ENCRYPT TECH

PROJECT CONTRIBUTORS :

Date: 07 / 14 / 2023		
Prepared by: **Hajra Rao (CT-AI 003)** **Qurat-ul-Ain Akhter (CT-AI 002)** **Ali Haider Rana (CT-AI 044)** **Nofal shamim (CT-AI 039)**	**Department:** **Computer Science And Information Technology**	**Project Proposal :** **Making an Encryption and Decryption program that will ensure data security that will protect data from data breaches and cyberattacks .**

PROJECT Summary :

Our project aims to develop a secure message encryption and decryption program with user authentication functionality. The program will provide a seamless and user-friendly experience, enabling users to sign up, log in, and choose between free and premium membership options. Both user types will have access to encryption and decryption features, but premium users will enjoy additional benefits and enhanced capabilities.

OBJECTIVES :

User Authentication: Implement a robust user authentication system that requires users to sign up and log in securely. This will ensure that only authorized individuals can access the program's features.

Membership Differentiation: Offer free and premium membership options to cater to different user requirements. Clearly define the features and limitations of each membership level to provide users with a transparent understanding of the benefits they will receive.

Secure Message Encryption: Develop a reliable encryption algorithm that can encrypt user-provided messages effectively. The encryption process will utilize industry-standard encryption techniques to ensure the confidentiality and integrity of the data.

Message Decryption: Implement a decryption feature that enables users to decrypt previously encrypted messages accurately. The program will ensure that only authorized users with the correct decryption key can access the decrypted message.

Premium User Benefits: Enhance the program's premium membership experience by offering additional features and functionalities. These may include encryption of their choice of files etc.

Security and Privacy: Prioritize data security by implementing industry-standard encryption techniques and robust security measures. Ensure that user data is securely stored and protected from unauthorized access or breaches.

Project Overview :

The Challenge:

Performance Optimization: Encryption and decryption processes can be computationally intensive, especially for large messages or complex encryption algorithms. Optimizing the program's performance to ensure quick response times and efficient resource utilization can be a challenge, particularly for users with limited computational resources.

Project Goals :

Develop a Secure Messaging System: The primary goal of the project is to create a secure messaging system that allows users to encrypt and decrypt messages to ensure the confidentiality and integrity of their communication.

