Министерство науки и высшего образования Российской Федерации

Новосибирский Государственный технический университет

Кафедра автоматизированных систем управления



ОТЧЁТ

по лабораторной работе №2

по дисциплине «Защита информации»

«Шифрование методом замены (подстановки)»

Выполнили: Проверил:

Студенты гр. «АВТ-812», «АВТФ» к.т.н., доцент

Березин Дмитрий Качальский В.Г.

Бородина Алина

Глинин Евгений

«\_\_\_» \_\_\_\_\_\_ 20\_\_г. «\_\_\_» \_\_\_\_\_\_ 20\_\_ г.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись) (подпись)

г. Новосибирск

2021 г.

Содержание

[1 Цель работы 3](#_Toc85048237)

[2 Постановка задачи 3](#_Toc85048238)

[4 Преобразования исходного текста в криптограмму и обратно 5](#_Toc85048239)

[5 Примеры шифрования-дешифрования текста 6](#_Toc85048240)

[6 Выводы 8](#_Toc85048241)

[7 Листинг 9](#_Toc85048242)

# 1 Цель работы

Изучить методы шифрования и основные понятия криптографии. Реализовать программно шифр Виженера.

# 2 Постановка задачи

* Построить блок схему шифрующего и дешифрующего устройства.
* Записать математические уравнения прямого и обратного преобразования исходного текста в криптограмму и обратно, используя выражения и уравнения (7) - (9).
* Включить в алфавит буквы кириллицы и вспомогательные знаки. Провести 3-5 примеров шифрования-дешифрования текста.
* Написать программу шифрования-дешифрования на любом доступном Вам языке программирования c формированием загрузочного .exe файла
  + с клавиатуры произвольного текста;
  + с чтением и записью в текстовый файл.

**3 Блок схема шифрующего и дешифрующего устройства**

На рисунках 1-2 представлены алгоритмы шифрования и дешифрования.

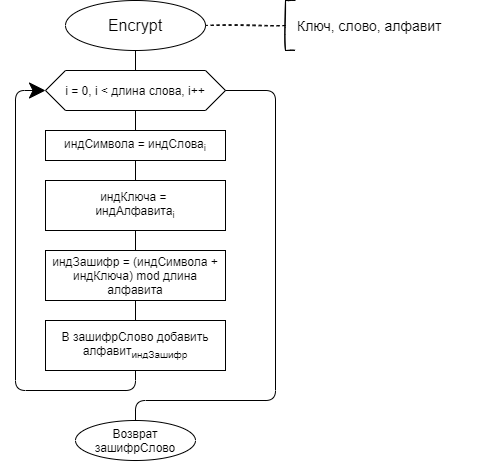


Рисунок 1 – Алгоритм шифрования Виженера

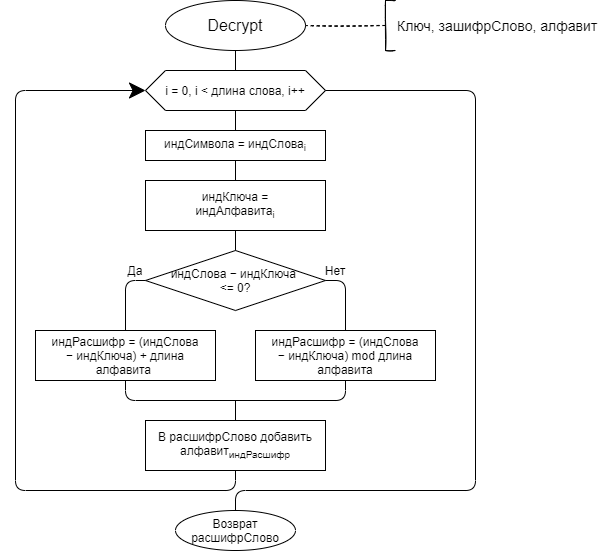


Рисунок 2 – Алгоритм дешифрования Виженера

# 4 Преобразования исходного текста в криптограмму и обратно

Рассмотрим шифрование с помощью таблицы Вижинера - квадратной матрицы с n2 элементами, где n - число символов используемого алфавита. В первой строке матрицы содержится исходный алфавит, каждая следующая строка получается из предыдущей циклическим сдвигом влево на один символ.

**Таблица Вижинера** для русского алфавита:

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

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

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

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

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

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

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

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

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

**…**

При шифровании символы из первой строки заменяются символами остальных строк по правилу

a(1,i) -> a(k,i), (7)

где k - номер используемой для шифрования строки.

