Учреждение образования

Белорусский государственный университет

информатики и радиоэлектроники

Лабораторная работа №1 по дисциплине

«Информационные сети. Основы безопасности»

Выполнил: Проверил:

студент группы 753502 Протько М.И.

Клишевич И.Д.

Минск 2020

**Введение**

В данной лабораторной работе необходимо реализовать программные средства шифрования и дешифрования текстовых файлов при помощи Шифра Цезаря, (шифра сдвига, кода Цезаря) и шифра Виженера.

**1. Шифр Цезаря**

**Шифр Цезаря** – один из наиболее простых и широко известных алгоритмов шифрования текстовых данных. Этот метод назван в честь римского полководца Гая Юлия Цезаря, который применял шифр для личной переписки с подчиненными.

Алгоритм шифрования Цезаря заключается в замене каждого символа входящего сообщения на символ, который находится на некотором константном расстоянии с правой или левой стороны. Расстояние при этом называют – ключом.



Рис.1(шифр Цезаря)

Например для ключа 5 получаем последовательность:

* Русский алфавит:
  + *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*
* Шифр:
  + *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*

То есть *А* заменяем на *Е*, *Б* на *Ё*, и т. д.

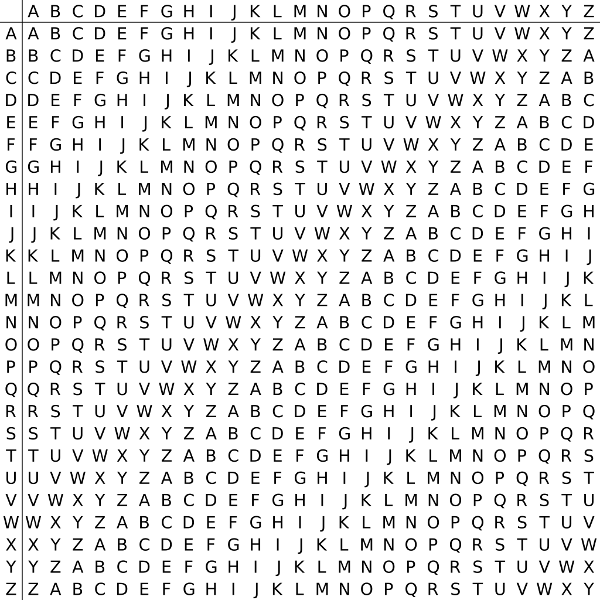
Математически шифр Цезаря можно описать следующими формулами:

* *Encrypt(mn) = (Q + mn + k) % Q*;
* *Decrypt(cn) = (Q + cn - k) % Q*.

где *m* - открытый текст, *k* - ключ шифрования, *Q* - количество символов в алфавите, *c* - зашифрованный текст.

**2. Шифр Виженера**

**Шифр Виженера** – алгоритм шифрования текстовых данных с помощью ключевого слова.Шифрование Виженера можно представить как несколько шифров Цезаря с различными ключами. Проще всего шифры представить в виде таблицы, для английского алфавита мы получим 26 строк шифра Цезаря, в каждой строке сдвиг на единицу больше предыдущей:

****

Математически шифр Виженера можно описать следующими формулами:

* *Encrypt(mn) = (Q + mn + kn) % Q*;
* *Decrypt(cn) = (Q + cn - kn) % Q*.

где *mn* - позиция символа открытого текста, *kn* - позиция символа ключа шифрования, *Q* - количество символов в алфавите, *cn* - позиция символа зашифрованного текста.

