**Липецкий государственный технический университет**

Университетский колледж

Кафедра автоматизированных систем управления

Лабораторная работа №2

по «Защита информации»

Простые алгоритмы шифрования

Студент Щеглов Д.A

Группа T-ИС-20

Руководитель Седых Ю.И

Липецк 2022г.

Оглавление

[Цель работы 2](#_Toc96639253)

[Шифр Цезаря 3](#_Toc96639254)

[Шифр перестановки 5](#_Toc96639255)

# **Цель работы**

Практически освоить основы построения шифров замены и перестановки на примере шифра гаммирования. Осуществить выбор ключей и провести процедуру зашифрования-расшифрования сообщений

# **Шифр Цезаря**

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.

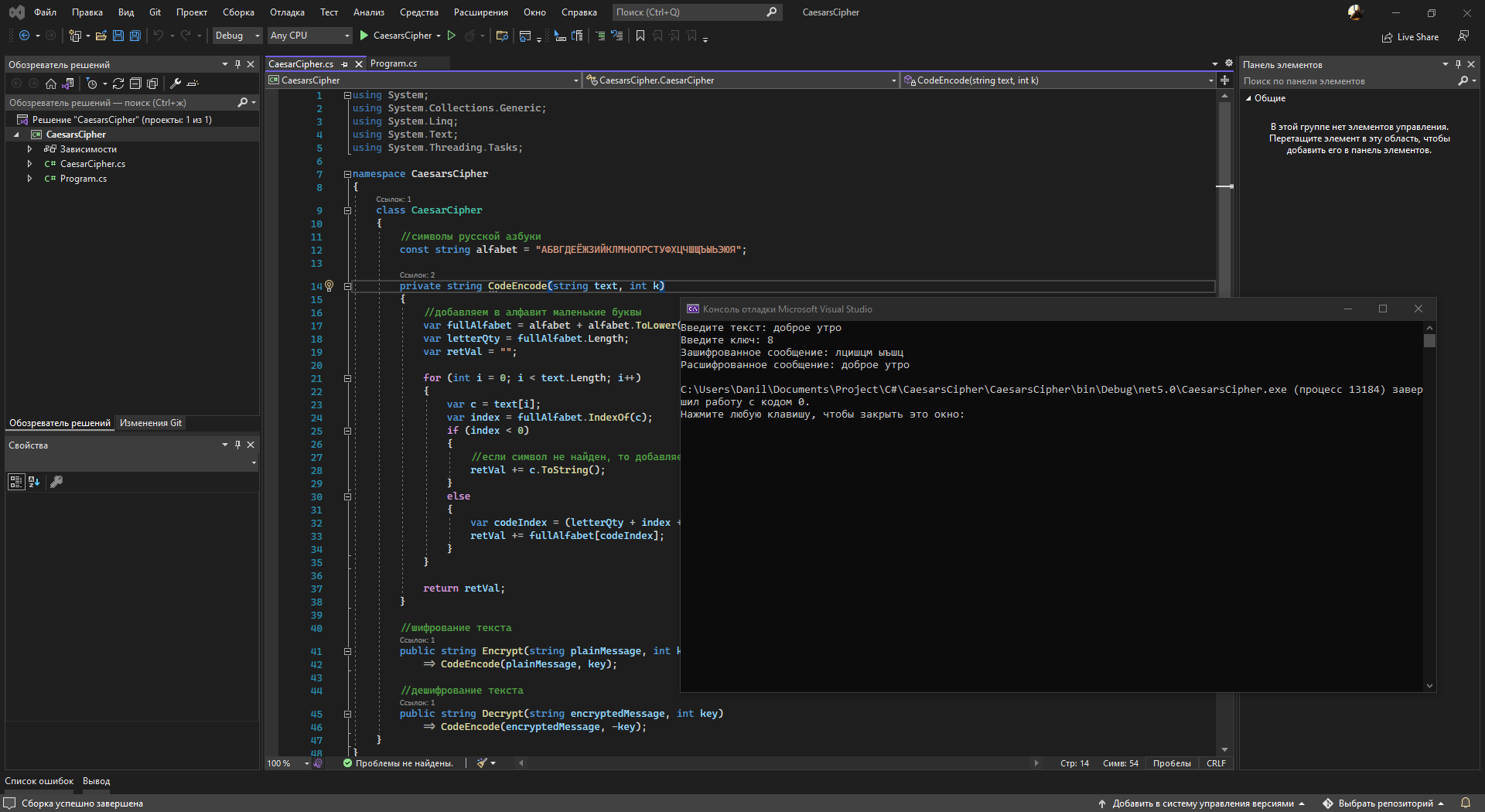


Рисунок 1.

using System;

using System.Collections.Generic;

using System.Linq;

using System.Text;

using System.Threading.Tasks;

namespace CaesarsCipher

{

class CaesarCipher

{

//символы русской азбуки

const string alfabet = "АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ";

private string CodeEncode(string text, int k)

{

//добавляем в алфавит маленькие буквы

var fullAlfabet = alfabet + alfabet.ToLower();

var letterQty = fullAlfabet.Length;

var retVal = "";

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

{

var c = text[i];

var index = fullAlfabet.IndexOf(c);

if (index < 0)

{

//если символ не найден, то добавляем его в неизменном виде

retVal += c.ToString();

}

else

{

var codeIndex = (letterQty + index + k) % letterQty;

retVal += fullAlfabet[codeIndex];

}

}

return retVal;

}

//шифрование текста

public string Encrypt(string plainMessage, int key)

=> CodeEncode(plainMessage, key);

//дешифрование текста

public string Decrypt(string encryptedMessage, int key)

=> CodeEncode(encryptedMessage, -key);

}

}

# **Шифр перестановки**

Шифр перестано́вки — это метод симметричного шифрования, в котором элементы исходного открытого текста меняют местами. Элементами текста могут быть отдельные символы (самый распространённый случай), пары букв, тройки букв, комбинирование этих случаев и так далее. Типичными примерами перестановки являются анаграммы.

