1. server和client连接上之后，各自生成一对RSA Key Pair

2. 通过Diffie-Hellman Key Exchange, server和client之间生成一个公用的secret key

3. server和client分别把用secret key加密过的，各自的RSA Public Key发给对方，再分别用secret key解密得到对方的RSA Public Key

Key of server: server RSA key pair, secret key, client RSA public key

Key of client: client RSA key pair, secret key, server RSA public key

4. 注册时，client用server的RSA public key加密用户名，密码，邮箱按次序发给server，server解密后传到数据库，用AES加密后去核对（不需要key）

5. 登录时，client用server的RSA public key 加密用户名和密码发给server，server解密后传到数据库验证，然后再把AES解密后的email，通过client的RSA public key加密后传回给client，client解密后核对

6. 登录/注册成功后，显示目前可用的waiting room，没有的话用户可以选择创建，创建后默认同意chat，等另一个用户加入后开始形成chat room

7. 不加入waiting room默认退出（没写）