Министерство науки и высшего образования Российской Федерации

Пензенский государственный университет

Кафедра «Вычислительная техника»

**ОТЧЕТ**

по лабораторной работе №1

по курсу «Защита информации в сети Internet»

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

Выполнили  
студенты группы 18ВВ1:

Ручкин М.А.

Коновалова Д.А.

Дубинин А.В.

Приняли:

к.т.н., доцент Дубравин А.В.

к.т.н., доцент Карамышева Н.С.

2020

**Цель работы:** разработать программу шифрования/дешифрирования текста с использованием перестановочного шифра.

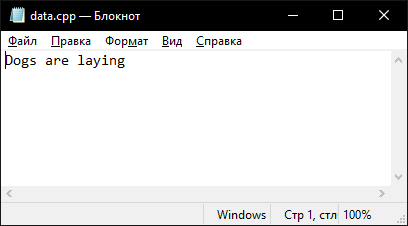
**Задания:** разработать программу, выполняющую шифрование и расшифровывание произвольного текстового файла с использованием перестановочного шифра используя в качестве ключа последовательность, соответствующую номеру варианта. Выполнить проверку путем двоичного сравнения исходного файла и фала, полученного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

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

Работа программы:

Для осуществления шифрования и расшифровывания необходимо создать текстовый файл, где будет отображена последовательность перестановки. Также нужно создать файл, над которым будет проводиться шифрование.

Для демонстрации работы программы создали следующий текстовый файл:



Вывод программы:



Листинг:

#include <stdio.h>

#include <string.h>

#include <locale.h>

#include <conio.h>

#include <malloc.h>

int ReadText(char\* &text, char\* fileName)

{

FILE \*data;

data = fopen(fileName, "rb");

fseek(data, 0, SEEK\_END);

int size = ftell(data);

text = (char\*)malloc(size \* sizeof(char));

fseek(data, 0, SEEK\_SET);

fread(text, 1, size, data);

fclose(data);

return size;

}

void WriteText(char\* text, int size, char\* fileName)

{

FILE \*data;

data = fopen(fileName, "wb");

fwrite(text, 1, size, data);

fclose(data);

}

int OptText()

{

char\* ntext;

FILE \*data;

char\* text;

int length\_text = ReadText(text, "data.cpp");

while (length\_text % 10 != 0)

{

ntext = (char\*)malloc((length\_text) \* sizeof(char));

for (int i = 0; i < (length\_text); i++)

{

ntext[i] = text[i];

}

free(text);

length\_text++;

text = (char\*)malloc((length\_text) \* sizeof(char));

for (int i = 0; i < (length\_text - 1); i++)

{

text[i] = ntext[i];

}

free(ntext);

text[length\_text - 1] = ' ';

}

ntext = (char\*)malloc((length\_text) \* sizeof(char));

for (int i = 0; i < (length\_text); i++)

{

ntext[i] = text[i];

}

free(text);

length\_text++;

text = (char\*)malloc((length\_text) \* sizeof(char));

for (int i = 0; i < (length\_text - 1); i++)

{

text[i] = ntext[i];

}

free(ntext);

text[length\_text - 1] = '\0';

printf("Initial text: \n");

printf(text);

printf("\n\n");

int loop = length\_text / 10;

WriteText(text, length\_text, "data.txt");

free(text);

return loop;

}

void getKey(char key[])

{

int i = 0;

FILE\* dataKey;

dataKey = fopen("key.txt", "r");

for (i = 0; i < 10; i++)

fscanf(dataKey, "%d", &key[i]);

fclose(dataKey);

}

void Encryption(char key[], int loop)

{

int i, j;

int start = 0;

char\* ntext;

char\* text;

int size = ReadText(text, "data.txt");

ntext = (char\*)malloc(size \* sizeof(char));

for (j = 0; j < loop; j++) {

for (i = start; i < start + 10; i++) {

ntext[i] = text[key[i - start] + start - 1];

}

start = start + 10;

}

free(text);

ntext[i] = '\0';

WriteText(ntext, size, "encrypted.txt");

printf("Encrypted text: \n");

printf(ntext);

printf("\n\n");

free(ntext);

}

void Decryption(char key[], int loop)

{

int i, j;

int n = 0;

int start = 0;

int loopQ = loop;

char\* ntext;

int size = ReadText(ntext, "encrypted.txt");

char\* revntext = (char\*)malloc(size \* sizeof(char));

while (loopQ != 0) {

for (i = start; i < start + 10; i++) {

for (j = 0; j < 10; j++) {

if ((i % 10) == (key[j] - 1))

revntext[i] = ntext[j + n];

}

}

start += 10;

loopQ--;

n += 10;

}

free(ntext);

revntext[i] = '\0';

printf("Final text: \n");

printf(revntext);

printf("\n\n");

WriteText(revntext, size, "decrytped.txt");

free(revntext);

}

void ErrorTest()

{

int s1, s2;

int alarm = 0;

FILE \*data, \*ddata;

data = fopen("data.txt", "r");

ddata = fopen("decrytped.txt", "r");

while (!feof(ddata) && !feof(data)) {

s1 = fgetc(data);

s2 = fgetc(ddata);

if (s1 != s2)

{

alarm = 1;

}

}

if (alarm != 1)

printf("Files are the same");

else

printf("Files are defferent");

fclose(data);

fclose(ddata);

}

int main()

{

char key[10];

// Read text

int loop = OptText();

// Read key

getKey(key);

//Encryption

Encryption(key, loop);

//Decryption

Decryption(key, loop);

//Comparison

ErrorTest();

getch();

}

Вывод: разработали программу шифрования/дешифрирования текста с использованием перестановочного шифра.