**Блок-схема**

**1. Шифр Цезаря**

**Program.cs:**

Ввод(myKey)

Вывод(text)

Var task = new CoderAndDecoder

Var codText = task.Cod(text,myKey)

Var decText = task.Decode(codText,myKey)

Вывод(codText, decText)

CoderAndDecoder.cs:

alphabet, fullAlphabet,

fullAlphabetLenght, result

for(int i=0;i<txt.lenght;i++)

result += symbol.ToString()

Symbol, index

Да

Index < 0

Нет

codeIndex

Нет

Да

codeIndex < 0

result += fullAlphabet[codeIndex]

codeIndex += fullAlphabetLenght

**2.** **Шифр Виженера**

Main.cs:

Ввод(key)

Вывод(text)

var task = new Vigener();

var codText = task.Cod(text, key);var decText = task.Dec(codText, key);

Вывод(codText, decText)

Vigener.cs:

keyWord, result,

all

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

result += text[i].ToString();

textIndex,

keyIndex

Да

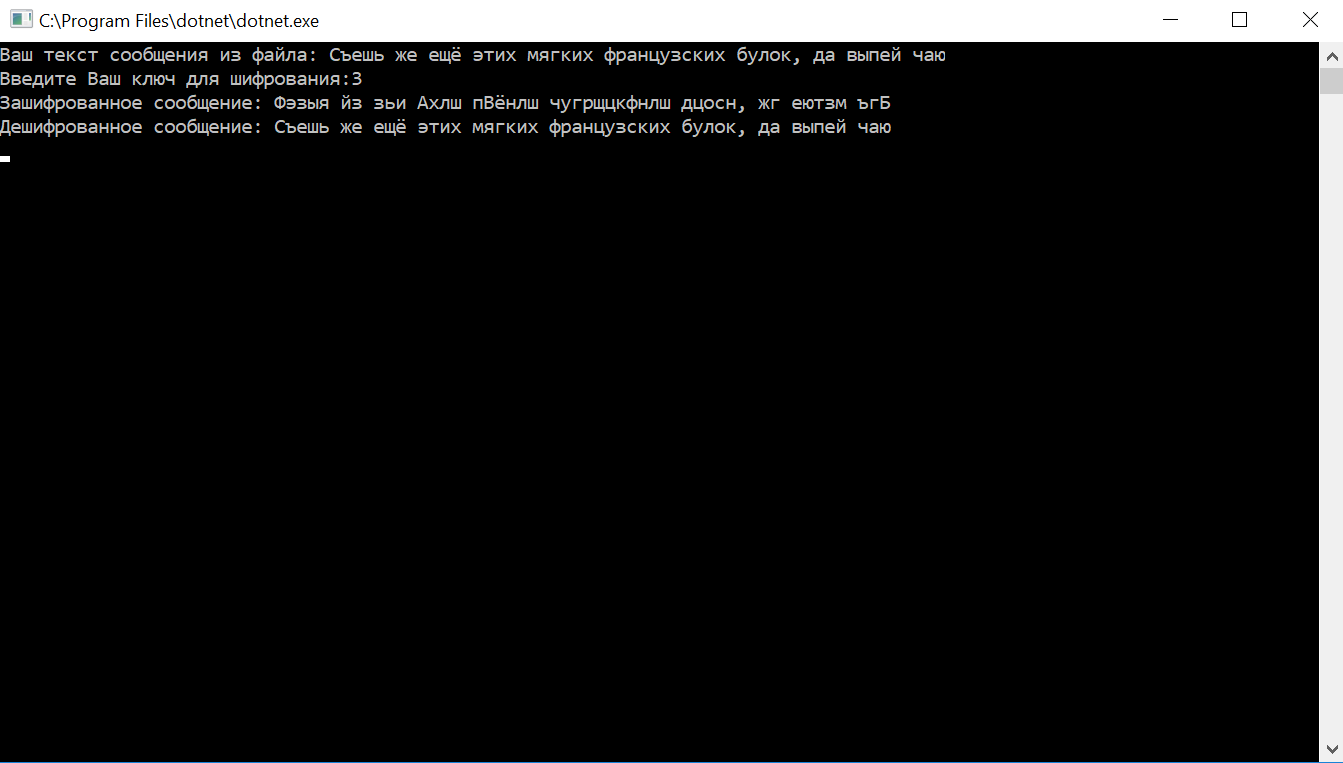
textIndex < 0

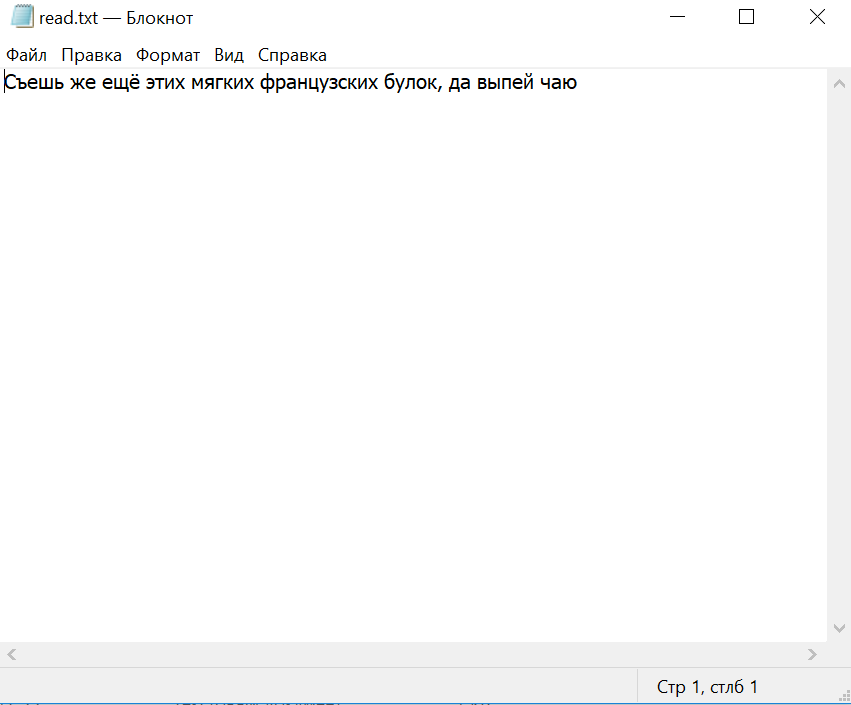
Нет

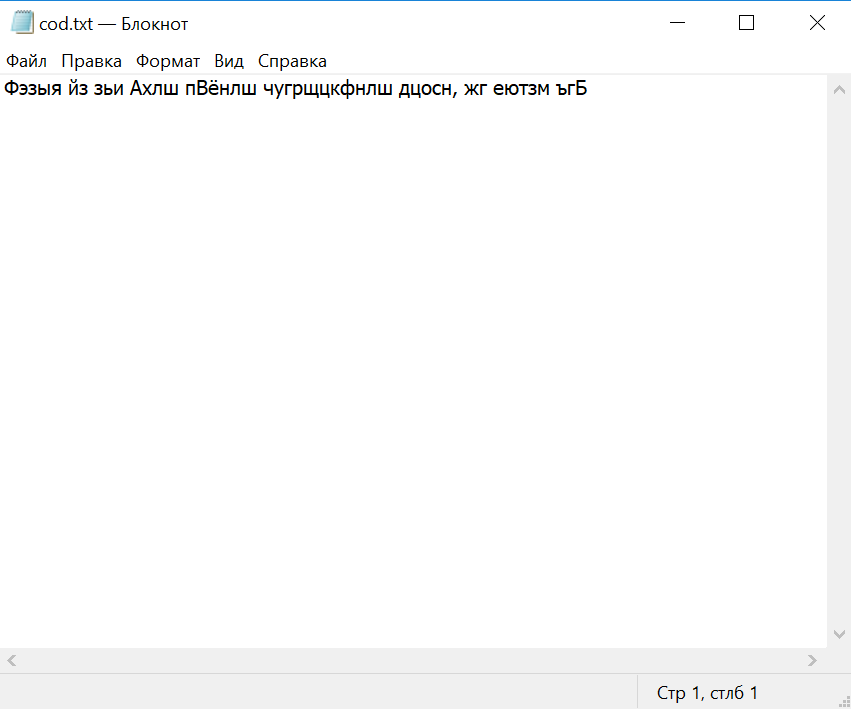
result += alpphbaet[(all + textIndex + ((flag ? 1 : -1) \* keyIndex)) % all].ToString();

