

Учреждение образования "Полоцкий Государственный Университет"

Факультет информационных технологий
Кафедра вычислительных систем и сетей

ЛАБОРАТОРНАЯ РАБОТА № 1

по дисциплине: **"Объектно-Ориентированные Технологии
Программирования и Стандарты Проектирования"**

ВЫПОЛНИЛ

студент группы 16-ИТ-3
Яблонский А.С.
вариант № 21

ПРОВЕРИЛ

преподаватель
Ярошевич П.В.

Полоцк 2019 г.

1 Задача

В рамках данной лабораторной работы необходимо ознакомиться и изучить функции библиотеки OpenSSL, а также создать приложение, которое шифрует и дешифрует содержимое текстового файла, согласно алгоритму, описанному в варианте задания.

2 Вариант № 21

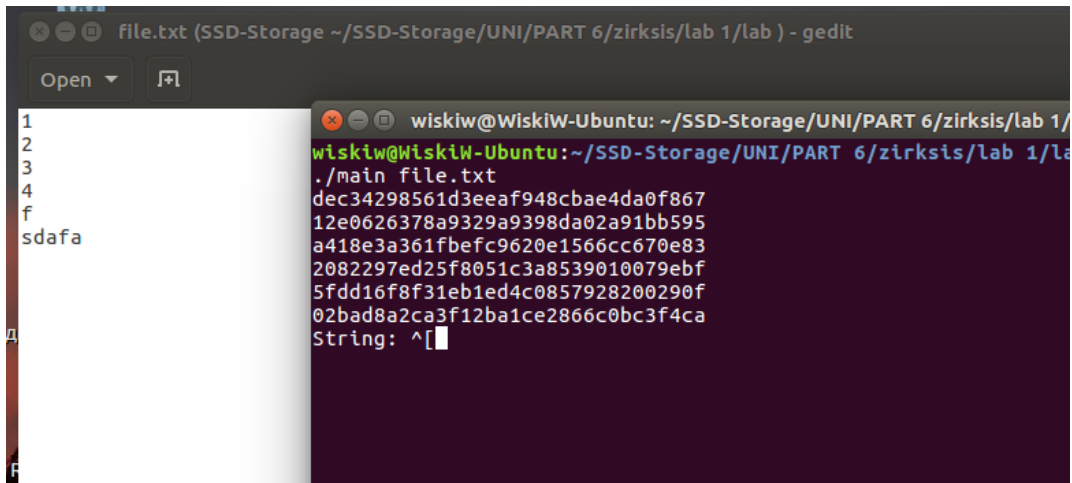
Преобразование строки с использованием хеш-функции MD5. На входе программы файл со списком строк, с помощью хеш-функции преобразуем все строки. Затем на вход подаем искомую строку, также с помощью хеш-функции преобразовываем ее и ищем в общем списке преобразованных строк.

3 Ход выполнения

Выполнение лабораторной работы включало в себя следующие шаги:

1. Реализацию операции чтения из файла.
2. Создание функции генерации MD5 хэша.
3. Создание функции, поиск значения по хэшу.
4. Реализация обработки параметров, полученных из командной строки.
5. Компиляция и запуск программы.

