**МИНОБРНАУКИ РОССИИ**

**Санкт-Петербургский государственный**

**электротехнический университет**

**«ЛЭТИ» им. В.И. Ульянова (Ленина)**

**Кафедра Информационной безопасности**

отчет

**по лабораторной работе №1**

**по дисциплине «Программирование»**

Тема: Разработка хэш-функции

|  |  |  |
| --- | --- | --- |
| Студент гр. 6361 |  | Нерсисян А. |
| Преподаватель |  | Халиуллин Р.А. |

Санкт-Петербург

2017

**Постановка задачи**

Реализовать хэш-функцию в программе. Написать программу для аутентификации пользователя с помощью пароля. Программа должна работать в двух режимах:

1. Создание пароля
2. Проверка пароля

Пароль не должна сохранится в программе. Для этого нужно использовать хэширование\* (хэш-функцию).

**\*Хэширование** — преобразование массива входных данных произвольной длины в (выходную) битовую строку фиксированной длины, выполняемое определённым алгоритмом.

**Исходный код**

#include <stdio.h>

#include <conio.h>

unsigned long long hash\_function(char\* str)

{

const int p = 32;

long hash = 0, pow = 1;

for (size\_t i=0; i<sizeof(str); ++i)

{

hash += (str[i] - 'a' + 1) \* pow;

pow \*= p;

}

return hash;

}

int main()

{

// choosing programm mode //

printf("Please choose the programm mode\n");

printf("Enter 1 to enter new password\n");

printf("Enter 2 for cheking password\n ");

int mode;

scanf("%d",&mode);

if(mode !=1 && mode!=2)

{

printf("%sError!");

}

if(mode == 1)

{

printf("Enter the new password, and press ENTER\n");

printf("Password length is 32 symbols\n");

char str[33];

scanf("%32c" ,str);

long long hash = hash\_function(str);

FILE\* f = fopen("hash.txt", "w");

for(int i=0; i<32; i++) fprintf(f, "%d", hash);

fclose(f);

}

if(mode == 2)

{

printf("Enter password\n");

char stw[33];

scanf("%32c", stw);

long long newhash = hash\_function(stw);

FILE\* nf = fopen("newhash.txt", "w");

for(int i=0; i<32; i++) fprintf(nf, "%d", newhash);

fclose(nf);

int counter=0;

FILE \*file1;

file1 = fopen("hash.txt", "r" );

FILE \*file2;

file2 = fopen("newhash.txt", "r" );

bool f1, f2;

do

{

f1=getc(file1);

f2=getc(file2);

if(f1!=f2)

{

counter++;

printf("%s ACCESS DENIED!");

}

}while(f1 != EOF);

if (counter == 0)

printf("%s ACCESS GRATED!");

fclose(file1);

fclose(file2);

}

return 0;

}

**Результаты тестирования, рисунки**

Программа реализована следующим образом:

* Запуск программы
* Выбор режима

Режим 1:

* Ввод нового пароля
* Хеширование пароля
* Сохранение пароля в текстовой файл (hash.txt)

Режим 2:

* Ввод пароля
* Хеширование пароля
* Сохранение пароля в текстовой файл (newhash.txt)
* Сравнение содержания файлов hash.txt и newhash.txt

Программу нужно запустить в командной стоке. После запуска программы нужно ввести 1 или 2 для выбора режима работы программы (рис. 1).

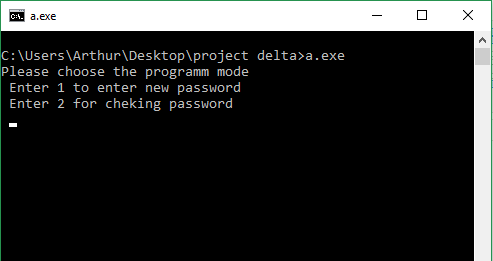


рисунок 1

После выбора режима нужно вводить новый пароль (рис. 2)

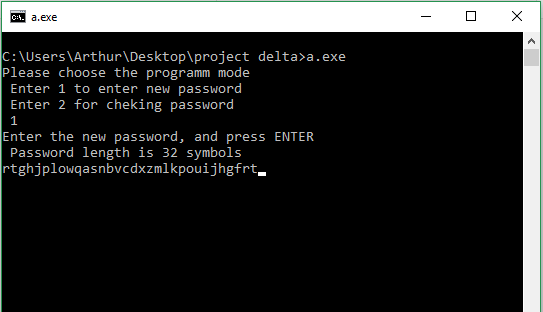


рисунок 2

Потом нужно программу заново запустить и выбрать режим 2 (рис. 3).

Ввести пароль.

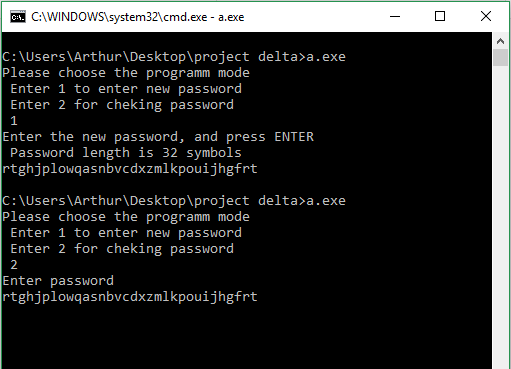


рисунок 3

В случае, если пароль введен правильно программа выводит сообщение “Access Grated!” (если введен неправильно, то “Access Denied!”)