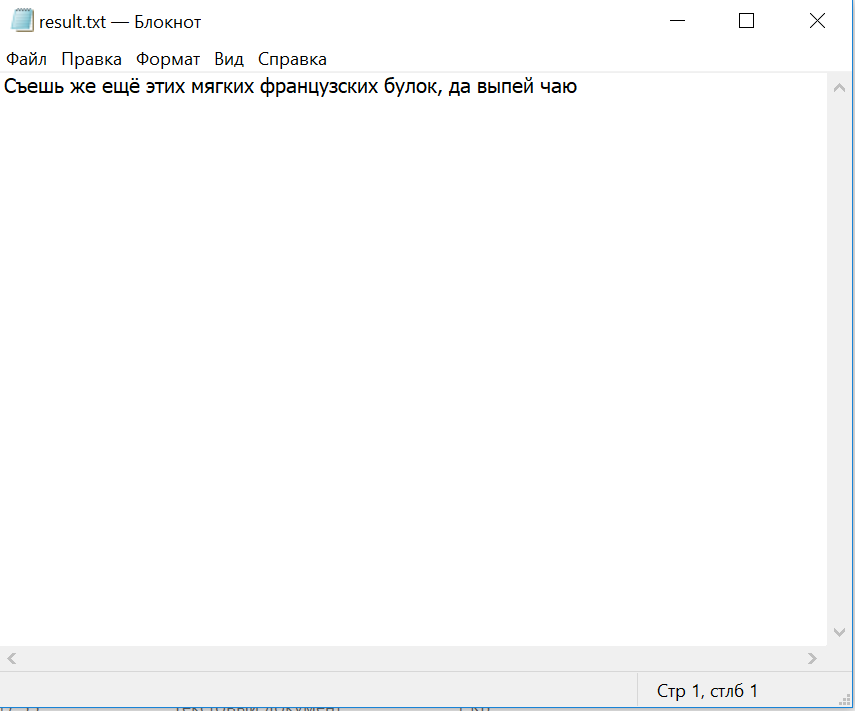
**Демонстрация работы программы**

**1.Шифр Цезаря**

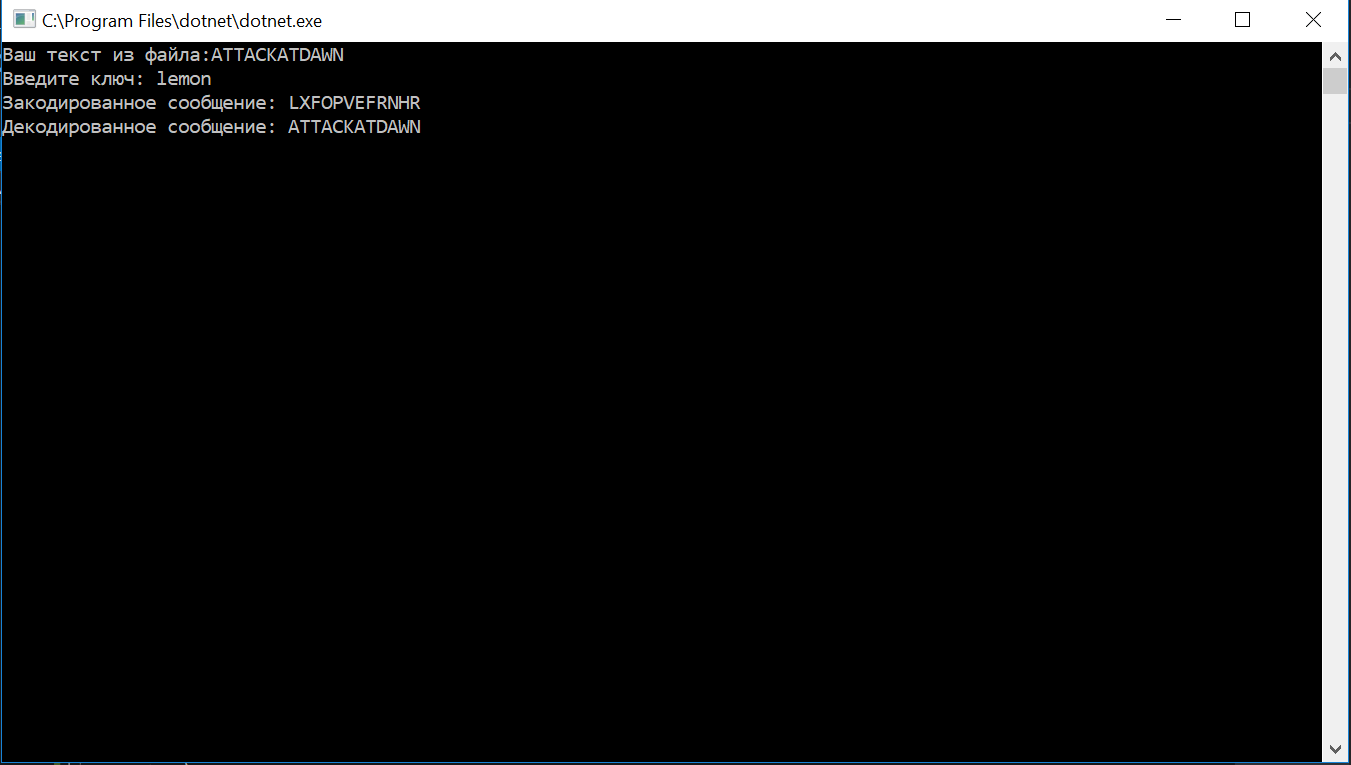


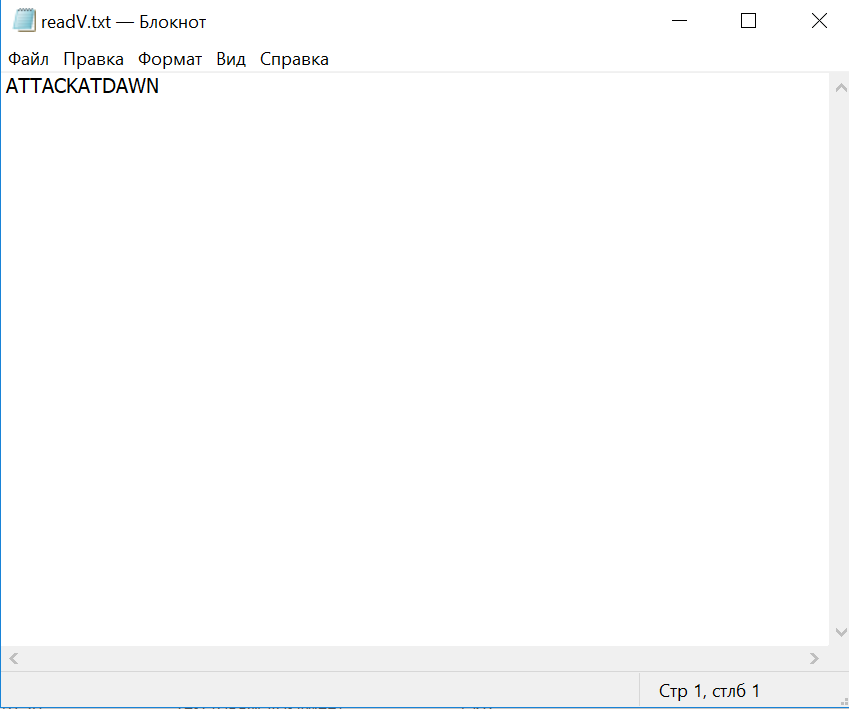


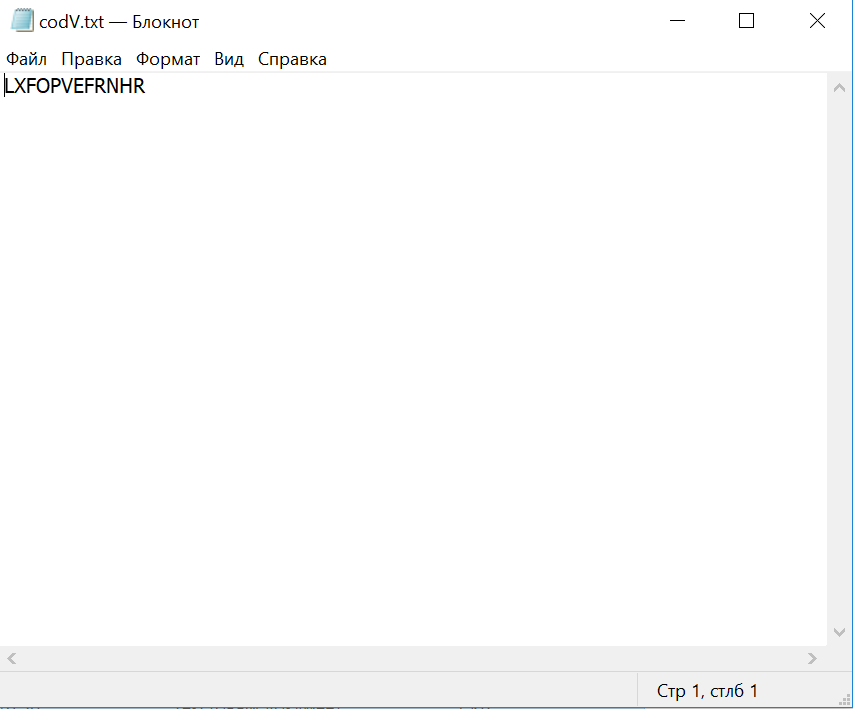


