**VIDEO PROJET ISN :**

Bonjour et bienvenue sur la vidéo explicative du logiciel CryptoMessenger, que nous avons développé en langage PYTHON pour notre projet d’ISN.

Qu’est-ce que CryptoMessenger ?

CryptoMessenger est un programme de communication sécurisé permettant d’échanger avec un groupe de personnes connectées sur un même serveur. Les utilisateurs peuvent crypter les messages avant de les envoyer aux autres.

La connexion

Voici la page d’accueil de notre logiciel : l’écran de connexion.

N’importe quel ordinateur peut se connecter à un serveur distant tant qu’il dispose de l’adresse IP et du PORT de l’ordinateur hébergeant le serveur. Il faut donc faire tourner le SERVEUR en permanence afin que les utilisateurs puissent se connecter à tout moment. Pour le fonctionnement de ce programme, nous avons mis en place un Raspberry Pi qui fait tourner en permanence le serveur distant.

La page de connexion demande 5 entrées : l’adresse IP et le PORT comme expliqué précédemment. Vous pouvez aussi sélectionner directement ces paramètres dans le tableau situé à droite qui enregistre tous les paramètres des serveurs auxquels vous vous êtes déjà connectés.

---------------------------------------------------------------------------------------------

Puis, il faut rentrer son nom d’utilisateur qui sera vu par les autres personnes connectées

(ici, prenons par exemple Arthur).

Enfin, il faut rentrer 2 nombres premiers qui permettent de former une clef publique et une clef privée qui servira pour le cryptage des messages en RSA, que nous expliquerons dans la suite de la vidéo (nous prendrons par exemple les nombres 101 et 331).

--------------------------------------------------------------------

Ces 3 derniers paramètres sont enregistrés par défaut dans un fichier crypter et il n’est pas nécessaire de retaper à chaque fois le nom et les chiffres premiers. Si vous voulez cependant changer ces valeurs, vous pouvez en saisir des nouvelles, qui seront à nouveau enregistrées.

Lorsque cela est fait, appuyez sur le bouton CONNEXION afin de vous connecter et d’accéder à l’interface MESSAGERIE !

L’interface

Vous voici maintenant sur la page la plus importante de notre programme : celle sur laquelle vous allez pouvoir envoyer et recevoir des messages cryptés.

En haut à gauche, la zone de texte est celle sur laquelle vous verrez tous les messages envoyés et reçus. Juste en-dessous, la barre de saisie permet d’écrire les messages. Si vous voulez envoyer un message sans le crypter, tapez votre texte et appuyer sur la touche ENTREE.

Vous verrez votre message apparaître dans la zone de texte située au-dessus.

Ici, nous pouvons constater qu’un autre utilisateur s’est connecté : Marty, et qu’il a envoyé un message en clair.

Cryptage d’un message

Nous avons instauré une règle afin de sécuriser un maximum les messages que nous envoyons mais vous pouvez adopter votre propre méthode. Il faut tout d’abord taper en clair le nom de l’utilisateur à qui vous voulez envoyer le message.

A droite, vous pouvez voir un tableau avec deux méthodes de cryptage : le RSA et le DES. Ce sont deux méthodes de cryptage ultra sécurisées et pratiquement « incraquables » sans les clefs de cryptage.

-----------------------------

Commencez par taper dans la barre de saisie supérieure le message que vous souhaitez crypter. Sélectionnez ensuite la méthode de cryptage DES dans le tableau à droite. Tapez ensuite la clef de cryptage de 8 caractères que vous souhaitez utiliser. Si vous tapez une clef de plus de 8 caractères, seuls les 8 premiers seront utilisés. Vous pouvez aussi utiliser une clef de cryptage de moins de 8 caractères.

Appuyez ensuite sur le bouton CRYPTER/ENVOYER.

------------------------------------------

Vous pouvez voir que le message crypté s’affiche dans la zone de réception.

Tapez ensuite dans la zone de saisie, la clef que vous avez utilisée pour crypter votre message afin que l’utilisateur à qui vous envoyez le message puisse le décrypter. Sélectionnez ensuite l’autre méthode de cryptage : le RSA.

Il faut maintenant rentrer la clef publique de l’utilisateur à qui vous souhaitez envoyer le message. Vous trouverez la clef publique à côté du nom des utilisateurs. Vous pouvez la copier/coller dans la zone de saisie de la clef ou bien sélectionner directement l’utilisateur dans la liste des personnes connectées et appuyer sur le bouton SELECTIONNER. Appuyez finalement sur CRYPTER/ENVOYER pour transmettre le message crypté.

ATTENTION : Seule la personne ayant la clef publique utilisée lors du cryptage pourra le décrypter.

Décryptage d’un message

Toute la partie décryptage se passe dans la partie inférieure de l’écran.

Pour décrypter un message, il va falloir tout d’abord décrypter la clef. Pour cela, cliquer sur le bouton TRANSFERER, situé au-dessus de la zone de décryptage afin de transférer le dernier message reçu dans la zone de saisie de la partie décryptage. Sélectionnez la méthode de décryptage RSA et cliquez sur le bouton DECRYPTER. Vous pouvez vous apercevoir qu’aucune clef n’est demandés car le décryptage se fait grâce à la clef privée de l’utilisateur qui est stockée sur son ordinateur et créée à partir des deux nombres premiers saisis sur l’écran de connexion.

La clef apparaît alors en clair dans la zone de texte inférieure et dans la zone de saisie des clefs de la partie décryptage.

Il ne reste plus qu’à décrypter le message. Pour cela, copier/coller le message crypté en DES de la zone de réception vers la zone de saisie de décryptage. Sélectionnez la méthode DES et appuyez sur DECRYPTER. Le message s’affiche finalement en clair dans la zone de texte inférieure.

Astuce

Pour différencier des messages cryptés en DES et RSA, il suffit de constater la forme du message reçu. S’il s’agit d’une suite de chiffres, c’est un cryptage par RSA. S’il s’agit d’une suite de chiffres et lettres minuscules, qui correspond à de l’hexadécimal, c’est un cryptage par DES.

Autres fonctionnalités

Une barre de menu est disponible pour faciliter l’utilisation de notre logiciel.

Le menu d’aide vous permet d’accéder à un mode d’emploi du logiciel, en cas d’oubli par exemple.

Vous pouvez aussi basculer en mode plein écran en appuyant sur le bouton prévu et rebasculer en fenêtré en appuyant sur la touche ECHAP, ou le bouton.

Enfin, le bouton quitter permet de se déconnecter du serveur et de fermer le fenêtre.

Remerciements

Nous vous remercions d’avoir écouté cette vidéo de présentation du logiciel CryptoMessenger.

Nous espérons qu’elle vous aura aidé à prendre en main notre logiciel et que notre projet vous plaira.