Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра информатики

Дисциплина: Информационные сети. Основы безопасности

**ОТЧЕТ**

к лабораторной работе № 1

на тему «Шифр Цезаря»

Выполнил:

студент гр. 153504

Хрищанович А.К.

Проверил:

Лещенко Е.А.

Минск 2023

СОДЕРЖАНИЕ

[1 Постановка задачи 3](#_Toc146622147)

[2 Краткие теоретические сведения 4](#_Toc146622148)

[3 Результаты выполнения лабораторной работы 6](#_Toc146622149)

[Выводы 8](#_Toc146622150)

[Список использованных источников 9](#_Toc146622151)

[Приложение А (обязательное) Листинг кода 10](#_Toc146622152)

## 1 ПОСТАНОВКА ЗАДАЧИ

Целью выполнения лабораторной работы является изучения теоретических сведений о шифре Цезаря и шифре Виженера, а также создание программ, читающих данные из файла и шифрующие (дешифрующие) их с помощью шифра Цезаря и шифра Виженера.

## 2 КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

**2.1 Шифр Цезаря**

Шифр Цезаря, также известный, как шифр сдвига, код Цезаря или сдвиг Цезаря – один из самых простых и наиболее широко известных методов шифрования.

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 4 «А» была бы заменена на «Г», «Б» станет «Д», и так далее.

Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами.

Шаг шифрования, выполняемый шифром Цезаря, часто включается как часть более сложных схем, таких как шифр Виженера, и все ещё имеет современное приложение в системе ROT13. Как и все моноалфавитные шифры, шифр Цезаря легко взламывается и не имеет практически никакого применения на практике.



Рисунок 1 – Шифр Цезаря

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами модульной арифметики:

y=(x+k)\ \mod\ n

x=(y-k+n)\ \mod\ n,

где ~x – символ открытого текста, ~y – символ шифрованного текста, ~n – мощность алфавита, а ~k – ключ.

С точки зрения математики шифр Цезаря является частным случаем аффинного шифра.

**2.2 Шифр Виженера**

Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая tabula recta или квадрат (таблица) Виженера. Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 26 различных шифров Цезаря. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова. Например, предположим, что исходный текст имеет такой вид:

ATTACKATDAWN

Человек, посылающий сообщение, записывает ключевое слово («LEMON») циклически до тех пор, пока его длина не будет соответствовать длине исходного текста:

LEMONLEMONLE

Первый символ исходного текста A зашифрован последовательностью L, которая является первым символом ключа. Первый символ L шифрованного текста находится на пересечении строки L и столбца A в таблице Виженера. Точно так же для второго символа исходного текста используется второй символ ключа; то есть второй символ шифрованного текста X получается на пересечении строки E и столбца T. Остальная часть исходного текста шифруется подобным способом:

1 Исходный текст:  ATTACKATDAWN

2 Ключ:  LEMONLEMONLE

3 Зашифрованный текст: LXFOPVEFRNHR

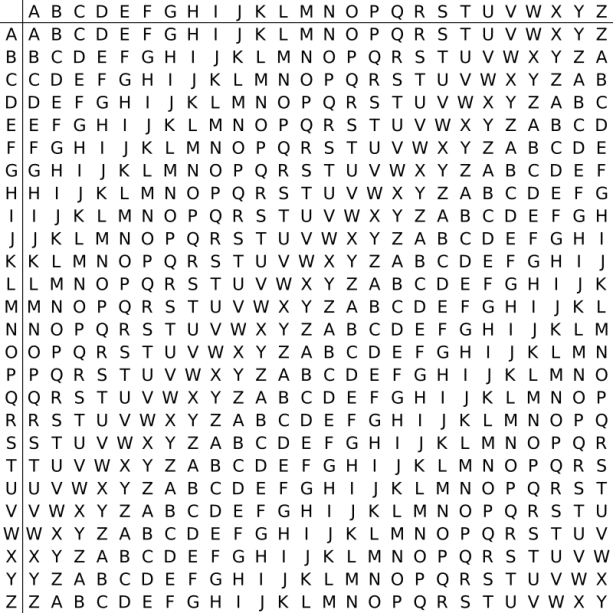


Рисунок 2 – Квадрат Виженера

Расшифровывание производится следующим образом: находим в таблице Виженера строку, соответствующую первому символу ключевого слова; в данной строке находим первый символ зашифрованного текста. Столбец, в котором находится данный символ, соответствует первому символу исходного текста. Следующие символы зашифрованного текста расшифровываются подобным образом.c j = m j + k j ( mod n )