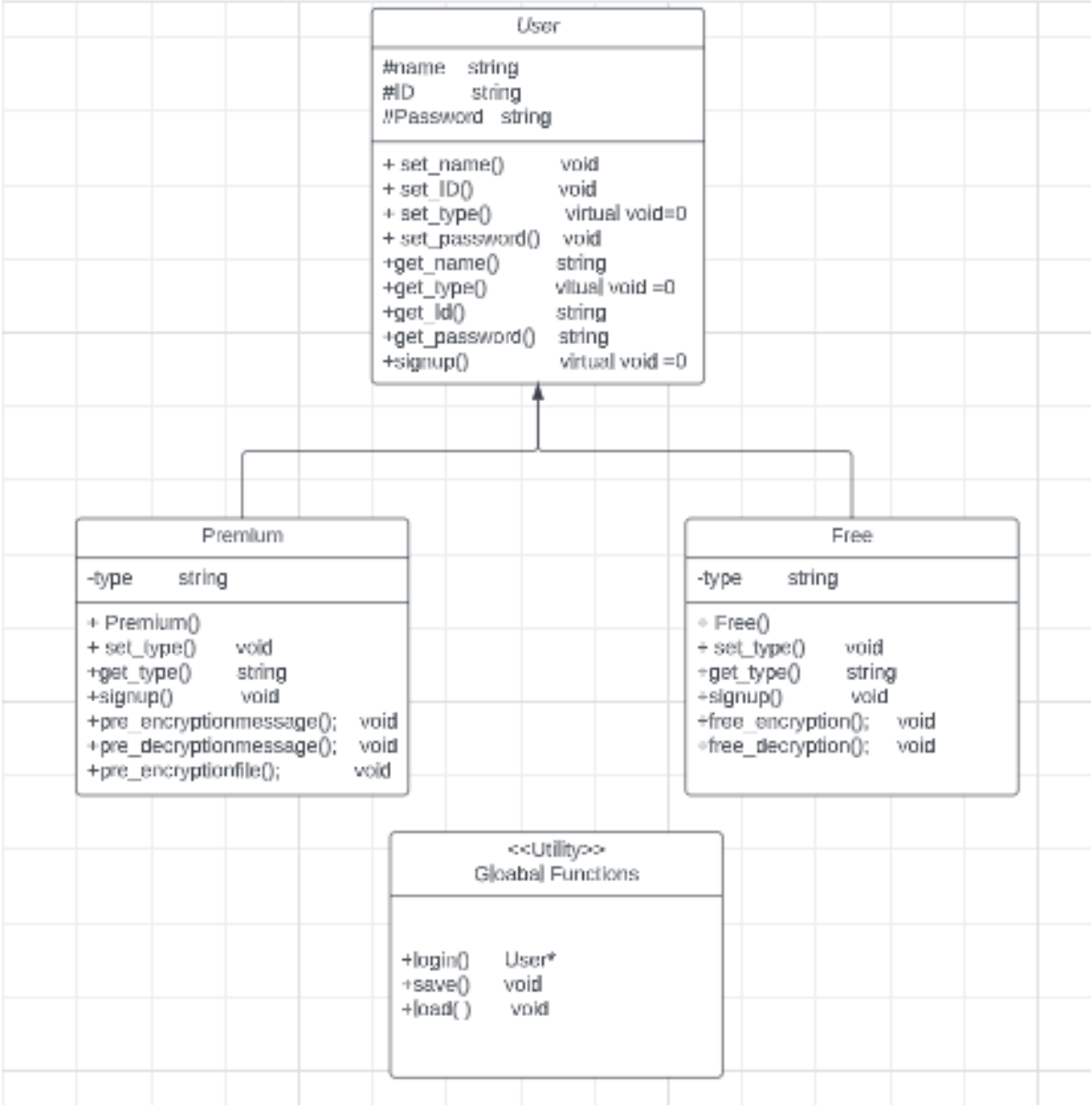
User Authentication: Implement a robust user authentication system to ensure that only authorized individuals can access the program's features. This includes providing options for user sign-up and login processes with appropriate security measures.

Membership Differentiation: Offer different membership options (free and premium) to cater to the diverse needs of users. Clearly define the features and limitations of each membership level to provide users with a transparent understanding of the benefits they will receive.

Secure Encryption and Decryption: Develop a reliable encryption algorithm and decryption process that effectively protects the confidentiality and integrity of user messages. Use industry-standard encryption techniques to ensure the security of the data.

Data Security and Privacy: Prioritize the security and privacy of user data by implementing strong encryption measures, secure storage, and protection against potential vulnerabilities or breaches.

THE UML CLASS DIAGRAM OF OUR PROJECT :



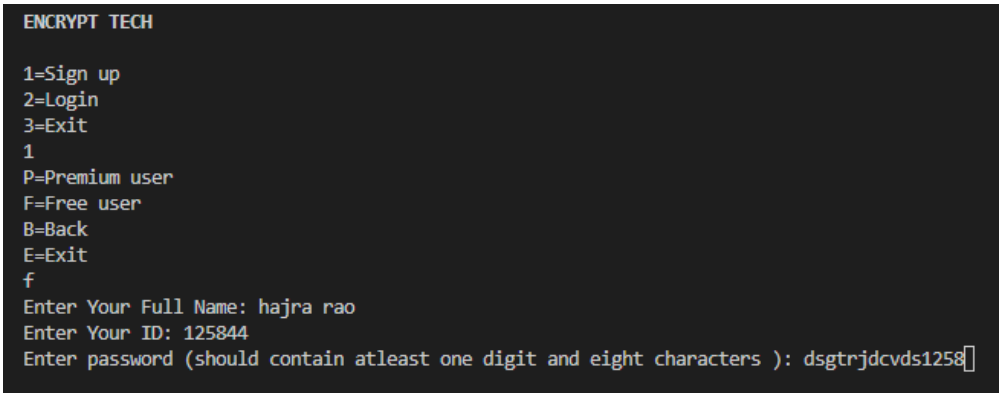
FUNCTIONALITIES :