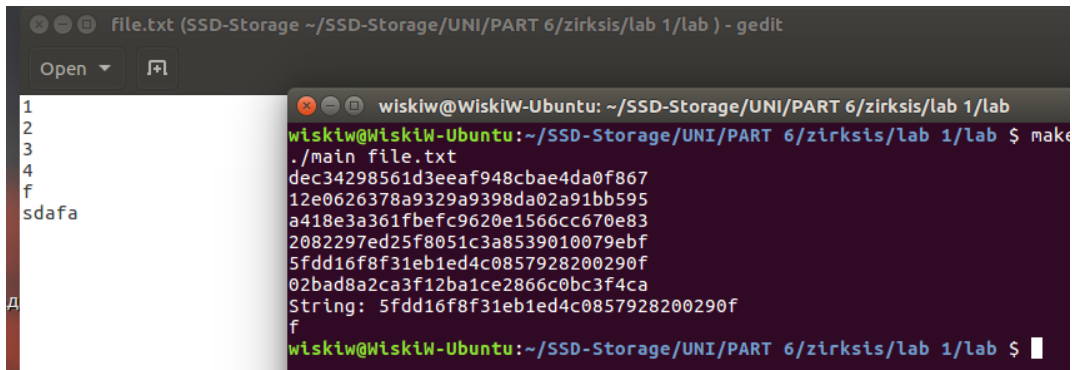
4 Скриншоты



The screenshot shows a terminal window with the following content:

```
wiskiW@WiskiW-Ubuntu: ~/SSD-Storage/UNI/PART 6/zirksis/lab 1/la
wiskiW@WiskiW-Ubuntu:~/SSD-Storage/UNI/PART 6/zirksis/lab 1/la
./main file.txt
dec34298561d3eeaf948cbae4da0f867
12e0626378a9329a9398da02a91bb595
a418e3a361fbefc9620e1566cc670e83
2082297ed25f8051c3a8539010079ebf
5fdd16f8f31eb1ed4c0857928200290f
02bad8a2ca3f12ba1ce2866c0bc3f4ca
String: ^[
```

Рис. 1: Генерация MD5-хэше



The screenshot shows a terminal window with the following content:

```
wiskiW@WiskiW-Ubuntu: ~/SSD-Storage/UNI/PART 6/zirksis/lab 1/la
wiskiW@WiskiW-Ubuntu:~/SSD-Storage/UNI/PART 6/zirksis/lab 1/la $ make
./main file.txt
dec34298561d3eeaf948cbae4da0f867
12e0626378a9329a9398da02a91bb595
a418e3a361fbefc9620e1566cc670e83
2082297ed25f8051c3a8539010079ebf
5fdd16f8f31eb1ed4c0857928200290f
02bad8a2ca3f12ba1ce2866c0bc3f4ca
String: 5fdd16f8f31eb1ed4c0857928200290f
f
wiskiW@WiskiW-Ubuntu:~/SSD-Storage/UNI/PART 6/zirksis/lab 1/la $
```

Рис. 2: Посик значения по хэшу

5 Source Code

lab.c

```
#include <openssl/md5.h>
#include <openssl/pem.h>
#include <openssl/err.h>
#include <stdio.h>
#include <string.h>
#include <sys/types.h>
#include <sys/stat.h>
#include <fcntl.h>

char* search(char* search_name, char*** str, int *count){

    for (int i=0;i<*count;i++){
        if (strcmp(str[i],search_name)==0){
            return str[i];
        }
    }
    return "String_not_found";
}

void MD5_FUN(char* file_name, char*** str, int *count){

    FILE *file=fopen(file_name,"r");
    char* string=(char*)calloc(1024,sizeof(char));

    SHA_CTX ctx;

    SHA1_Init(&ctx);

    while (fgets(string,1024,file) != NULL) {

        (*count)++;
        string[strlen(string)-1]=0;

        str[0]=(char**)realloc(str[0],sizeof(char*)*(*count))
        str[0][*count-1]=calloc(strlen(string)+1,sizeof(char))
```

```

    str[1]=(char**)realloc(str[1],sizeof(char*)*(*count));
    str[1][*count-1]=calloc(33,sizeof(char));

    strcpy(str[0][*count-1], string);

    unsigned char md5digest[MD5_DIGEST_LENGTH];
    //MD5(string, strlen(string), md5digest);
    SHA1_Update(&ctx, md5digest, MD5_DIGEST_LENGTH);

    SHA1_Final(md5digest, &ctx);

    for (int i=0; i < MD5_DIGEST_LENGTH; i++){
        sprintf(str[1][*count-1],"%s%02x", str[1][*count-2], md5digest[i]);
    }

    printf("%s\n",str[1][*count-1]);

}

}

void main(int argc,char** argv){

    char*** str=(char***)calloc(2,sizeof(char**));
    str[0]=(char**)malloc(0);
    str[1]=(char**)malloc(0);
    int count=0;

    if (argc==2){

        MD5_FUN(argv[1],str, &count);

        printf("String:_");
        char string[1024];
        scanf("%s",string);

        while (strlen(string)!=32) {

```

```

        printf("MD5_must_be_32byte_length_\n");
        scanf("%s",string);
    }

    printf("%s\n",search(string, str, &count));
}

```