

برای پیاده‌سازی پروژه از نرم‌افزار متلب استفاده شده است. برای رمزگذاری متقارن AES و برای تابع چکیده‌ساز SHA-2، به طور ویژه SHA-512، مورد استفاده قرار گرفته است. هر دو الگوریتم به طور کامل در کد پیاده‌سازی شده است.

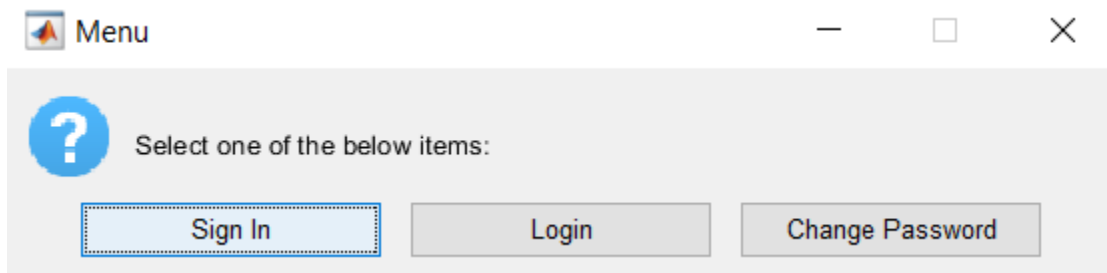
فایل اصلی Project.m است. با اجرای تابع GUI، ابتدا وجود فایل info.mat مورد بررسی قرار می‌گیرد. در صورت وجود، این فایل در برنامه لود می‌شود، در غیر این صورت فایلی با این عنوان ایجاد می‌شود. اطلاعات کاربران در این فایل ذخیره می‌شود.

فالی info.mat در واقع یک struct است که چهار field دارد. هر یک از این چهار field آرایه‌ای از نوع string است.

field اول EncryptedUsername1، field دوم EncryptedSalt، field سوم EncryptedUsername2 و field چهارم EncryptedData است. در ادامه کاربرد هر یک از موارد ذکر شده توضیح داده می‌شود.

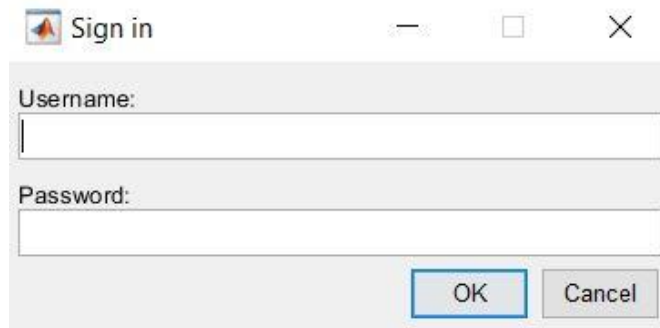
با توجه به توضیحات دستور کار مبنی بر اینکه نمی‌توان Password را به هیچ طریقی ذخیره کرد، برای بررسی صحت Password باید از روش دیگری استفاده می‌شد. در ابتدا برای حل این مشکل در مرحله Sign In، Username به دو صورت، یکی PlainText و دیگری رمز شده با استفاده از الگوریتم AES و کلید تولید شده با استفاده از الگوریتم SHA-512، ذخیره شد. لازم به ذکر است برای تولید کلید به عنوان ورودی تابع چکیده‌ساز از Username + Password + Salt استفاده شد، در نتیجه مقدار Salt نیز باید به صورت PlainText ذخیره می‌شد. استفاده از این روش، مشکل مطرح شده را به طور کامل بر طرف می‌کرد زیرا مقدار Salt کاملاً تصادفی است و در نتیجه استفاده از یک جدول از پیش آماده از Password های ممکن را بی‌فایده می‌کند. اما همچنان یک مشکل باقی بود. زیرا با توجه به فرض مطرح شده در دستور پروژه، مهاجم ممکن است به اطلاعات ذخیره شده برای شناسایی هر کاربر دسترسی داشته باشد. در این حالت مهاجم می‌تواند با استفاده از Username و Salt مربوط به یک کاربر خاص، جدولی از کلیدهای محتمل برای آن کاربر درست کند و با رمز کردن Username کاربر با کلیدهای محتمل، به دنبال Password کاربر بگردد. تنها راه حل این مشکل این، ذخیره Salt به صورت رمز شده است. برای این کار کلید دیگری با استفاده از Username کاربر ساخته می‌شود و مقدارهای Username و Salt با استفاده از این کلید رمز شده و ذخیره می‌گردد.

