Team Members:

K22-4768

K22-4723

CYS-3B

Project Name: “Password Manager”

Overview:

Our project is a cpp based program which stores the users’ passwords securely by encrypting them with Caeser cipher algorithm. The project also provides the functionality of allowing users to check the strength of the passwords they want to store. It also allows the user to generate a random and secure password if they want to.

Key Features:

1.Securely Storing User’s Passwords:

-> Stores the users’ passwords securely by applying a secure algorithm for encryption.

2.Console Based Approach:

->Since the project is console based, the user may in inputs and get neat and clean outputs without any interruption of garbage or already shown previous output by clearing them.

3.Generating Password:

->Users may also ask for a secure random password which will be generated of the users’ desired length. **[1]**

Security Aspects:

1.Encryption:

->For additional security purposes, Caeser Cipher Algorithm have been applied so that passwords can be stored securely in the files.

2.Login Session:

->The user only can view their passwords once they enter the correct username and account password in login session.

Implementation:

Languages used: C++

The passwords will be stored in txt files after getting encrypted.

STEP BY STEP Procedure:

First, the user will have to create an account. They will be asked to input their username and password. Once the account is created, they will be asked to enter their credentials. If they enter wrong credentials, “try again” option will appear else 4 options will emerge. Whether they want to see already stored passwords, Store new passwords, generate new passwords or to Check the strength of already stored passwords. Now if the user chooses option ‘1’ they will be directed to the file which displays the passwords which were stored by the users already. If the user chooses option ‘2’ they will be asked to input the number of passwords that they want to store and will be asked to enter that number of passwords, then those passwords will get encrypted first and get saved. By choosing option ‘3’ a random password will be generated of the user's desired length. By choosing option ‘4’ the password strength will be determined.

Conclusion:

The purpose of the project is to provide a service for the users in which they can trust and ensure the security of safe and secure storage of their credentials. The important aspect is that the project provides an all-in-one platform where storing, generating as well as checking the strength of passwords takes place. By furthermore enhancements in user interface and security updates, it can be enhanced more in its effectiveness and usability.

Reference:

ChatGPT (2023), [1] ***Key Features,*** **9December2023**

THANK YOU