

## Chat sécurisé:

Pour lancer le serveur : (src/server) python server.py

pour l'arrêter : kill server.py dans une console (Je n'ai rien prévu pour l'arrêter)

Pour lancer le client : (src/client) python client.py

python client.py python client.py python client.py

Côté client, vous avez le choix des commandes.

Interaction : pour quitter : "/quit" pour s'identifier : "/identify password"  
"/identify RSA" pour changer de login : "/nick newnick" pour s'enregistrer :  
"/register password"

## Description

Il y a un serveur et plusieurs client. Le serveur tient le rôle de salon de chat. Les clients se connectent au serveur et établissent échange de clefs selon le protocole spécifié par le client. (Diffie Hellman ou RSA)

## Patterns

Role, single access point, session, proxy, strategie

## Role implementation:

Roles are used on server side only.

The client can try to tipe text but relying on his role /session, his messages will be printed or not.

Each client that connects to the server will have a session attached to him on server side.

## RFC:

Server is listening on his port.

Client connects.

Chiffrement des communications -> Inutile chiffrement lors de l'échange de mots de passes?

python -i file > interact