کاربر با اجرای برنامه با پنجره زیر مواجه می‌شود:

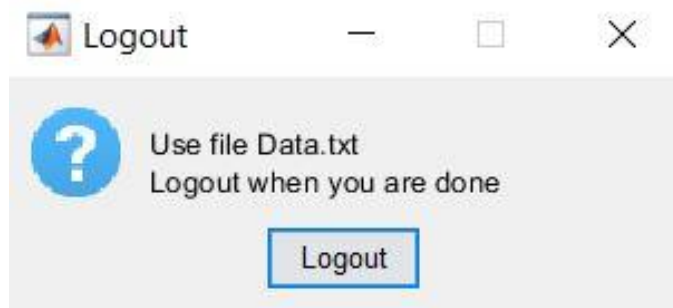


در ادامه به کاربرد هر یک از گزینه‌های موجود پرداخته می‌شود.

Sign In: بعد از انتخاب این گزینه، پنجره زیر نمایش داده می‌شود:

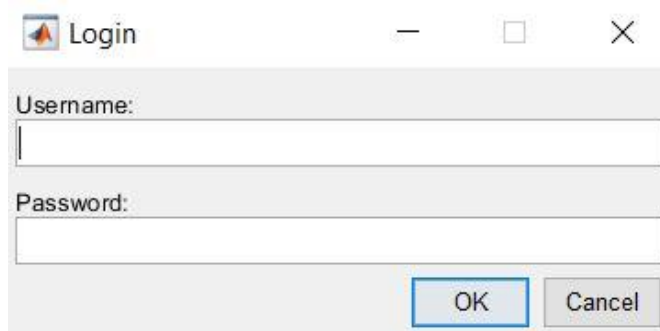
A small dialog box titled "Sign in" with a standard Windows icon. It contains two text input fields: "Username:" and "Password:". Below the fields are two buttons: "OK" and "Cancel".

در صورتی که روی گزینه OK کلیک شود، Username و Password وارد شده توسط کاربر به صورت آرایه‌ای از کاراکتر دریافت می‌شود. در صورتی که هر یک از این مقادیر خالی باشد، Error ای نمایش داده می‌شود و از ایجاد کاربر جدید جلوگیری می‌شود. در غیر این صورت، کلیدی با استفاده از Username وارد شده ساخته می‌شود و با استفاده از این کلید، Username وارد شده رمز می‌شود. سپس این مقدار با مقادیر موجود در فایل info.mat مقایسه می‌شود. در صورتی که کاربری با Username مشابه وجود داشته باشد، Error ای نمایش داده می‌شود و از ایجاد کاربر جدید جلوگیری می‌شود. در غیر این صورت، یک عبارت باینری تصادفی ۲۰۴۸ بیتی به عنوان Salt تولید و با استفاده از Username، Password و Salt کلید دوم ساخته می‌شود. در ادامه مقدار Salt با استفاده از کلید اول و مقدار Username یک بار با کلید اول و بار دیگر با کلید دوم رمز می‌شود و ذخیره می‌گردد. در آخر فایلی به نام Data.txt ایجاد می‌شود و از کاربر خواسته می‌شود تا اطلاعات محرمانه خود را در آن وارد کند. همچنین پنجره زیر نمایش داده می‌شود:

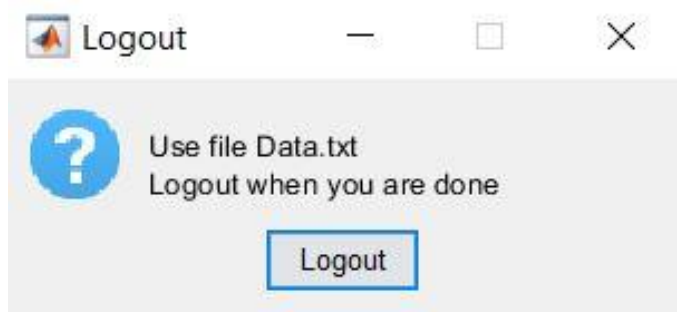
A small dialog box titled "Logout" with a standard Windows icon. It features a blue question mark icon on the left. To the right of the icon, the text reads "Use file Data.txt" and "Logout when you are done". At the bottom center, there is a "Logout" button.