Используя свойства циклического сдвига влево элементы k-ой строки можно выразить через элементы первой строки

|a(1,i+k-1), если i<=n-k+1

a(k,i)= | (8)

|a(1,i-n+k-1), если i>n-k+1

При дешифровании производится обратная замена

a(k,i) -> a(1,i). (9)

# 5 Примеры шифрования-дешифрования текста

* Ключ: абвгдеабвгдеабвгдеабвгдеабвгдеабвгдеабвгдеабвгдеабвгдеабвгдеабвгдеабвгдеабвгдеабвгдеабвгдеабвгде
* Текст: абвгдеабвгдеабвгдеабвгдеабвгдеабвгдеабвгдеабвгде
* Код: авджилавджилавджилавджилавджилавджилавджилавджил

На рисунках 3-4 представлены результаты работы программы.

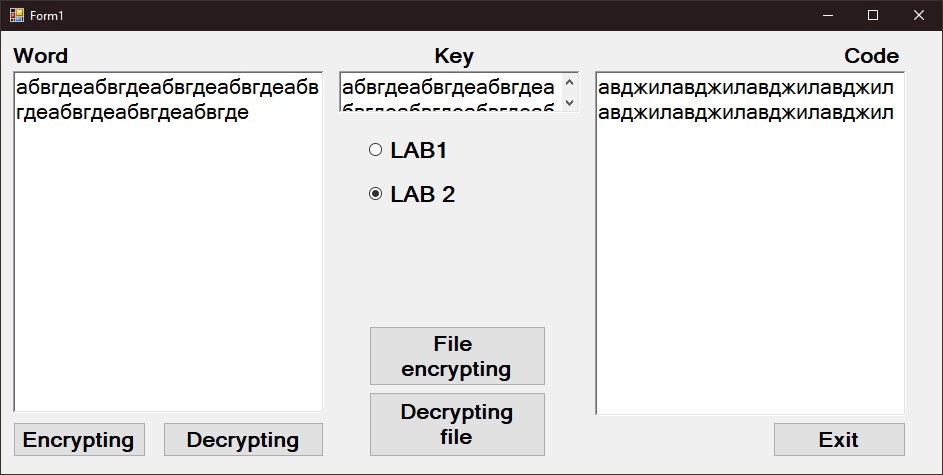


Рисунок 3 – Модель криптографической системы

* Ключ:едгвбаедгвбаедгвбаедгвбаедгвбаедгвбаедгвбаедгвбаедгвбаедгвбаедгвбаедгвбаедгвбаедгвбаедгвбаедгвбаедгвбаедгвба
* Текст: последнее преобразование записвается в виде
* Код: фтфнждтки ррлтдтбзужгпке мгсксздифтя ж дкдл

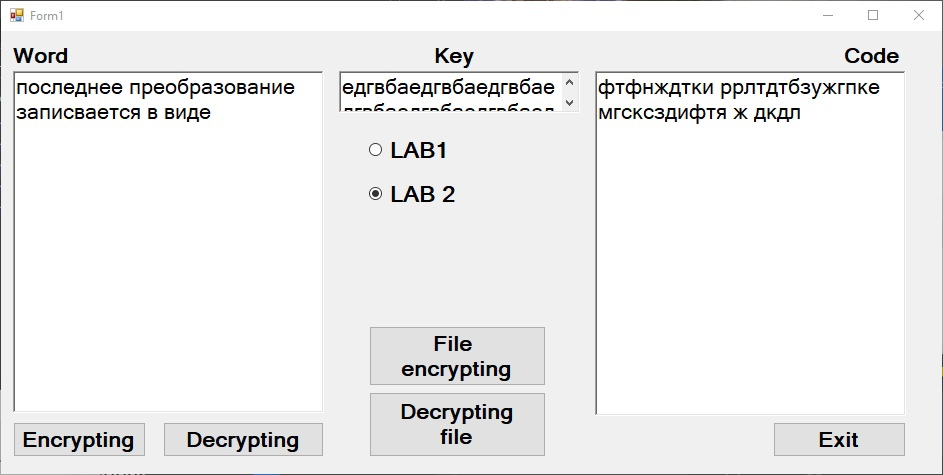


Рисунок 4 – Модель криптографической системы

На рисунке 6 представлен текстовый файл с исходной информацией.

На рисунке 7 представлен зашифрованный файл со следующим ключом:

тестшифрованияфайла.