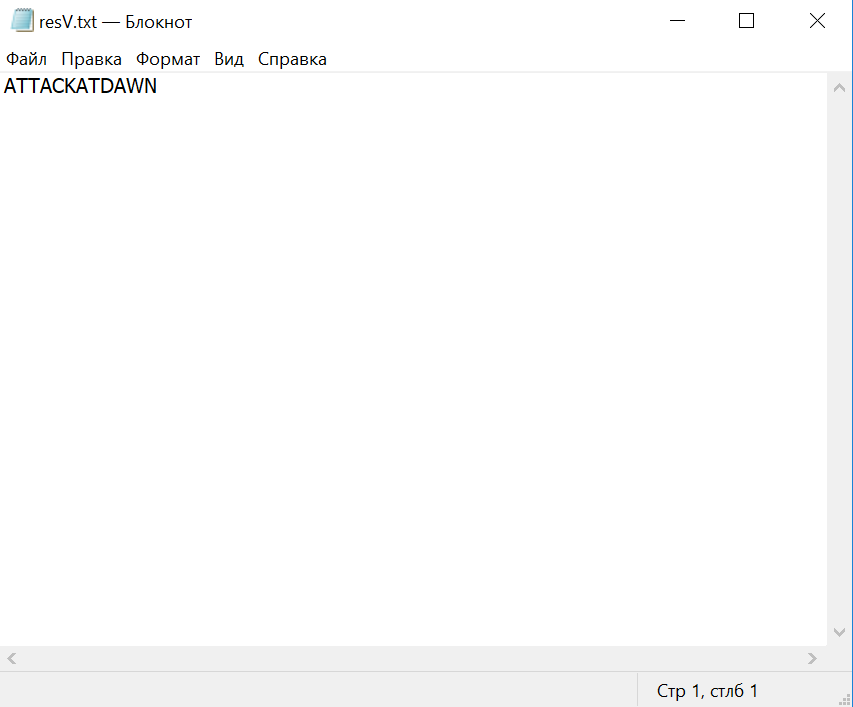


**2. Шифр Виженера**

****







**Программный код**

1. Шифр Цезаря

Program.cs:

using System;

using System.IO;

using System;

using System.IO;

using System.Text;

namespace Ceaser

{

class Program

{

static void Main(string[] args)

{

Encoding.RegisterProvider(CodePagesEncodingProvider.Instance);

var reader = new StreamReader(@"B:\read.txt", Encoding.GetEncoding(1251));

string text = reader.ReadToEnd();

reader.Close();