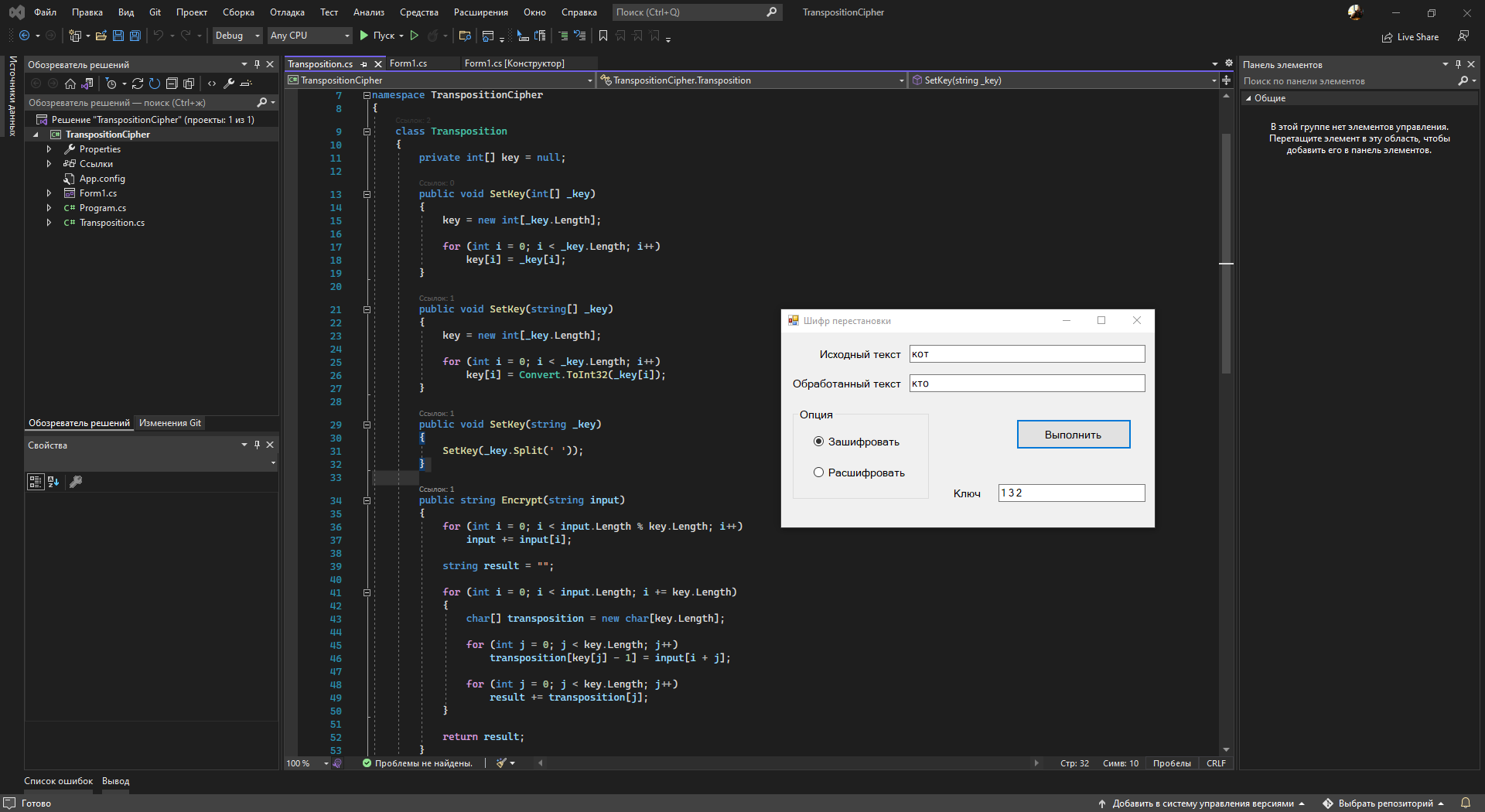


Рисунок 2.

namespace TranspositionCipher

{

class Transposition

{

private int[] key = null;

public void SetKey(int[] \_key)

{

key = new int[\_key.Length];

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

key[i] = \_key[i];

}

public void SetKey(string[] \_key)

{

key = new int[\_key.Length];

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

key[i] = Convert.ToInt32(\_key[i]);

}

public void SetKey(string \_key)

{

SetKey(\_key.Split(' '));

}

public string Encrypt(string input)

{

for (int i = 0; i < input.Length % key.Length; i++)

input += input[i];

string result = "";

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

{

char[] transposition = new char[key.Length];

for (int j = 0; j < key.Length; j++)

transposition[key[j] - 1] = input[i + j];

for (int j = 0; j < key.Length; j++)

result += transposition[j];

}

return result;

}

public string Decrypt(string input)

{

string result = "";

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

{

char[] transposition = new char[key.Length];

for (int j = 0; j < key.Length; j++)

transposition[j] = input[i + key[j] - 1];

for (int j = 0; j < key.Length; j++)

result += transposition[j];

}

return result;

}