**LYCEE LA SALLE PASSY BUZENVAL**



***Projet :***

***CRYPTOMESSENGER***



**Terminale**

**Concours Labex Digicosme**

**Spécialité Informatique et Sciences du Numérique**

**Le 2 juillet 2018**

**Groupe de travail :**

*Paul Nadal*

*Julien Marzal-Hilaire*

*Donatien Philippo*

1. Présentation du projet

Le projet CryptoMessenger est un projet de réalisation d’un logiciel de communication entre plusieurs ordinateurs avec comme particularité le fait de proposer la possibilité de crypter les messages avec des méthodes de cryptage simples à utiliser tout en étant complexes à cracker.

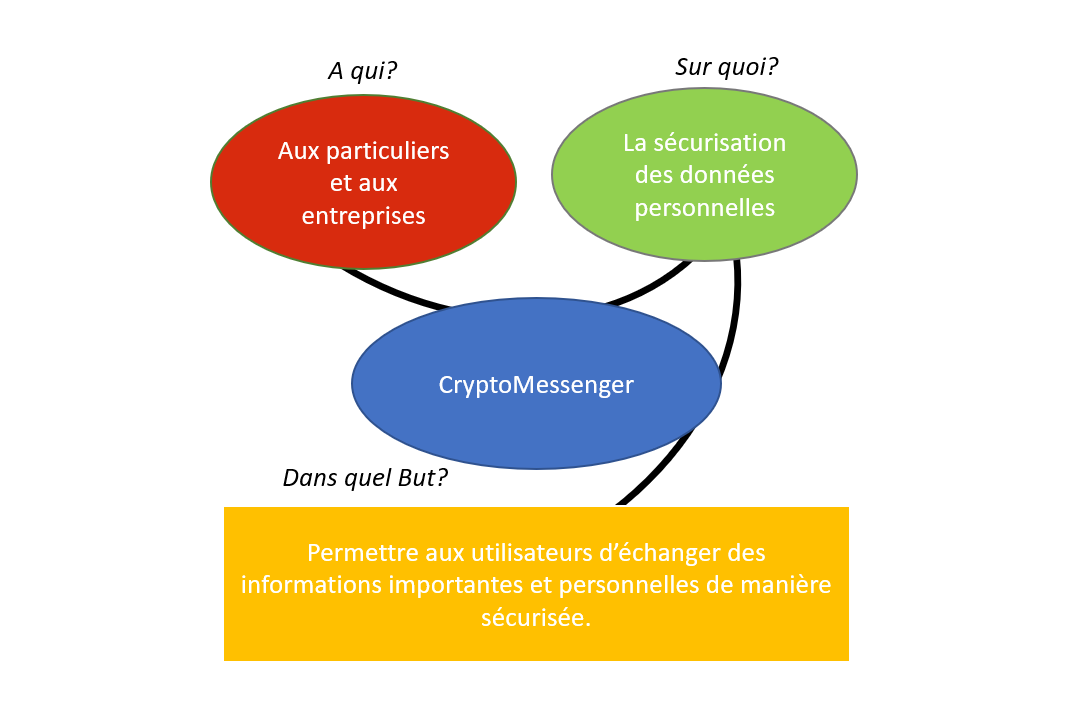
1. Démarche de projet
2. Analyse du besoin

La protection des données et de la confidentialité représente un enjeu important de la communication dans la société actuelle. La communication tenant elle-même une place prépondérante, le cryptage est nécessaire, notamment avec l’essor d’internet, des ordinateurs et des programmes en tout genre, certains servant de logiciel espion pour des sociétés peu scrupuleuses qui vendent ensuite ces informations confidentielles à des publicitaires ou tout autre fournisseur de service nécessitant des informations sur les utilisateurs.

