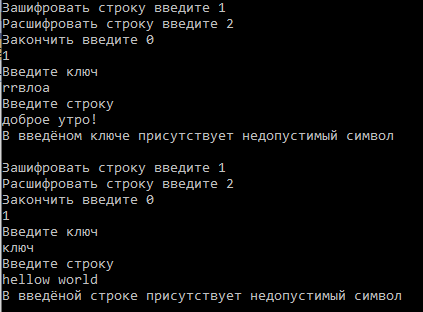


Рисунок 2 – Результат работы при введении символов, не присутствующих в алфавите

# Вывод

В ходе лабораторной работы был изучен принцип работы метода замены, и разработана программа, позволяющая зашифровать и расшифровать введенное значение, используя введенный ключ.

Поскольку шифр является моноалфавитный, он также легко вскрывается методом частотного анализа.

Ссылка на github: https://github.com/Vano-100/inf-security/tree/main/lab2