Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

Кафедра информатики

Отчет по лабораторной работе №1

Шифр Цезаря. Шифр Виженера.

Выполнил:

студент гр. 953501

Кондрашов И.Д.

Проверил:

ассистент кафедры информатики

Протько М.И.

Минск 2022

**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

Блок-схема выполнения алгоритма шифра Цезаря:

A picture containing diagram

Description automatically generated

Блок-схема выполнения алгоритма шифра Виженера:

Diagram

Description automatically generated

**Результат выполнения программы**

1. Шифр Цезаря

A screenshot of a computer

Description automatically generated with medium confidence

1. Шифр Виженера

Text

Description automatically generated

**Вывод.**

В данной лабораторной работе ознакомился с методами шифрования (декодирования) Цезаря и Виженера. Изучил и предоставил реализацию алгоритмов методов шифрования и дешифрования текстовых файлов Шифра Цезаря и Виженера на языке программирования C#. 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.**

static string Caesar(string message, int key)

{

string lowerEnAlphabet = enAlphabet.ToLower();

string fullEnAlphabet = enAlphabet + lowerEnAlphabet;

int alphabetAmount = fullEnAlphabet.Length;

string result = "";

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

{

char letter = message[i];

int letterIndex = fullEnAlphabet.IndexOf(letter);

if(letterIndex >= 0)

{

//если индекс найден, то шифруем его

var codedIndex = (alphabetAmount + letterIndex + key) % alphabetAmount;

result += fullEnAlphabet[codedIndex];

}

else

{

//если индекса нет, то так его и добавляем без шифрования

result += letter.ToString();

}

}

return result;

}

static string VigenerEncode(string inputText, string password)

{

string result = "";

int alphabetCount = enAlphabet.Length;

inputText = inputText.ToUpper();

var message = inputText.Trim(new char[] { '\r' });

password = password.ToUpper();

int passwordIndex = 0;

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

{

//Находим позицию буквы из сообщения в алфавите, затем буквы из пароля в алфавите

int position = (enAlphabet.IndexOf(inputText[i]) + enAlphabet.IndexOf(password[passwordIndex])) % alphabetCount;

result += enAlphabet[position];

passwordIndex++;

//Обнуляем индекс, если он достигает длины пароля

if(passwordIndex == password.Length)

{

passwordIndex = 0;

}

}

return result;

}

static string VigenerDecode(string mes, string pas)

{

string res = "";

mes = mes.ToUpper();

pas = pas.ToUpper();

int pasIndex = 0;

int alphCount = enAlphabet.Length;

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

{

int pos = (enAlphabet.IndexOf(mes[i]) + alphCount - enAlphabet.IndexOf(pas[pasIndex])) % alphCount;

res += enAlphabet[pos];

pasIndex++;

if(pasIndex == pas.Length)

{

pasIndex = 0;

}

}

return res;

}