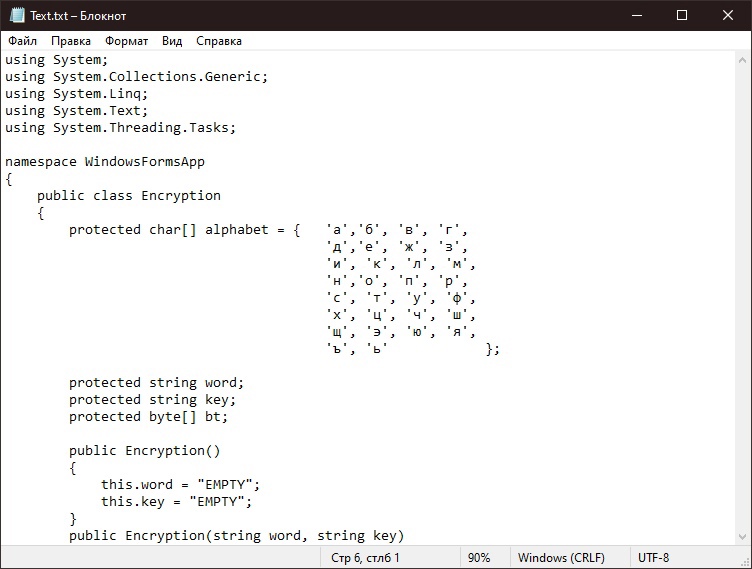


Рисунок 6 – Текстовый файл с исходной информацией

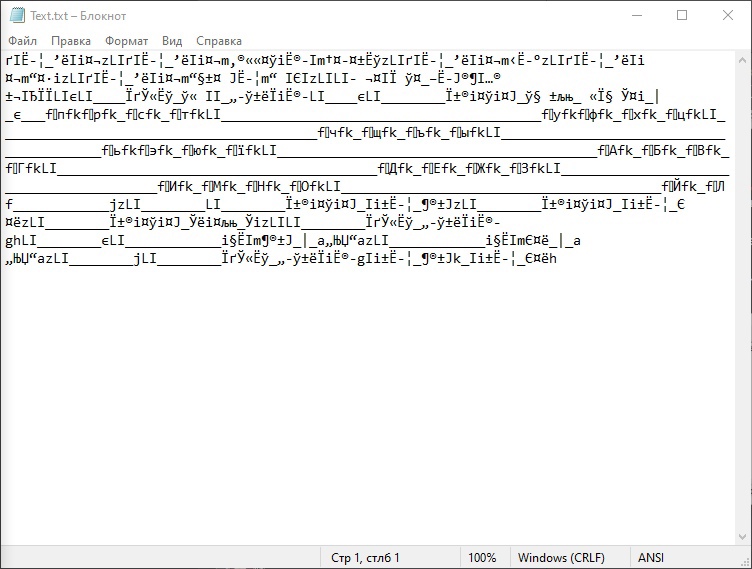


Рисунок 7 – Текстовый файл с зашифрованной информацией

# 6 Выводы

Изучили методы шифрования и основные понятия криптографии. Реализовали программно шифр Виженера на языке программирования C#.

# 7 Листинг

Encryption.cs

using System;

using System.Collections.Generic;

using System.Linq;

using System.Text;

using System.Threading.Tasks;

namespace WindowsFormsApp

{

public class Encryption

{

protected char[] alphabet = { 'а','б', 'в', 'г',

'д','е', 'ж', 'з',

'и', 'к', 'л', 'м',

'н','о', 'п', 'р',

'с', 'т', 'у', 'ф',

'х', 'ц', 'ч', 'ш',

'щ', 'э', 'ю', 'я',

'ъ', 'ь' };

protected string word;

protected string key;

protected byte[] bt;

public Encryption()

{

this.word = "EMPTY";

this.key = "EMPTY";

}

public Encryption(string word, string key)

{

this.word = word;

this.key = key;

}

public Encryption(byte[] bt, string key)

{

this.bt = bt;

this.key = key;

}

public string Encrypt()

{

int indexEncrypt = 0;

int indexWord;

int indexKey;

string encryptWord = "";

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

{

if(word[i] == ' ')

{

encryptWord += ' ';

continue;

} else if ((word[i] == '\r') && (word[i+1] == '\n'))

{

encryptWord += "\r\n";

continue;

}

indexWord = Array.IndexOf(alphabet, word[i]);

indexKey = Array.IndexOf(alphabet, key[i % key.Length]);

indexEncrypt = (indexWord + indexKey + 1) % alphabet.Length ;

encryptWord += alphabet[indexEncrypt];