m j = c j − k j ( mod n )

В компьютере такая операция соответствует сложению кодов ASCII символов сообщения и ключа по некоторому модулю. Кажется, что если таблица будет более сложной, чем циклическое смещение строк, то шифр станет надежнее. Это действительно так, если ее менять чаще, например, от слова к слову. Но составление таких таблиц, представляющих собой латинские квадраты, где любая буква встречается в строке или столбце один раз, трудоемко и его стоит делать лишь на ЭВМ. Для ручного же многоалфавитного шифра полагаются лишь на длину и сложность ключа, используя приведенную таблицу, которую можно не держать в тайне, а это упрощает шифрование и расшифровывание

## 3 РЕЗУЛЬТАТЫ ВЫПОЛНЕНИЯ ЛАБОРАТОРНОЙ             РАБОТЫ

В ходе выполнения лабораторной работы было разработано два консольных приложения, которые шифруют текст из файла при помощи шифра Цезаря и шифра Виженера. Блок схемы алгоритмов, реализующих шифр Цезаря и шифр Виженера, представлены в приложения Б и В соответственно.

**3.1 Шифрование (дешифрование) текста при помощи шифра Цезаря**

При запуске программы пользователю предоставляется текст из файла, который находится в корневой папке программы. Пользователь может ввести ключ, по которому будет происходить сдвиг и который является числом. Ключ может быть как положительным, так и отрицательным. При положительном ключе сдвиг будет происходить вправо на указанное число позиций. При отрицательном ключе сдвиг будет происходить влево. Результат работы программы предоставлен на рисунке 3.1.

