Universitatea Tehnică a Moldovei

Facultatea Calculatoare Informatică şi Microelectronică

Departamentul Ingineria Software și Automatică

**RAPORT**

Lucrarea de laborator nr. 1

# La disciplina „Tehnici de Inginerie Inversa”

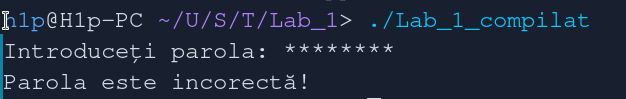
A efectuat: st. gr. SI-211 S. Chirita

A verificat: C. Maxim

Chișinău – 2024

Codul sursa:

#include <functional>   
#include <iostream>   
#include <string>   
#include <termios.h>   
#include <sstream>   
#include <iomanip>   
#include <openssl/sha.h>   
  
void hidePassword(char\* password) {   
   struct termios orig\_term, new\_term;   
   tcgetattr(0, &orig\_term);   
   new\_term = orig\_term;   
   new\_term.c\_lflag &= ~ECHO;  // Turn off echo   
   tcsetattr(0, TCSANOW, &new\_term);   
  
   std::cout << "Introduceți parola: ";   
   int i = 0;   
   while (true) {   
       char ch = std::cin.get();   
       if (ch == '\n') {   
           break;   
       }   
       password[i++] = ch;   
       std::cout << '\*';  // Replace each character with '\*'   
   }   
   password[i] = '\0';   
  
   tcsetattr(0, TCSANOW, &orig\_term);   
}   
  
int main() {   
   std::string hashPass = "54bdc049d97f97d64d3c401bd6febca9b7a89990b2a7b7b215031dcb147a3b4a"; //the\_secret\_password\_is = "54bdc049d97  
f97d64d3c401bd6febca9b7a89990b2a7b7b215031dcb147a3b4a"   
   char password[100];     
   hidePassword(password);   
   std::cout << std::endl;   
   std::string data = password;   
   // Calcularea hash-ului SHA-256   
   unsigned char hash[SHA256\_DIGEST\_LENGTH];   
   SHA256\_CTX sha256;   
   SHA256\_Init(&sha256);   
   SHA256\_Update(&sha256, data.c\_str(), data.length());   
   SHA256\_Final(hash, &sha256);   
  
   // Salvarea valorii hash într-o variabilă de tip std::string   
   std::stringstream ss;   
   for (int i = 0; i < SHA256\_DIGEST\_LENGTH; ++i) {   
       ss << std::hex << std::setw(2) << std::setfill('0') << static\_cast<int>(hash[i]);   
   }   
   std::string hashValue = ss.str();   
  
   // Afișarea valorii hash pentru debug   
   //std::cout << "Hash SHA-256: " << hashValue << std::endl;   
  
      
   if (hashValue == hashPass) {   
       std::cout << "Parola este corectă!" << std::endl;   
   } else {   
       std::cout << "Parola este incorectă!" << std::endl;   
   }   
  
   return 0;   
}



**Concluzie:**

Acest cod este un mic program în C++ care permite utilizatorului să introducă o parolă ascunsă, iar apoi calculează hash-ul SHA-256 al acestei parole și îl compară cu un hash pre-stabilit. Dacă hash-urile coincid, programul afișează un mesaj că parola este corectă, altfel afișează că parola este incorectă.