ligne horizontale

**Le groupe**

Clément Thiry

Loris Lahon

Julie Khao

Chatsnap

**02 juin 2022**

# VUE D'ENSEMBLE

Lors du chapitre sur le réseau nous avons abordé la communication entre différentes machines. Dans ce projet, nous devions faire en sorte que cette communication permette de transférer s messages.

# OBJECTIFS

1. Créer un chat rapide entre deux terminaux en python
2. Rendre ce chat sécurisé
3. Créer une interface

# CARACTÉRISTIQUES

Pour réaliser ce projet nous avions le droit au cours ainsi qu'aux différentes ressources pédagogiques à notre disposition.

Ce projet à été réalisé en python 3.7 , pour y avoir accès l'installation des bibliothèques **Qt5** et **unidecode** est nécessaire.

Le fichier *README.txt* donne des informations complémentaires sur le projet.

# GRANDES ÉTAPES

## Création du chat

À l'aide du cours fourni par la plateforme open classroom nous devions essayer de faire communiquer deux terminaux entre eux (un étant le serveur et l'autre seulement le client).

Suite à cela il fallait faire communiquer deux clients en passant par un serveur (différent des deux clients).

## Sécurisation du chat

La sécurisation du chat se joue en 5 étapes : 1. Le client, chiffré symétriquement au début, envoie sa clé publique au serveur; 2. Le serveur, chiffré symétriquement, code la clé de chiffrement symétrique avec la clé publique envoyée par le client; 3. Le serveur envoie la clé symétrique chiffrée au client; 4. Le client déchiffre la clé publique avec sa clé privée; 5. Le client chiffre maintenant ses messages symétriquement de la même façon que le serveur.

Ainsi, pour ces 5 étapes, nous avions besoin de chiffrement symétrique et asymétrique. Pour cela, nous voulions d’abord utiliser le module python pédagogique “Sympy” or dès les premières lignes de la documentation, il est conseillé d’utiliser le module “Cryptography”.

Ce module est très avantageux car il permet de chiffrer Symétriquement et de manière sécurisée avec la classe Fernet et aussi assymétriquement. Or dans le cas du chiffrement asymétrique, malgré les nombreuses réinstallations du module sur l’ordinateur personnel ou en salle, une erreur nous empêchait d’utiliser la partie asymétrique du module “Cryptography”.

C’est pour cela que nous avons codé à la main les différentes fonctions du chiffrement RSA asymétrique d’après les algorithmes de ce [document](https://jpq.pagesperso-orange.fr/divers/rsa/rsa.pdf).

Donc pour le chiffrement SYMÉTRIQUE, la classe FERNET du module cryptography est utilisée et pour le chiffrement ASSYMÉTRIQUE, nous avons créé un module par nous même. D’ailleurs, quelques commentaires sont disponibles en début de module “chiffrement\_assymetrique.py” concernant les difficultés rencontrées lors de l'élaboration du module.

## Embellissement du chat

À l'aide de Qt désigner il fallait essayer de créer une interface simple à utiliser.

Or comprendre comment créer une interface avec cet outil n'est pas chose aisée. Cet donc après avoir appris les bases que le véritable travail à commencé. Mais une fois avoir compris comment utiliser l'outil la tâche fut plutôt simple à réaliser.

# Bilan

Bien que ce projet nous a permis de se rappeler certaines notions apprises tout au long de l'année, le fait qu'il nous force à découvrir de nouveaux outils tel que Qt désigner est une bonne chose

Ce projet était sympathique pour finir l'année.