

BBM 465: Information Security Laboratory Programming Assignment-2

Teachers:

- Ahmet Selman Bozkır
- Ali Baran Taşdemir

Students:

- Mert Tazeoğlu (21946606)
- Mehmet Emin Yıldız (21527602)

Heading.....	Page
Problem Definition.....	2
Important Implementation Details.....	2
Current Database Configurations.....	6
Important Technical Details.....	6
Important Note About Source Code & Testing.....	7

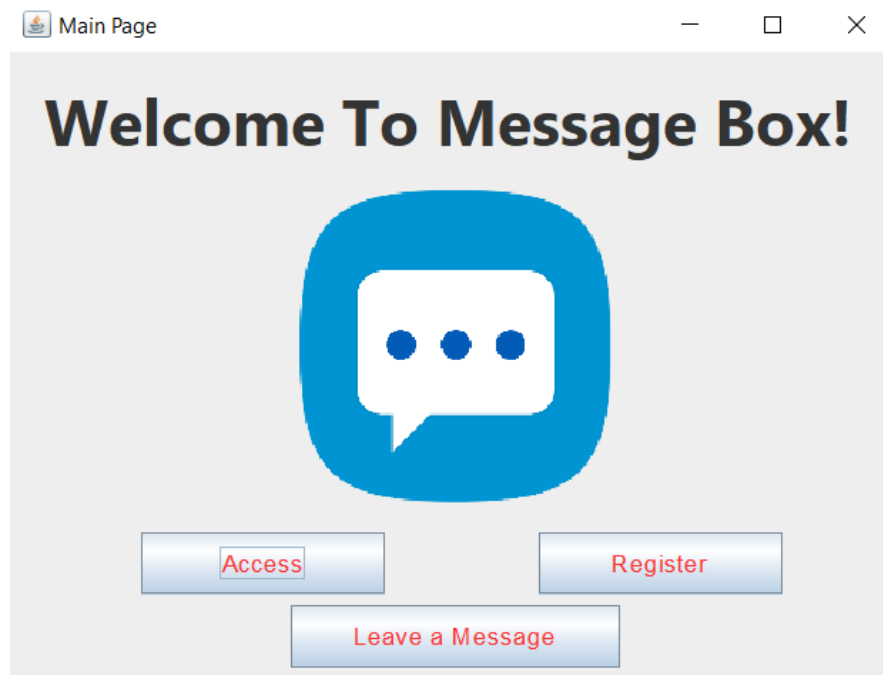
Problem Definition

In this assignment we implemented a messaging system.

Important Implementation Details

1. Main Page (Initial Page)

This is the first page displayed when the application starts. Image added but **image should be in correct folder in order to see it!**



2. User Register Page (Main Page > Register)

This is the page that shows up when user clicks the “register” button in the main page. This **an extra functionality. (*)**

A screenshot of a web browser window titled "Register User". The page has a light gray background. It contains two input fields: "Username (*)" and "Password (*)". Below these fields, there are two warning messages: "Warning: Username must be unique, password must be at least 7 char." and "Warning: Inputs can't contain space character or Turkish characters." Below the warnings, there is a checkbox labeled "Show Password". At the bottom of the page, there are two buttons: "Register" on the left and "Return Homepage" on the right. All buttons are light blue with a slight gradient and a thin border.