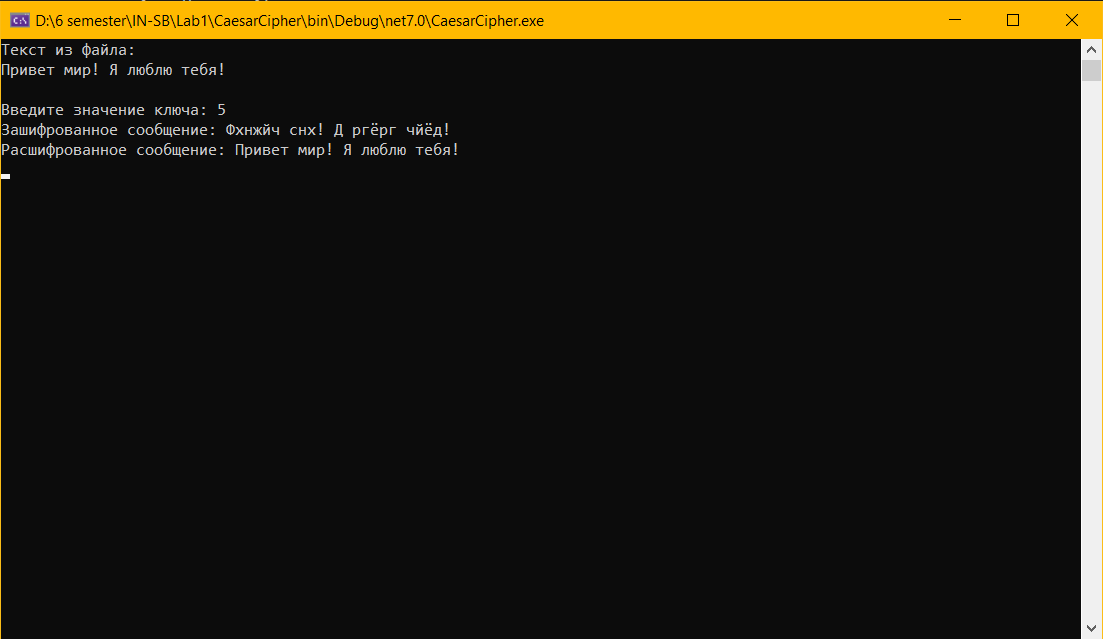


Рисунок 3.1 – Результат работы программы, реализующей шифр Цезаря

**3.2 Шифрование (дешифрование) текста при помощи   
                шифра Виженера**

При запуске программы пользователю предоставляется текст из файла, который находится в корневой папке программы. Пользователь может ввести ключ, который является словом или набором символов. Результат работы программы представлен на рисунке 3.2.

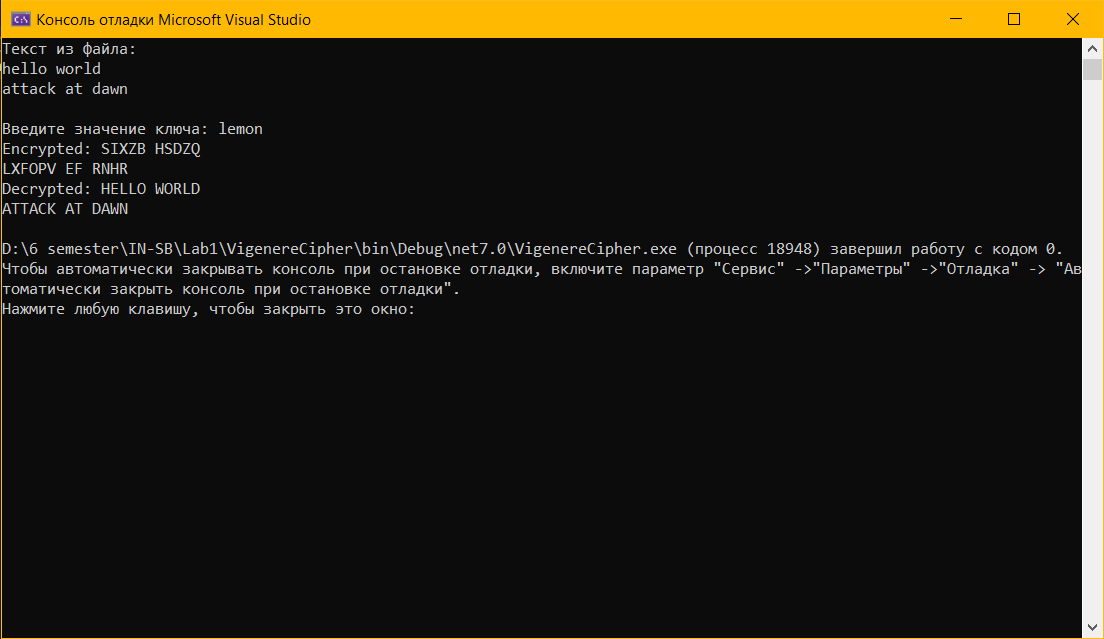


Рисунок 3.2 – Результат работы программы, реализующей шифр Виженера

## ВЫВОДЫ

В ходе выполнения лабораторной работы были изучены теоретические сведения о шифре Цезаря и шифре Виженера, а также были созданы программы, читающие данные из файла и шифрующие (дешифрующие) из с помощью шифры Цезаря и шифра Виженера.