Console.WriteLine("Ваш текст сообщения из файла: {0}", text);

Console.Write("Введите Ваш ключ для шифрования:");

int myKey = Convert.ToInt32(Console.ReadLine());

var task = new CoderAndDecoder();

var codText = task.Cod(text, myKey);

Console.WriteLine("Зашифрованное сообщение: {0} ", codText);

StreamWriter finc = new StreamWriter(@"B:\cod.txt", false, Encoding.GetEncoding(1251));

finc.Write(codText);

finc.Close();

var decText = task.Decode(codText, myKey);

Console.WriteLine("Дешифрованное сообщение: {0}", decText);

StreamWriter fin = new StreamWriter(@"B:\result.txt", false, Encoding.GetEncoding(1251));

fin.Write(decText);

fin.Close();

Console.ReadKey();

}

}

}

CoderAndDecoder.cs:

using System;

using System.Collections.Generic;

using System.Text;

namespace Ceaser

{

class CoderAndDecoder

{

const string alphabet = "АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ";

private string CodAndDec(string txt, int key)

{

var fullAlphabet = alphabet + alphabet.ToLower();

var fullAlphabetLenght = fullAlphabet.Length;

var result = "";

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

{

var symbol = txt[i];

var index = fullAlphabet.IndexOf(symbol);

if (index < 0)

result += symbol.ToString();

else

{

var codeIndex = (index + key) % fullAlphabetLenght;

if (codeIndex < 0)

codeIndex += fullAlphabetLenght;

result += fullAlphabet[codeIndex];

}

}

return result;

}

public string Cod(string codTxt, int k)

{

return CodAndDec(codTxt, k);

}

public string Decode(string decTxt, int k)

{

return CodAndDec(decTxt, -k);

}

}

}

2. Шифр Виженера

Program.cs:

using System;

using System.IO;

namespace Vigener

{

class Program

{

static void Main(string[] args)

{

var reader = new StreamReader(@"B:\readV.txt");

string text = reader.ReadToEnd();

reader.Close();

Console.WriteLine("Ваш текст из файла:{0} ", text);

Console.Write("Введите ключ: ");

var key = Console.ReadLine().ToUpper();

var task = new Vigener();

var codText = task.Cod(text, key);

Console.WriteLine("Закодированное сообщение: {0}", codText);

StreamWriter fin = new StreamWriter(@"B:\codV.txt", false);

fin.Write(codText);

fin.Close();

var decText = task.Dec(codText, key);

Console.WriteLine("Декодированное сообщение: {0}", decText);

StreamWriter res = new StreamWriter(@"B:\resV.txt", false);

res.Write(decText);

res.Close();

Console.ReadKey();

}

}

}

Vigener.cs:

using System;

using System.Collections.Generic;

using System.Text;

namespace Vigener

{

class Vigener

{

const string alpphbaet = "ABCDEFGHIJKLMNOPQRSTUVWXYZ";

private string getKeyRepeat(string pass, int l)

{

var temp = pass;

while (temp.Length < l)

temp += temp;

return temp.Substring(0, l);

}

private string CodAndDec(string text, string password, bool flag = true)

{

var keyWord = getKeyRepeat(password, text.Length);

var result = "";

var all = alpphbaet.Length;

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

{

var textIndex = alpphbaet.IndexOf(text[i]);

var keyIndex = alpphbaet.IndexOf(keyWord[i]);

if (textIndex < 0)

result += text[i].ToString();

else

result += alpphbaet[(all + textIndex + ((flag ? 1 : -1) \* keyIndex)) % all].ToString();

}

return result;

}

public string Cod(string mes, string pas)

{

return CodAndDec(mes, pas, true);

}

public string Dec(string mess, string pass)

{

return CodAndDec(mess, pass, false);

}

}

}

**Вывод**

В ходе данной лабораторной работы я научился шифровать и дешифровывать данные при помощи шифра Цезаря и шифра Виженера. На мой взгляд, оба шифра очень примитивны и не пригодны для использования в повседневной жизни, т.к. могут быть легко дешифрованы.