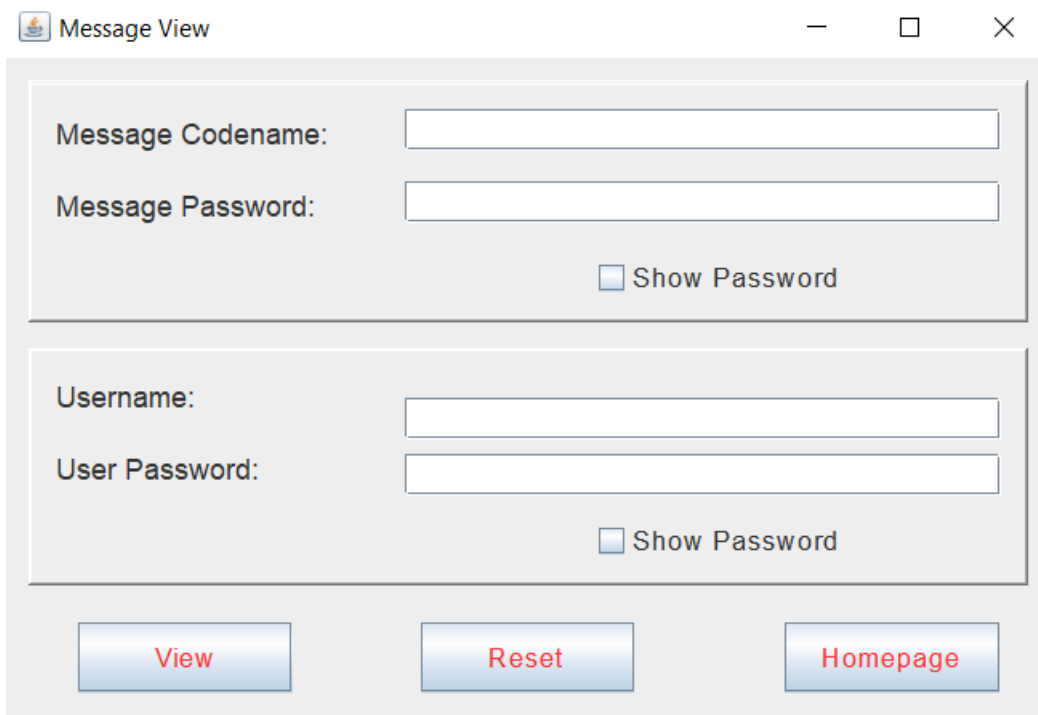
Included error handlings in this form are these:

- If inputs are empty, program will warn with a message dialog.
- If password length is less than 7 characters, program will warn with a message dialog.
- If username is not unique, program will warn with a message dialog.
- If inputs contain space or underscore () character, program will warn with a message dialog. (It cause an issue while splitting database files)
- If inputs contain Turkish characters (ğ, ç, ü, ö, İ, ı etc.), program will warn with a message dialog. (It may cause problems in encryption and decryption due to character set problems)

If inputs meet these conditions, program will authorize user and register user, and finally give information with a message dialog.

3. Access Page (Main Page > Access)

This is the page that shows up when user clicks the “access” button in the main page. In this page, a basic authorization test is performed in order to show to message.



The screenshot shows a Windows-style dialog box titled "Message View". It has standard window controls (minimize, maximize, close) in the top right corner. The dialog is divided into two main sections by a horizontal line. The top section is for "Message" and contains two text input fields: "Message Codename:" and "Message Password:". Below the "Message Password:" field is a checkbox labeled "Show Password". The bottom section is for "User" and contains two text input fields: "Username:" and "User Password:". Below the "User Password:" field is another checkbox labeled "Show Password". At the bottom of the dialog, there are three buttons: "View", "Reset", and "Homepage", each with a red text label on a blue button background.

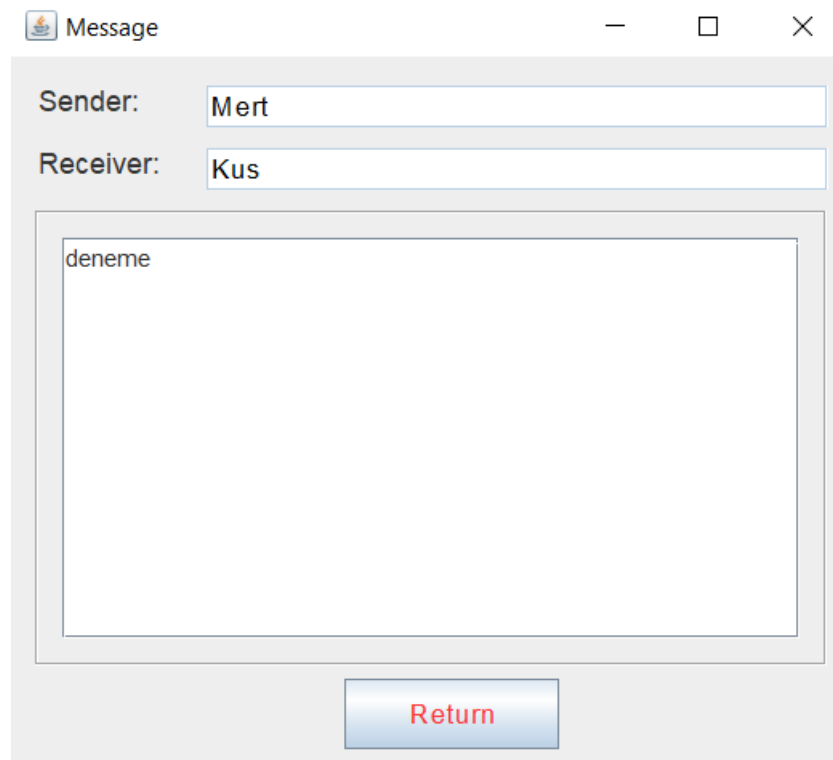
Included error handlings in this form are these:

- If a user with that username and password doesn't exist, program will warn with a message dialog.
- If a message with that code name and password doesn't exist, program will warn with a message dialog.
- If such a message exists, but that message is not sent for that user, program will warn with a message dialog.

If inputs meet these conditions, program will authorize user and finally show message with showing a new page.

4. Message Page (Main Page > Access > Message Page)

This is the page that shows up when user fills access page form properly. In this page, if such a message exists and if authorization is done, this page will be show.



Message

Sender: Mert

Receiver: Kus

deneme

Return

5. Leave Message Page (Main Page > Leave a Message)

This is the page that shows up when user clicks the "leave a message" button in the main page.

Message Register Form

Auth. Username (*): Mert

User Password (*):

Confirm Password (*):

☐ Show Password

Receiver Username (*): Mert

Warning: Inputs can't contain space character or Turkish characters.

Message Codename (*):

Message Password (*):

Your Message (*):

Warning: Message can't contain underscore (low line) (_) character.

Send Message

Return Homepage

Included error handlings in this form are these:

- If inputs are empty, program will warn with a message dialog.
- If inputs contain Turkish characters (ğ, ç, ü, ö, İ, ı etc.), program will warn with a message dialog. (It may cause problems in encryption and decryption due to character set problems)
- If inputs contain underscore (_) character, program will warn with a message dialog. (It cause an issue while splitting database files)
- If password and confirm password fields are not equal, program will warn with a message dialog.
- If a user with that username and password doesn't exist, program will warn with a message dialog.
- If sender and receiver are same person, program will warn with a message dialog.
- If code name is not unique, program will warn with a message dialog.

If inputs meet these conditions, program will authorize user, send message and finally show dialog about successful process.

Current Database Configurations

1. Registered Users

Username	Password
Mert	Mert123.
Mehmet	1234567
AliBaran	password
AhmetSelman	Admin123.

2. Existing Messages

ID (Code)	Content	Sender	Receiver	Password
1	*long text	Mert	Mehmet	pw1
41	*short text	Mehmet	AliBaran	passcode
topsecret	*avg. text	AliBaran	AhmetSelman	topsecret
0!KzM	*longest txt	AhmetSelman	Mert	123.

Important Technical Details

- Message ID and usernames must be unique and program checks it.
- Passwords of users and messages are stored in encrypted version of hashed format in database files. Other details are just encrypted in order to provide maximum security.
- Program requires (and has) only two database files which are for users and messages. Also they are in same directory with program.
- Program has an authorization system with three main functionalities (access, register, view). For example, program checks that whether current message is send for that user. If users knows message ID and password but if that message is not sent for that user, than that user can't see that it.
- User interfaces are designed with Java Swing.
- Encryption is done with DES algorithm with using Crypto API.
- MD5 function is used for hashing. (Since there is not dehashing function like decryption it is wise to store passwords in hashed form.
- In encryption, key is hard-coded since it contains lower case letters, upper case letters, numbers and special characters.

Important Note About Source Code & Testing

We developed our code in Netbeans IDE. In existing source code .data files are in main project folder. But in PDF document of this assignment, in submission format part both of .java and .data files are in src folder.

Therefore we submitted both of in the format as you stated in PDF but we also sent original project folder completely as a ZIP file which is named as 'CompleteSourceFromNetBeansIDE.zip' with e-mail.

We added image to main page. In order to make program work properly, we recommend you to use project files in the ZIP file completely.