Projet S4

Cryptochat

Principe :

Un serveur de chat ou les client n’envoie que des messages crypter et chaque client doivent connaître le mot de passe des utilisateurs qu'ils veulent parler pour pouvoir décrypter leur messages.

Comment le lancer :

Une fois dans le dossier du git :

Pour lancer un serveur : "./gradlew serv"

Pour lancer un client : "./gradlew client"

Pour lancer les test de cryptage : "./gradlew encryTestRun"

Fonctionnement :

Une fois le serveur lancer, quand un client démarre il demande l'ip du serveur, localhost si le serveur est héberger sur la même machine que le client. Une fois cet étape passer, l'utilisateur est demander un pseudo puis un mot de passe.

Une fois connecter, sur le côté il peut voir une liste des utilisateurs connecter, si il clic sur un nom le logiciel lui demande le mot de passe de la personne sur lequel il a cliquer, puis il décryptera les prochain messages envoyer sur le serveur.

Cryptage :

Le cryptage est en AES, la clé est former d'un hash du mot de passe fait en « PBKDF2WithHmacSHA1 » qui permet de créer des clef secrète via un mot de passe dans un seul sens, fonction qui est définie par PKCS v2.0.

Une fois ceci fait, le cryptage est fait en AES via un PKCS5Padding tout en stockant la SecretKey qui permet un décryptage par n'importe qui a n'importe quel moment