کاربر باید بعد از اتمام کار خود، روی گزینه Logout کلیک کند تا اطلاعات وارد شده توسط او با استفاده از کلید دوم رمز شود و ذخیره گردد.

Login: بعد از انتخاب این گزینه، پنجره زیر نمایش داده می‌شود:

A small dialog box titled "Login" with a standard Windows icon. It contains two text input fields: "Username:" and "Password:". Below the fields are two buttons: "OK" and "Cancel".

در صورتی که روی گزینه OK کلیک شود، Username و Password وارد شده توسط کاربر به صورت آرایه‌ای از کاراکتر دریافت می‌شود. در صورتی که هر یک از این مقادیر خالی باشد، Error ای نمایش داده می‌شود و از ورود کاربر جلوگیری می‌شود. در غیر این صورت، کلیدی با استفاده از Username وارد شده ساخته می‌شود و با استفاده از این کلید، Username وارد شده رمز می‌شود. سپس این مقدار با مقادیر موجود در فایل info.mat مقایسه می‌شود. در صورتی که کاربری با Username مشابه وجود نداشته باشد، Error ای نمایش داده می‌شود و از ورود کاربر جلوگیری می‌شود. در غیر این صورت، Salt ذخیره شده مربوط به این کاربر، با استفاده از کلید اول رمزگشایی می‌شود. سپس با استفاده از Username، Password و Salt کلید دوم ساخته می‌شود. سپس مقدار Username با استفاده از این کلید رمز می‌شود. در ادامه مقدار بدست آمده با مقدار Username مربوط به این کاربر که با کلید دوم رمز شده است، مقایسه می‌شود. در صورتی که این دو مقادیر یکسان نباشند، Error ای نمایش داده می‌شود و از ورود کاربر جلوگیری می‌شود. در غیر این صورت اطلاعات محرمانه کاربر با استفاده از کلید دوم رمزگشایی می‌شود و در فایل به نام Data.txt وارد می‌شود و از کاربر خواسته می‌شود تا تغییرات مورد نیاز را در آن وارد کند. همچنین پنجره زیر نمایش داده می‌شود:



کاربر باید بعد از اتمام کار خود، روی گزینه Logout کلیک کند تا اطلاعات وارد شده توسط او با استفاده از کلید دوم رمز شود و ذخیره گردد.

Change Password: بعد از انتخاب این گزینه، پنجره زیر نمایش داده می‌شود:

در صورتی که روی گزینه OK کلیک شود، Username، Password قبلی و Password جدید وارد شده توسط کاربر به صورت آرایه‌ای از کاراکتر دریافت می‌شود. در صورتی که هر یک از این مقادیر خالی باشد، Error ای نمایش داده می‌شود و از تغییر Password جلوگیری می‌شود. در غیر این صورت، کلیدی با استفاده از Username وارد شده ساخته می‌شود و با استفاده

از این کلید، Username وارد شده رمز می‌شود. سپس این مقدار با مقادیر موجود در فایل info.mat مقایسه می‌شود. در صورتی که کاربری با Username مشابه وجود نداشته باشد، Error ای نمایش داده می‌شود و از تغییر Password جلوگیری می‌شود. در غیر این صورت، Salt ذخیره شده مربوط به این کاربر، با استفاده از کلید اول رمزگشایی می‌شود. سپس با استفاده از Username، Password قدیم و Salt کلید دوم قدیمی ساخته می‌شود. سپس مقدار Username با استفاده از این کلید رمز می‌شود. در ادامه مقدار بدست آمده با مقدار Username مربوط به این کاربر که با کلید دوم قدیمی رمز شده است، مقایسه می‌شود. در صورتی که این دو مقادیر یکسان نباشند، Error ای نمایش داده می‌شود و از تغییر Password جلوگیری می‌شود. در غیر این صورت اطلاعات محرمانه کاربر با استفاده از کلید دوم قدیمی رمزگشایی می‌شود. سپس با استفاده از Username، Password جدید و Salt کلید دوم جدید ساخته می‌شود. در آخر Username و اطلاعات محرمانه کاربر با استفاده از این کلید رمز می‌شود و جایگزین مقادیر قبلی می‌گردد.

لازم به ذکر است الگوریتم‌های مربوط به رمز متقارن AES و تابع چکیده‌ساز SHA-512 به طور کامل در کد پیاده‌سازی شده است. فایل مربوط به این موارد به همراه گزارش ارسال شده است.