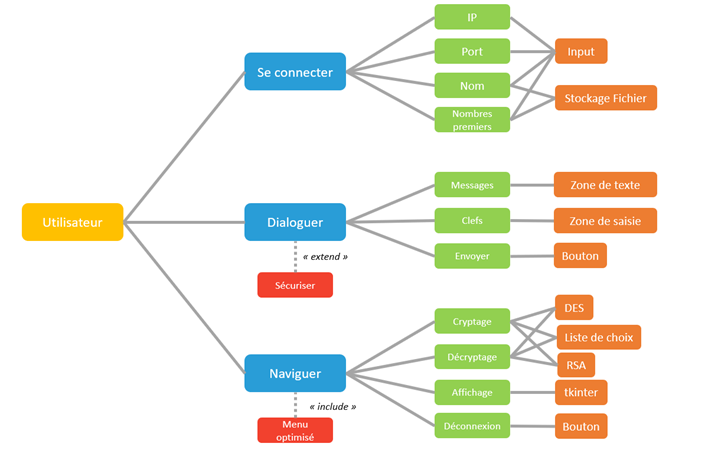
Pour la sécurisation des données conservées sur l’ordinateur, il existe déjà des solutions comme les antivirus qui repèrent les logiciels malveillants.

Cependant, il reste un problème majeur, celui du transport des données, c’est-à-dire qu’il est simple de récupérer des données pendant leur transit entre les deux communicants. Notre programme répond donc à ce besoin de confidentialité en proposant à l’utilisateur de crypter lui-même ses données avant même qu’elles ne soient envoyées. Elles seront ainsi plus compliquées à récupérer.

1. Cahier des charges, contraintes et moyens.

A partir de la définition du besoin, nous avons créé le diagramme « bête à cornes » suivant :

Pour notre projet, nous nous sommes donnés pour contrainte d’utiliser le python comme langage de programmation, de faire une interface graphique complète pour rendre l’utilisation de notre logiciel agréable, et de permettre à 2 personnes ou plus de communiquer.

Nous avons choisi de nous servir de Tkinter pour faire l’interface graphique car c’est un module très utilisé donc pour lequel il est simple de se documenter en cas de souci. Pour simplifier la lisibilité de notre code, nous avons créé un module contenant nos méthodes de cryptage.

Pour la communication entre les utilisateurs, nous pensions faire un client qui fasse aussi office de serveur mais nous sommes finalement partis sur un serveur séparé du client. Nous avons mis en place un Raspberry Pi qui permet de faire tourner le serveur en permanence afin que les utilisateurs puissent se connecter à distance (IP : 176.144.205.251 ; PORT : 60000). Pour le stockage des données à utiliser sur le long terme comme les clefs de cryptage du RSA et le nom de l’utilisateur nous avons choisi d’utiliser le module Pickle qui permet de stocker dans un fichier les variables en tant qu’objets et non en tant que texte. Nous avons ainsi pu faire le diagramme utilisateur ci-dessous.

1. Répartition des tâches

Après avoir trouvé l’idée de notre logiciel CryptoMessenger, nous nous sommes lancés dans la recherche d’une méthode de cryptage que nous pourrions implémenter dans notre programme. Nous avons tous travaillé sur la transmission des données (code du serveur et du client) car ce code était la base même de notre programme.

|  |  |  |
| --- | --- | --- |
| Paul | Julien | Donatien |
| Cryptage DES | Interface Tkinter | Cryptage RSA |
| Client + Serveur | | |

1. Contenu du projet

Avec ce dossier, vous trouverez les éléments suivants :

* Une vidéo explicative permettant de prendre en main notre logiciel
* Le code source du serveur : Serveur.py (qui n’est pas à exécuter car il tourne actuellement sur un Raspberry Pi auquel vous pouvez directement vous connecter)
* Le code source du logiciel CryptoMessenger : CryptoMessenger.py (à exécuter via Python ou EduPython)
* Le module de cryptage : encryption2.py qui se trouve dans le même dossier que le programme CryptoMessenger.py.

1. Contact

Elèves :

Paul NADAL : [paul.nadal@passy-buzenval.com](mailto:paul.nadal@passy-buzenval.com)

Julien MARZAL-HILAIRE : [julien.marzal-hilaire@passy-buzenval.com](mailto:julien.marzal-hilaire@passy-buzenval.com)

Donatien PHILIPPO : [donatien.philippo@passy-buzenval.com](mailto:donatien.philippo@passy-buzenval.com)

Enseignant :

Nicolas Didrit : [n.didrit@passy-buzenval.com](mailto:n.didrit@passy-buzenval.com)