Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

Кафедра информатики

Отчет по лабораторной работе №1

Шифр Цезаря. Шифр Виженера.

Выполнил: Студент гр. 853503

Яговдик О.И.

Проверил: Протько М.И.

Минск 2021

**Шифр Цезаря.**

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

Формула шифра

*Y = (x + k) mod n,*

*X = (y – k) mod n*

где {\displaystyle x}x  — символ открытого текста, {\displaystyle y}y — символ шифрованного текста, {\displaystyle n}n — мощность алфавита, а {\displaystyle k}k — ключ.

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

Шифрование с использованием ключа {\displaystyle k=3}. Буква «Е» «сдвигается» на три буквы вперёд и становится буквой «З». Твёрдый знак, перемещённый на три буквы вперёд, становится буквой «Э», буква «Я», перемещённая на три буквы вперёд, становится буквой «В», и так далее:

Исходный 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

Шифрованный: 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

Оригинальный текст:

Съешь же ещё этих мягких французских булок, да выпей чаю.

Шифрованный текст получается путём замены каждой буквы оригинального текста соответствующей буквой шифрованного алфавита:

Фэзыя йз зьи ахлш пвёнлш чугрщцкфнлш дцосн, жг еютзм ъгб.

**Шифр Виженера**

Шифр Виженера — метод полиалфавитного шифрования буквенного текста с использованием ключевого слова

В шифре Цезаря каждая буква алфавита сдвигается на несколько позиций; например в шифре Цезаря при сдвиге +3, A стало бы D, B стало бы E и так далее. 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 зашифрованного текста ("L") 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 зашифрованного текста ("X") получается на пересечении строки E и столбца T. Остальная часть исходного текста шифруется подобным способом.

Исходный текст: ATTACKATDAWN

Ключ: LEMONLEMONLE

Зашифрованный текст: LXFOPVEFRNHR

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.

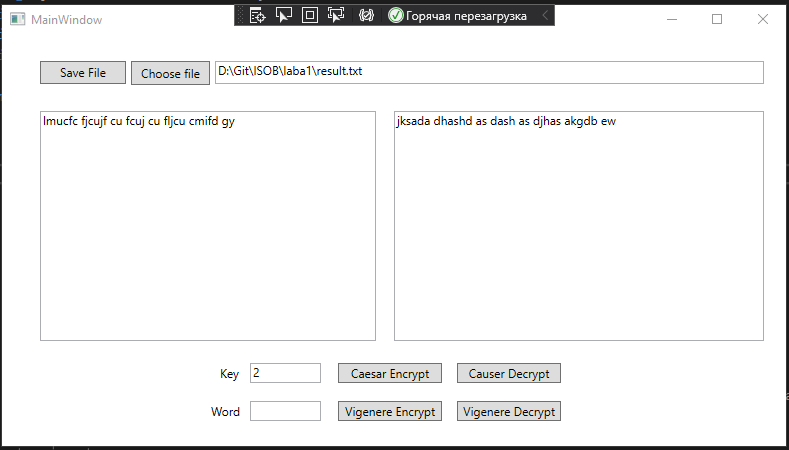
Если {\displaystyle n}n — количество букв в алфавите, {\displaystyle m\_{j}}mj — буквы открытого текста, {\displaystyle k\_{j}}kj — буквы ключа, то шифрование Виженера можно записать следующим образом:

