HIDDEN CHAT

Ce projet de sécurité mené par Alexandre Courand et moi-même, Pierre Bourgeois, porte sur l'implémentation d'un échange sécurisé de message par l'intermédiaire d'un chiffrement PGP. Dans notre implémentation, le client se connecte à une salle privée sur le serveur qui génère une paire de clé privée/publique. Une fois connecté au serveur, le client récupère la clé publique de la salle et génère sa propre paire, où il envoie sa clé publique au serveur. Lors des échanges des messages, les messages sont alors chiffrés avec ces clés publiques.

Il y a deux parties importantes pour ce projet :

- Server-side :
  - NodeJS
  - SocketIO
  - Express
  - KBPGP
- Client-side :
  - AngularJS
  - SocketIO
  - KBPGP
  - Bower (pour installer les assets)

Les difficultés

Il n'y a pas eu de difficulté particulièrement notable en se référant aux documentations officielles des technologies utilisées. La seule difficulté fût de synchroniser les bibliothèques de génération de clé publiques et privées PGP. Une fois une librairie compatible à la fois au niveau serveur et du côté client, le projet a pu être terminé assez rapidement.

Lancer le projet

Pour lancer un projet, se mettre à la racine du projet, et lancer avec nodeJS :

node bin/www

Dans le cas où des librairies seraient manquantes :

npm install (pour installer les librairies côté serveurs)

bower install (pour installer les librairie côté client)