Министерство образования Российской Федерации

Пензенский государственный университет

Кафедра «Вычислительная техника»

**ОТЧЕТ**

по курсу **«Защита информации в сети Internet»**

по лабораторной работе №1

на тему «**Разработка программы шифрования/дешифрования текста с использованием перестановочного шифра**»

Выполнили  
студенты группы 18ВВ1:  
 Кривозубов А. К.

Махров А. А.

Приняли:  
к.т.н., доцент Дубравин А.В.

Пенза 2020

**Цель работы:** Изучение шифрования и расшифровывания произвольного текстового файла с использованием перестановочного шифра используя, в качестве ключа последовательность, соответствующую номеру варианта.

**Задание:**

Разработать программу, выполняющую шифрование и расшифровывание произвольного текстового файла с использованием перестановочного шифра используя в качестве ключа последовательность, соответствующую номеру варианта. Выполнить проверку путем двоичного сравнения исходного файла и файла, полученного после расшифровывания.

|  |  |
| --- | --- |
| Номер варианта | Последовательность перестановки |
| 6 | 2 5 9 3 4 10 1 7 6 8 |

**Листинг программы:**

#include <iostream>

#include <fstream>

#include <vector>

#include <conio.h>

using namespace std;

bool filecompare(ifstream &first, ifstream &second)

{

char ch1 = 0, ch2;

while (ch1 != EOF)

{

ch1 = first.get(); ch2 = second.get();

if (ch1 != ch2) return false;

}

return true;

}

void encryption(int key[]) {

char buffer;

char space = { ' ' };

vector <char> v1, v2;

ifstream fin("Text1.txt", ios::binary);

int c, j = 0, a = 0;

while (fin.get(buffer)) {

v1.push\_back(buffer);

}

fin.close();

c = 10 - v1.size() % 10;

if (c != 10) {

for (int i = 0; i < c; i++) {

v1.push\_back(space);

}

}

for (int i = 0; i < v1.size(); i++) {

v2.push\_back(v1[j + key[a] - 1]);

if (a > 8) {

a = 0;

j = j + 10;

}

else {

a++;

}

}

ofstream fout("Result.txt", ios\_base::trunc | ios::binary);

for (int i = 0; i < v2.size(); i++) {

fout << v2[i];

}

fout.close();

}

void decryption(int key[]) {

char buffer;

char space = { ' ' };

vector <char> v1, v2;

ifstream fin("Result.txt", ios::binary);

int c, j = 0, a = 0;

int filesize = 0;

while (fin.get(buffer)) {

v1.push\_back(buffer);

}

fin.close();

c = 10 - v1.size() % 10;

if (c != 10) {

for (int i = 0; i < c; i++) {

v1.push\_back(space);

}

}

v2.resize(v1.size());

for (int i = 0; i < v1.size(); i++) {

v2[j + key[a] - 1] = v1[i];

if (a > 8) {

a = 0;

j = j + 10;

}

else {

a++;

};

}

ifstream fin2("Text1.txt", ios::binary);

while (fin2.get(buffer)) {

filesize++;

}

fin2.close();

ofstream fout("Text2.txt", ios\_base::trunc | ios::binary);

for (int i = 0; i < filesize; i++) {

fout << v2[i];

}

fout.close();

//---Сравнение---

ifstream first ("Text1.txt", ios::binary);

ifstream second ("Text2.txt", ios::binary);

if (filecompare(first, second)) {

cout << "Файлы одинаковы!" << endl;

}

else {

cout << "Файлы не совпали!" << endl;

}

}

void menu() {

char ch\_key;

int c, key[] = { 2, 5, 9, 3, 4, 10, 1, 7, 6, 8 };

cout << "1 - Зашифровать файл" << endl;

cout << "2 - Расшифровать файл" << endl;

cout << "ESC - Выйти" << endl;

switch (ch\_key = \_getch())

{

case '1':

cout << "Шифрование файла..." << endl;

encryption(key);

cout << "Файл зашифрован" << endl;

system("pause");

break;

case '2':

cout << "Дешифрование файла..." << endl;

decryption(key);

cout << "Файл расшифрован" << endl;

system("pause");

break;

case 27:

cout << "Exit from program\n";

exit(0);

break;

default:

break;

}

}

int main()

{

setlocale(LC\_ALL, "Russian");

while (true) {

system("cls");

menu();

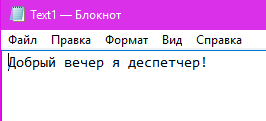
}

system("pause");

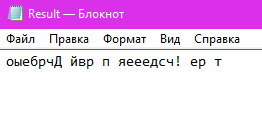
}

**Результат работы программы:**

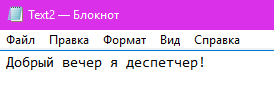
Исходный файл:

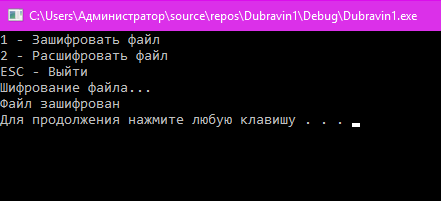


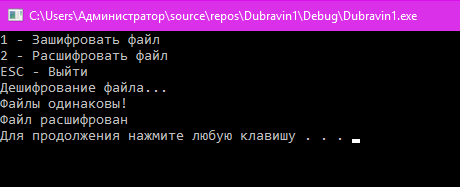
Закодированный файл:

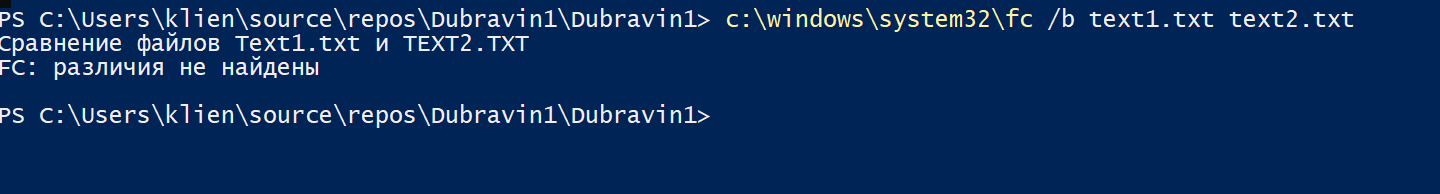


Раскодированный файл:







****

**Вывод:** Мы изучили, шифрование и расшифровывание произвольного текстового файла с использованием перестановочного шифра используя, в качестве ключа последовательность, соответствующая номеру варианта.