Cj = (mj + kj) mod n

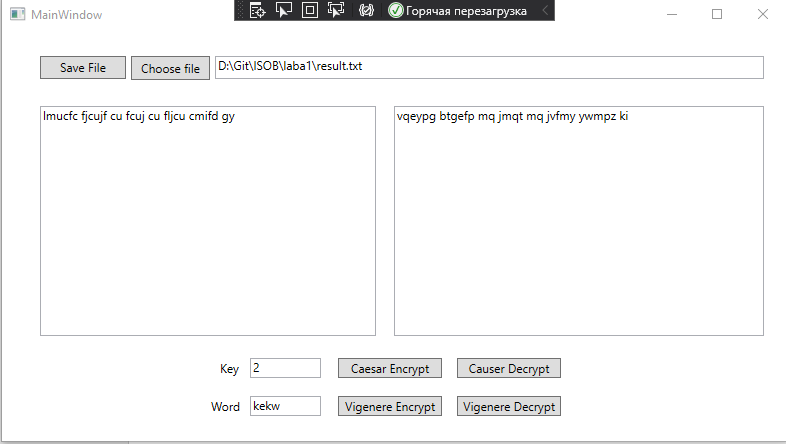
Mj = (cj + n – k) mod n

**Результат выполнения программы**

1. Шифр Цезаря



1. Шифр Виженера



**Вывод.**

В данной лабораторной работе познакомился с методами шифрования (декодирования) Цезаря и Виженера. Изучил алгоритмы методов шифрования и дешифрования текстовых файлов Шифра Цезаря, (шифра сдвига, кода Цезаря) и шифра Виженера и научился реализовать программные средства шифрования и дешифрования текстовых файлов. Изучил основные особенности, преимущества и недостатки Шифра Цезаря и Шифра Виженера. 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. 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. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова. Общим недостатком Шифра Цезаря и Шифра Виженера является то, что его достаточно легко взломать, как и все многоалфавитные шифры, зная лишь зашифрованный текст. Именно поэтому они редко применяются в наше время.

**Код программы.**

using System;

using System.Collections.Generic;

using System.Linq;

using System.Text;

using System.Threading.Tasks;

namespace laba1.Model

{

class Сiphers

{

private const int PowerAlhabet = 'z' - 'a' + 1;

public static string CauserEncrypt(string inputText, int key)

{

StringBuilder stringBuilder = new StringBuilder();

inputText = inputText.ToLower();

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

{

if (CheckSymbol(inputText[i]))

{

stringBuilder.Append((char)((inputText[i] - 'a' + key) % PowerAlhabet + 'a'));

}

else

{

stringBuilder.Append(inputText[i]);

}

}

return stringBuilder.ToString();

}

public static string CauserDecrypt(string inputText, int key)

{

StringBuilder stringBuilder = new StringBuilder();

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

{

if (CheckSymbol(inputText[i]))

{

stringBuilder.Append((char)((inputText[i] - 'a' - key + PowerAlhabet) % PowerAlhabet + 'a'));

}

else

{

stringBuilder.Append(inputText[i]);

}

}

return stringBuilder.ToString();

}

public static string VigenereEncrypt(string inputText, string word)

{

StringBuilder stringBuilder = new StringBuilder();

word = word.ToLower();

inputText = inputText.ToLower();

for (int i = 0, j = 0; i < inputText.Length; i++, j++)

{

if (j == word.Length)

{

j = 0;

}

if (CheckSymbol(inputText[i]))

{

stringBuilder.Append((char)((inputText[i] + word[j] - 2 \* 'a') % PowerAlhabet + 'a'));

}

else

{

stringBuilder.Append(inputText[i]);

}

}

return stringBuilder.ToString();

}

public static string VigenereDecrypt(string inputText, string word)

{

StringBuilder stringBuilder = new StringBuilder();

word = word.ToLower();

inputText = inputText.ToLower();

for(int i = 0, j = 0; i < inputText.Length; i++, j++)

{

if (j == word.Length)

{

j = 0;

}

if (CheckSymbol(inputText[i]))

{

stringBuilder.Append((char)((inputText[i] - word[j] + PowerAlhabet) % PowerAlhabet + 'a'));

}

else

{

stringBuilder.Append(inputText[i]);

}

}

return stringBuilder.ToString();

}

private static bool CheckSymbol(char symbol)

{

switch (symbol)

{

case ' ':

case ',':

case '.':

case ':':

case '-':

case '\r':

case '\n':

return false;

default:

return true;

}

}

}

}