1 Introduction

This assignment is actually much better than Comp2017's o.O

2 Approach explanation

Part: Basic Functionality Requirements:

1

Basically provided by template...

2

King Zhou !!!

3

King Zhou !!!

5

Users can click on a friend to open a chatroom. **King Zhou**

The process of ensuring secure communication between users:

1. During the signup or login process, each user generates a pair of cryptographic keys: a public key and a private key. The public key is uploaded to the server and stored in a database called public_keys, while the private key is retained in the user's local storage. These keys are generated based on the user's password, ensuring that they are consistently the same each time they are generated.
2. For establishing a shared secret key, each party uses their own private key and the other party's public key to compute a value using elliptic curve cryptography (ECC). Despite the involvement of individual private keys and the corresponding public key, both parties arrive at the same shared secret key.
3. This key is then used for symmetric encryption, enabling encrypted communication between the two. Symmetric encryption, which utilizes the same key for both encryption and decryption, is faster than asymmetric encryption and is well-suited for encrypting large volumes of data.

Part: Additional Criteria:

1

When signing up, after checking if the user has already signed up, the server will generate a random salt and hash the password with this salt. Finally, it stores the username, salt, and hashed password in the database.

```python
# inserts a user to the database
def insert_user(username: str, password: str):
    with Session(engine) as session:
        salt = gensalt()
        hashed_password = hashpw(password.encode('utf-8'), salt)

        user = User(username=username, password=hashed_password,salt=salt)

        session.add(user)
        session.commit()

```

Figure 1: db.py insert_user()

	username	salt	password
	Filter	Filter	Filter
1	a	$2b$12$fME/2FrWEdFHlC7KEAX27.	$2b$12$fME/2FrWEdFHlC7KEAX27./...
2	b	$2b$12$H5HjuJ1BqghUNOogEcapce	$2b$12$H5HjuJ1BqghUNOogEcapcemqPrBlgrnxxtyBdVu...

Figure 2: main.db Table: user

3 Contribution

```
#include <iostream>

int main() {
    std::cout << "Hello, World!" << std::endl;
    return 0;
}
```