Login Functionality:

- Validate user credentials (username and password) against stored user data.
- Implement secure password hashing and salting techniques for password storage.
- Generate and store session tokens upon successful login to authenticate subsequent requests.
- Provide appropriate error messages for incorrect credentials or other login-related issues.

Signup Functionality:

- Allow users to create a new account by providing required information (username, password, email, etc.).
- Implement validation checks to ensure data integrity and enforce any necessary requirements (e.g., strong password policy).
- Store user information securely, including encrypted or hashed passwords, and unique user identifiers.
- Handle scenarios where a ID or password is already registered to prevent duplication.
- For Premium user a new file with user ID is created to store user encrypted data .



Encrypt Functionality:

- Provide a text input field for users to enter the message they want to encrypt.
- Implement encryption algorithms **(ceaser cipher)** to encrypt the user's message securely.
- Display the encrypted message to the user and provide options to copy or share it securely.
- For Premium users , they can also give us file to be encrypted.

Below is the output of implemented logic for encryption:

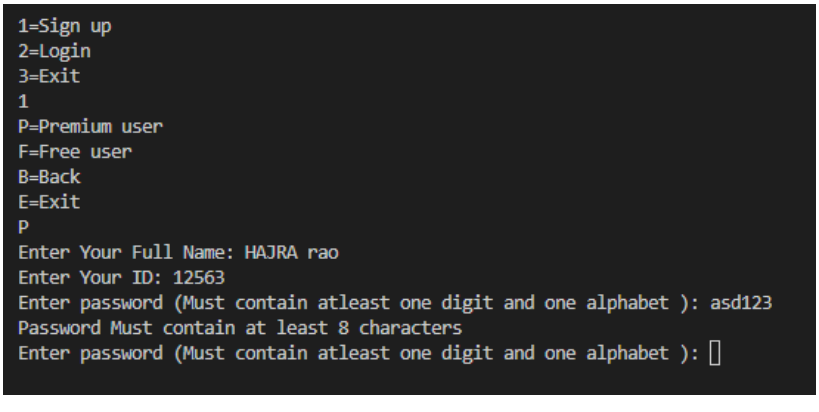
Decrypt Functionality:

- Accept the encrypted message as input from the user.
- Implement decryption algorithms corresponding to the encryption algorithm used.
- Decrypt the message and display the original plaintext to the user.
- For Premium users , they can also give us file to be decrypted.

Below is the output of implemented logic for decryption:

EXCEPTION HANDLING :

PASSWORD EXCEPTION: If the user enters less than 8 characters with no digit and character present in the password it will throw an exception .
As given below in code snippet:



LOGIN ID EXCEPTION : If the user login with incorrect id then it will throw an excepotion that incorrect id As given below in code snippet:

```
ENCRYPT TECH

1=Sign up
2=Login
3=Exit
2
Enter your ID: 12345
Enter your password: asdfghj1458
Incorrect ID or Password entered !
Enter your ID:
```

SIGNUP ID EXCEPTION : If the user signup with the ID already exists in our database then it will throw exception
As given below in code snippet:

```
ENCRYPT TECH

1=Sign up
2=Login
3=Exit
1
P=Premium user
F=Free user
B=Back
E=Exit
f
Enter Your Full Name: hajra rao
Enter Your ID: 12345
ID already Exist!
Enter Your ID:
```

CONCLUSION:

Overall, a data encryption and decryption program is invaluable to the tech industry as it strengthens security, ensures compliance, facilitates secure communication, protects against cyber threats, and enhances customer trust. By integrating such a program into their operations, tech companies can operate in a safer and more reliable manner while meeting the ever-growing demands for data protection.