**ПРИЛОЖЕНИЕ А**

## (обязательное)

## Листинг кода

Листинг 1 – Программный код алгоритма шифра Цезаря

public class CaesarCipher

{

const string alfabet = "АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ";

private string CodeEncode(string text, int k)

{

var fullAlfabet = alfabet + alfabet.ToLower();

var letterQty = fullAlfabet.Length;

var retVal = "";

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

{

var c = text[i];

var isUpper = Char.IsUpper(c);

var index = fullAlfabet.IndexOf(Char.ToUpper(c));

if (index < 0)

{

retVal += c.ToString();

}

else

{

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

retVal += isUpper ? Char.ToUpper(fullAlfabet[codeIndex]) : Char.ToLower(fullAlfabet[codeIndex]);

}

}

return retVal;

}

public string Encrypt(string plainMessage, int key)

=> CodeEncode(plainMessage, key);

public string Decrypt(string encryptedMessage, int key)

=> CodeEncode(encryptedMessage, -key);

}

class Program

{

static void Main(string[] args)

{

var cipher = new CaesarCipher();

// Чтение текста из файла

string encryptedText;

try

{

encryptedText = File.ReadAllText(@"D:\6 semester\IN-SB\Lab1\CaesarCipher\encryptedtext.txt");

}

catch (IOException e)

{

Console.WriteLine("Ошибка при чтении файла: " + e.Message);

return;

}

Console.WriteLine("Текст из файла:");

Console.WriteLine(encryptedText);

Console.WriteLine();

Console.Write("Введите значение ключа: ");

var secretKey = Convert.ToInt32(Console.ReadLine());

var encryptedMessage = cipher.Encrypt(encryptedText, secretKey);

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

Console.WriteLine("Расшифрованное сообщение: {0}", cipher.Decrypt(encryptedMessage, secretKey));

Console.ReadLine();

}

}

Листинг 2 – Программный код алгоритма шифра Виженера

class VigenereCipher

{

static char EncryptChar(char plainChar, char keyChar)

{

if (!char.IsLetter(plainChar))

return plainChar;

char baseChar = 'A';

return (char)(((plainChar + keyChar - 2 \* baseChar) % 26) + baseChar);

}

static char DecryptChar(char cipherChar, char keyChar)

{

if (!char.IsLetter(cipherChar))

return cipherChar;

char baseChar = 'A';

int result = ((cipherChar - keyChar + 26) % 26) + baseChar;

return (char)result;

}

public static string Encrypt(string plaintext, string key)

{

plaintext = plaintext.ToUpper();

key = key.ToUpper();

string encryptedText = "";

int keyIndex = 0;

foreach (char c in plaintext)

{

if (char.IsWhiteSpace(c))

{

encryptedText += c;

continue;

}

char keyChar = key[keyIndex];

encryptedText += EncryptChar(c, keyChar);

keyIndex = (keyIndex + 1) % key.Length;

}

return encryptedText;

}

public static string Decrypt(string ciphertext, string key)

{

ciphertext = ciphertext.ToUpper();

key = key.ToUpper();

string decryptedText = "";

int keyIndex = 0;

foreach (char c in ciphertext)

{

if (char.IsWhiteSpace(c))

{

decryptedText += c;

continue;

}

char keyChar = key[keyIndex];

decryptedText += DecryptChar(c, keyChar);

keyIndex = (keyIndex + 1) % key.Length;

}

return decryptedText;

}

static void Main()

{

string encryptedText;

try

{

encryptedText = File.ReadAllText(@"D:\6 semester\IN-SB\Lab1\VigenereСipher\encryptedtext.txt");

}

catch (IOException e)

{

Console.WriteLine("Ошибка при чтении файла: " + e.Message);

return;

}

Console.WriteLine("Текст из файла:");

Console.WriteLine(encryptedText);

Console.WriteLine();

Console.Write("Введите значение ключа: ");

var secretKey = Console.ReadLine();

string ciphertext = Encrypt(encryptedText, secretKey);

Console.WriteLine("Encrypted: " + ciphertext);

string decryptedText = Decrypt(ciphertext, secretKey);

Console.WriteLine("Decrypted: " + decryptedText);

}

}

**ПРИЛОЖЕНИЕ Б**

**(обязательное)**

**Блок схема алгоритма, реализующего шифр Цезаря**



**ПРИЛОЖЕНИЕ В**

**(обязательное)**

**Блок схема алгоритма, реализующего шифр Виженера**