}

return encryptWord;

}

public string EncryptTwo()

{

int indexEncrypt = 0;

int indexWord;

int indexKey;

string encryptWord = "";

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

{

if (word[i] == ' ')

{

encryptWord += ' ';

continue;

}

else if ((word[i] == '\r') && (word[i + 1] == '\n'))

{

encryptWord += "\r\n";

continue;

}

indexWord = Array.IndexOf(alphabet, word[i]);

indexKey = Array.IndexOf(alphabet, key[i % key.Length]);

indexEncrypt = (indexWord + indexKey) % alphabet.Length;

encryptWord += alphabet[indexEncrypt];

}

return encryptWord;

}

public string Decrypt()

{

int indexDecrypt = 0;

int indexText;

int indexKey;

string decryptWord = "";

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

{

if (word[i] == ' ')

{

decryptWord += ' ';

continue;

}else if ((word[i] == '\r') && (word[i + 1] == '\n'))

{

decryptWord += "\r\n";

continue;

}

indexText = Array.IndexOf(alphabet, word[i]);

indexKey = Array.IndexOf(alphabet, key[i % key.Length]);

if ((indexText - indexKey) <= 0)

{

indexDecrypt = (indexText - indexKey - 1) + alphabet.Length;

}

else

{

indexDecrypt = (indexText - indexKey - 1) % alphabet.Length;

}

decryptWord += alphabet[indexDecrypt];

}

return decryptWord;

}

public string DecryptTwo()

{

int indexDecrypt = 0;

int indexText;

int indexKey;

string decryptWord = "";

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

{

if (word[i] == ' ')

{

decryptWord += ' ';

continue;

}

else if ((word[i] == '\r') && (word[i + 1] == '\n'))

{

decryptWord += "\r\n";

continue;

}

indexText = Array.IndexOf(alphabet, word[i]);

indexKey = Array.IndexOf(alphabet, key[i % key.Length]);

if ((indexText - indexKey) <= 0)

{

indexDecrypt = (indexText - indexKey) + alphabet.Length;

}

else

{

indexDecrypt = (indexText - indexKey) % alphabet.Length;

}

decryptWord += alphabet[indexDecrypt % alphabet.Length];

}

return decryptWord;

}

public byte[] fileEncrypt()

{

byte[] keyInASCII = Encoding.ASCII.GetBytes(key);

byte[] indexEncrypt = new byte[bt.Length];

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

indexEncrypt[i] = Convert.ToByte((bt[i] + keyInASCII[i % keyInASCII.Length] + 1) % (Byte.MaxValue + 1));

return indexEncrypt;

}

public byte[] fileDecrypt()

{

byte[] keyInASCII = Encoding.ASCII.GetBytes(key);

byte[] indexDecrypt = new byte[bt.Length];

int indexByte;

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

{

if ((bt[i] - keyInASCII[i % keyInASCII.Length] - 1) < 0)

{

indexByte = bt[i] - keyInASCII[i % keyInASCII.Length] - 1;

indexDecrypt[i] = Convert.ToByte(indexByte + (Byte.MaxValue + 1));

}

else

{

indexByte = bt[i] - keyInASCII[i % keyInASCII.Length] - 1;

indexDecrypt[i] = Convert.ToByte(indexByte % (Byte.MaxValue + 1));

}

}

return indexDecrypt;

}

public byte[] fileEncryptTwo()

{

byte[] keyInASCII = Encoding.ASCII.GetBytes(key);

byte[] indexEncrypt = new byte[bt.Length];

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

indexEncrypt[i] = Convert.ToByte((bt[i] + keyInASCII[i % keyInASCII.Length]) % (Byte.MaxValue + 1));

return indexEncrypt;

}

public byte[] fileDecryptTwo()

{

byte[] keyInASCII = Encoding.ASCII.GetBytes(key);

byte[] indexDecrypt = new byte[bt.Length];

int indexByte;

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

{

if ((bt[i] - keyInASCII[i % keyInASCII.Length]) < 0)

{

indexByte = bt[i] - keyInASCII[i % keyInASCII.Length];

indexDecrypt[i] = Convert.ToByte(indexByte + (Byte.MaxValue + 1));

}

else

{

indexByte = bt[i] - keyInASCII[i % keyInASCII.Length];

indexDecrypt[i] = Convert.ToByte(indexByte % (Byte.MaxValue + 1));

}

}

return indexDecrypt;

}

}

}