МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

Кафедра «Информатики и систем управления»

ОТЧЕТ

по лабораторной работе № 1 «Биграммный шифр Плейфера»

по дисциплине

Методы и средства защиты информации

ПРЕПОДАВАТЕЛЬ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Капранов С.Н. (подпись) (фамилия, и.,о.)

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Гореев А.Д. (подпись) (фамилия, и.,о.)

19-ИСТ-2

(шифр группы)

Работа защищена «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_

С оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Нижний Новгород

2021

**Задача № 1.7** Реализовать алгоритм шифрования данных «Биграммный шифр Плейфейра».

Описание алгоритма:

Биграммный шифр Плейфейра предназначен для шифрования сообщений парами букв. Правила, необходимые для шифрования этим методом:

1. Входной текст должен иметь четное число букв
2. Если в результате разбиения на биграммы попались в парах одинаковые буквы, то второй элменет биграммы заменяется на каку-то другую букву. В моем примере это буква английского алфавита «X»
3. Если обе буквы биграммы исходного текста не лежат в одной строке или в одном столбце, тогда находят буквы в углах прямоугольника, определяемого данной парой букв.
4. Если обе буквы биграммы открытого текста принадлежат одной строке таблицы, то первой и второй буквами биграммы считаются буквы, лежащие справа, соответственно, от первой и второй букв биграммы открытого текста.
5. Если обе буквы биграммы открытого текста принадлежат одному столбцу таблицы, то первой и второй буквами биграммы считаются буквы, лежащие, соответственно, под первой и под второй буквами биграммы открытого текста.

**Листинг программы**

#include <iostream>

#include <vector>

using namespace std;

//Размерность алфавита

const int rowAbc = 5;

const int colAbc = 5;

//КОДОВОЕ СЛОВО TABLE

const char abc[rowAbc][colAbc] = {

{'T','A','B','L','E'},

{'C','D','F','G','H'},

{'I','K','M','N','O'},

{'P','Q','R','S','U'},

{'V','W','X','Y','Z'},

};

//Ввод текста с клавиатуры

void getText(vector<char>& text)

{

puts( "Enter the text you want to encode");

char symbol;

while(true)

{

symbol = getchar();

if (symbol >= (int)'a' && symbol <= (int)'z')

symbol -= 'a' - 'A';

else if (symbol == ' ')

continue;

else if (symbol == 'J')

text.push\_back('I');

else if(symbol == '\n')

break;

text.push\_back(symbol);

}

}

//Преобразование текста

void convertionString(vector<char>& text, vector<char>& message)

{

int countT = 0;

int countM = 0;

while (countT < text.size())

{

message.push\_back(text[countT]);

countT++;

//Если число элементов нечетное

if (countT == text.size())

{

message.push\_back('X');

break;

}

//Повтор символа

if (text[countT] == message[countM])

{

message.push\_back('X');

countM++;

countT++;

}

else

{

countM++;

message.push\_back(text[countT]);

countT++;

}

countM++;

}

}

//Поиск позиции элемента

void getPossition(char symbol, int& row, int& col)

{

for(auto i = 0; i<colAbc;i++)

{

for(auto j = 0; j<rowAbc ;j++)

{

if (symbol == abc[i][j])

{

row = i;

col = j;

}

}

}

}

//Если элементы находятся в одной строке

void encodingRow(int row, int colFirst, int colSecond, vector<char>& bigram)

{

bigram.push\_back(abc[row][(colFirst + 1)%5]);

bigram.push\_back(abc[row][(colSecond + 1)%5]);

}

//Элементы находятся в одном столбце

void encodingCol(int col, int rowFirst, int rowSecond, vector<char>& bigram)

{

bigram.push\_back(abc[(rowFirst + 1) % 5][col]);

bigram.push\_back(abc[(rowSecond+1) % 5][col]);

}

//Элементы находятся в разных строках и столбца

void encodingRowCol( int rowFirst, int rowSecond, int colFirst, int colSecond, vector<char>& bigram)

{

bigram.push\_back(abc[rowFirst][colSecond]);

bigram.push\_back(abc[rowSecond][colFirst]);

}

//Шифрование текста

void textEncryption(vector<char> mes, int len)

{

vector<char> text;

int i = 0;

int rowFirst = 0;

int rowSecond = 0;

int colFirst = 0;

int colSecond = 0;

//Группировка букв по парам

while (i < len)

{

//Поиск позицию первого элемента биграммы

getPossition(mes[i], rowFirst, colFirst);

i++;

//Поиск позиции второго элемента биграммы

getPossition(mes[i], rowSecond, colSecond);

//Находятся в одной строке

if (rowFirst == rowSecond)

encodingRow(rowFirst, colFirst, colSecond, text);

//В одном столбце

else if (colFirst == colSecond)

encodingCol(colFirst, rowFirst, rowSecond, text);

else

encodingRowCol(rowFirst, rowSecond, colFirst, colSecond, text);

i++;

}

puts("Encoded text");

//Вывод зашифрованного текста

for (char elem : text)

{

putchar(elem);

}

}

int main()

{

setlocale(LC\_ALL, "ru");

vector<char> text;

vector<char> message;

getText(text);

convertionString(text, message);

int length = message.size();

textEncryption(message, length);

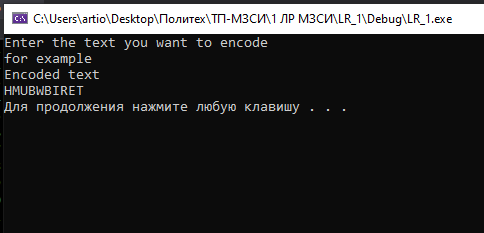
cout << endl;

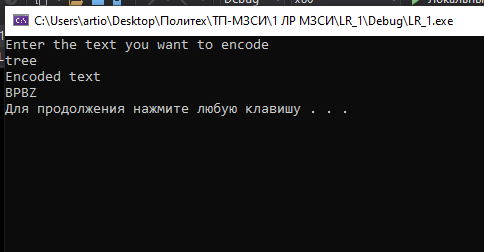
system("pause");

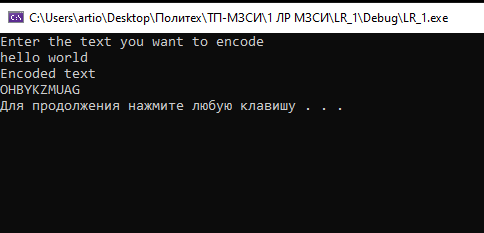
return 0;

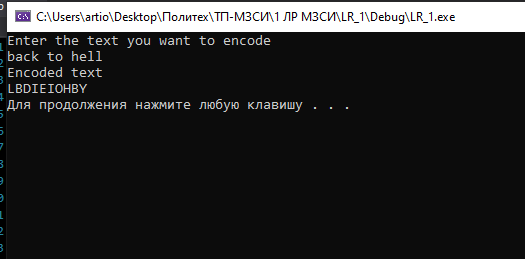
}

**Примеры работы программы**

****

****

****

****