

# Projet sécurité

Sa e Silva Bruno

## Application de chat en Python

### Installation des bibliothèque

Une bibliothèque pour créer le système de serveur client:

**pip install sockets**

Une bibliothèque pour aider a crée chiffré et déchiffré en RSA:

**pip install cryptodome**

Une bibliothèque pour exécuter plusieurs processus en même temps:

**il est installer nativement sur python**

Une bibliothèque pour exécuter plusieurs processus en même temps:

**il est installer nativement sur python**

### fonction disponible de l'application

Dans l'application on peut envoyer un message a chaque personne du serveur en écrivant le message.

Ou envoyé un message priver avec "@" + le\_nom\_de\_la\_personne + " " + le\_message il faut que la personne existe sinon il retourne un message pour dire qu'il n'existe pas.

## Principe de l'application

Le principe est ont démarre un serveur, puis le client se connecte et génère une paire de clés RSA dont il envoie la clé publique, le nom du client au serveur qui le stock. Après le client peut taper un message puis envoie une notification si y est il est privée ou public. Si il est public le serveur envoie un par un la clé puis attend le message chiffré par le client puis l'envoie à la personne qui le déchiffre avec sa clé privée et l'affiche

## Exemple pour l'application

démarré le serveur  
démarré un client et entre un nom  
démarré un autre client et entre un autre nom  
écrivez un message il s'affichera:  
**"nom\_l'expediteur ->message**  
écrivez @nom\_du\_recepteur un message il s'affichera pour l'expéditeur:  
**"mp pour nom\_du\_recepteur: message**  
pour le récepteur:  
**"mp de nom\_l'expediteur: message**