Министерство науки и высшего образования Российской Федерации

Пензенский государственный университет

Кафедра «Вычислительная техника»

**ОТЧЕТ**

по лабораторной работе №2

по курсу «Защита информации в сети Internet»

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

Выполнили  
студенты группы 18ВВ1:

Гросс Д.А

Репин И.А

Щербакова К.А

Приняли:

к.т.н., доцент Дубравин А.В.

к.т.н., доцент Карамышева Н.С.

2020

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

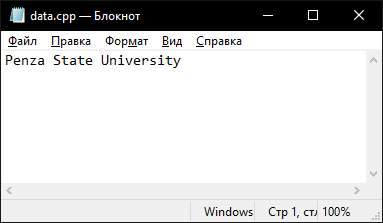
**Задания:** разработать программу, выполняющую шифрование и расшифровывание произвольного двоичного файла с использованием перестановочного шифра используя в качестве ключа последовательность, соответствующую номеру варианта. Выполнить проверку путем двоичного сравнения исходного файла и фала, полученного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

|  |  |
| --- | --- |
| Номер варианта | Последовательность перестановки |
| 7 | 20 7 10 8 30 4 3 25 2 6 19 0 9 16 13 1 17 5 15 11 29 24 22 14 26 31 28 23 12 18 21 27 |

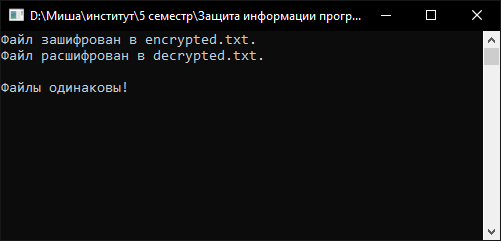
Работа программы:

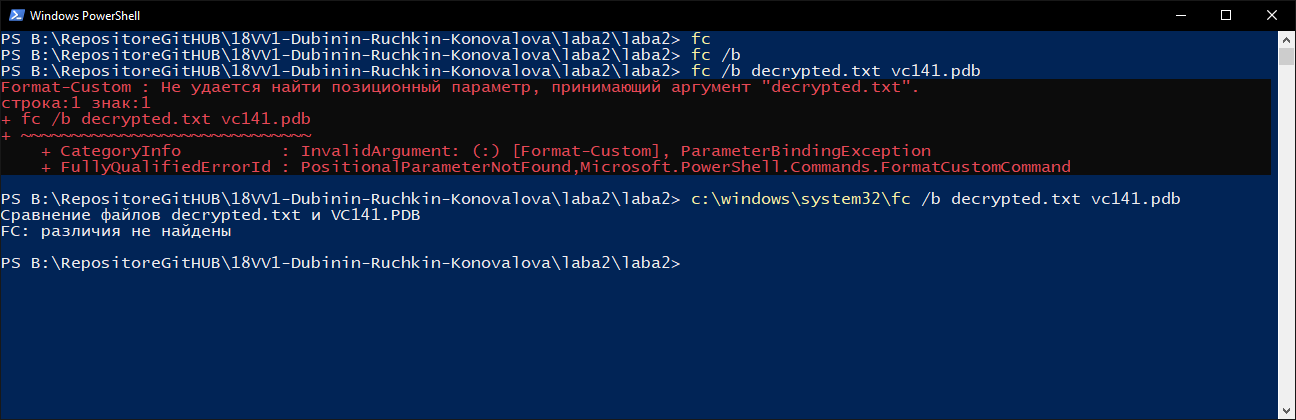
Для осуществления шифрования и расшифровывания необходимо создать текстовый файл, где будет отображена последовательность перестановки. Также нужно создать файл, над которым будет проводиться шифрование.

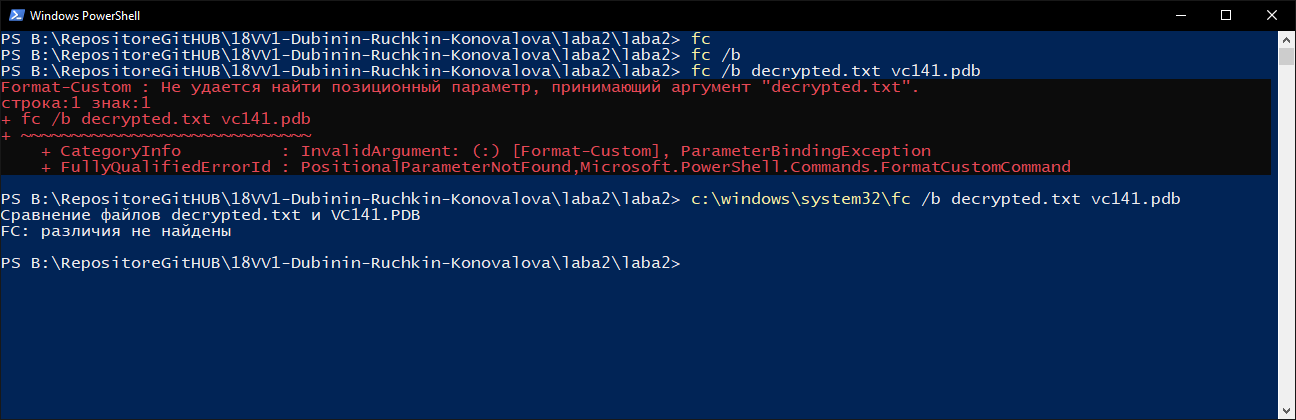
Для демонстрации работы программы создали следующий текстовый файл:



Вывод программы:







Листинг:

#define \_CRT\_SECURE\_NO\_WARNINGS

#include <iostream>

#include <conio.h>

#include <locale.h>

#define FILE\_NAME "data.cpp"

void char\_to\_bin(char text[4], int bin32[32])

{

int i = 0;

while (i < 32)

for (int j = 0; j < 4; j++)

{

for (unsigned q = 1U << 7; q; q >>= 1)

{

bin32[i] = !!((int)text[j] & q);

i++;

}

}

}

void bin\_to\_char(int bin32[], char ntext[5])

{

int j = 3;

int count = 0;

int count1 = 0;

int in\_code[4] = { 0,0,0,0 };

for (int i = 31; i > -1; i--)

{

if (bin32[i] == 1) {

in\_code[j] += pow(2, count - count1 \* 8);

}

if (i % 8 == 0)

{

j--;

count1++;

}

count++;

}

for (int i = 0; i < 4; i++)

{

ntext[i] = (char)in\_code[i];

}

ntext[4] = '\0';

}

char coder\_decoder(char key[32], int mod) { //шифрование/дешифрование

FILE \*data\_file, \*data\_file\_new;

char data[5];

data[4] = '\0';

char ntext[5];

int ntext\_in\_binary\_code[32];

int text\_in\_binary\_code[32];

if (mod == 0)

{

data\_file = fopen(FILE\_NAME, "rb");

data\_file\_new = fopen("encrypted.txt", "wb+");

}

else

{

data\_file = fopen("encrypted.txt", "rb");

data\_file\_new = fopen("decrypted.txt", "wb+");

}

while (fread(data, 4, 1, data\_file) != NULL) {

char\_to\_bin(data, text\_in\_binary\_code);

if (mod == 0)

for (int i = 0; i < 32; i++)

ntext\_in\_binary\_code[i] = text\_in\_binary\_code[key[i]]; //осуществление шифрования файла в заданной последовательности битов

else

for (int i = 0; i < 32; i++)

ntext\_in\_binary\_code[key[i]] = text\_in\_binary\_code[i]; //расшировка кода

bin\_to\_char(ntext\_in\_binary\_code, ntext);

fwrite(ntext, 1, 4, data\_file\_new);

}

fclose(data\_file\_new);

fclose(data\_file);

if (mod == 0)

printf("Файл зашифрован в encrypted.txt.\n");

else

printf("Файл расшифрован в decrypted.txt.\n");

}

void GetKey(char key[32])

{

FILE \*mykey;

mykey = fopen("key.txt", "rb");

for (int i = 0; i < 32; i++)

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

fclose(mykey);

}

void OptText() //добавление пробелов для правильного шифрования

{

FILE \*data\_file;

data\_file = fopen(FILE\_NAME, "rb+");

fseek(data\_file, 0, SEEK\_END);

while (ftell(data\_file) % 4 != 0)

fputs(" ", data\_file);

fclose(data\_file);

}

void Test()

{

FILE \*data\_file, \*data\_file\_new;

char s1 = { }, s2 = { };

data\_file = fopen(FILE\_NAME, "rb");

data\_file\_new = fopen("decrypted.txt", "rb");

while (!feof(data\_file\_new) && !feof(data\_file) && (s1 == s2)) {

s1 = fgetc(data\_file\_new);

s2 = fgetc(data\_file);

}

if (s1 == s2)

printf(" \nФайлы одинаковы!");

else

printf("\nФайлы разные!");

fclose(data\_file);

fclose(data\_file\_new);

}

int main()

{

setlocale(LC\_ALL, "Rus");

char key[32];

GetKey(key); //Получение ключа

OptText(); //Оптимизатор текста

coder\_decoder(key, 0); //шифрование

coder\_decoder(key, 1); //дешифрование

Test(); //Сравнение

\_getch();

}

**Вывод:** в ходе лабораторной работы разработали программу шифрования/дешифрирования двоичных файлов с использованием перестановочного шифра.