Documentation technique – Application de messagerie sécurisée

1. Choix de conception

a. Objectifs du projet

Cette application permet à des utilisateurs de communiquer en toute sécurité, avec des messages chiffrés, la possibilité de traduire des messages dans plusieurs langues, et même d'envoyer des photos chiffrées. L'interface est simple et intuitive, tout en assurant une sécurité maximale.

b. Langage, architecture et structure du projet

Langage utilisé : Python

Architecture : Programmation Orientée Objet (POO)

Structure du projet :

MESS/

mess/

clients/ → Gestion des comptes utilisateurs

core/ → Chiffrement, logique des messages, sécurité

db/ → Gestion de la base SQLite

ui/ → Interface utilisateur

main.py → Point d'entrée de l'application

Chaque dossier a une responsabilité spécifique :

- clients : inscription, connexion, gestion des infos utilisateur.

- core : gestion du chiffrement (RSA + AES), traduction, traitement des photos.
- db : connexion SQLite et création des tables.
- ui : menus d'interaction, affichage et saisie utilisateur.

2. Lancement du projet

1. S'assurer d'avoir Python installé (version 3.10 ou plus).
2. Installer les dépendances :

pip install bcrypt cryptography googletrans==4.0.0rc1

3. Lancer l'application :

python main.py

3. Sécurisation de l'application

a. Hachage des mots de passe

Les mots de passe sont hachés avec Bcrypt avant d'être stockés. Cela évite le stockage en clair et ajoute un salt pour chaque mot de passe, ce qui empêche les attaques par dictionnaire.

b. Chiffrement hybride RSA + AES

Les messages et images sont chiffrés avec un chiffrement hybride :

- AES est utilisé pour chiffrer les données (rapide et efficace).
- RSA est utilisé pour chiffrer la clé AES et l'IV.
- Chaque message est donc stocké sous forme chiffrée dans la base de données.

Pourquoi le type LONGBLOB ?

Les données chiffrées, notamment les images, peuvent contenir des caractères binaires et spéciaux issus de différentes langues ou systèmes. Le type LONGBLOB permet de stocker ces données en toute sécurité sans perte d'information.

c. Cryptage et enregistrement des images

Les images sont également chiffrées de manière hybride :

- Chacune est chiffrée deux fois : une fois pour l'émetteur, une fois pour le destinataire.
- Clé et IV AES sont chiffrés avec la clé RSA du destinataire.
- Stockage dans la table images avec les champs :
    - encrypted_key_for_receiver, encrypted_iv_for_receiver, encrypted_image_for_receiver
    - encrypted_key_for_sender, encrypted_iv_for_sender, encrypted_image_for_sender

Cela permet à chaque utilisateur de relire ses images chiffrées en toute autonomie.

d. Authentification sécurisée

- Vérification des identifiants avec des messages d'erreur génériques.
- Aucun mot de passe n'est stocké ou affiché en clair.

4. Fonctionnalités avancées

a. Traduction des messages

L'utilisateur peut choisir une langue (ex : anglais, espagnol, arabe, etc.) avant d'envoyer un message.

Fonctionnement :

- Utilisation de l'API googletrans.

- Le texte est traduit dans la langue cible avant chiffrement.
- Le message reste confidentiel même après traduction.

b. Envoi d’images

L’utilisateur peut :

- Choisir une image, elle est convertie en base64, puis chiffrée.
- Le destinataire pourra la déchiffrer uniquement avec sa clé privée RSA.

c. Messagerie classique

- Création de compte.
- Connexion sécurisée.
- Liste des utilisateurs disponibles.
- Envoi et réception de messages (texte ou images).
- Modification du mot de passe ou email.

5. Tests et validation

a. Tests unitaires

- Génération des clés RSA.
- Hachage/validation des mots de passe.
- Chiffrement et déchiffrement des messages et images.

b. Tests fonctionnels

- Connexion multi-utilisateurs.
- Envoi et lecture de messages/images.
- Changement des infos utilisateurs.

c. Tests de sécurité

- Tentative d’accès sans les clés privées → déchiffrement impossible.
- Vérification que les données en base sont bien chiffrées.
- Test du comportement en cas d’erreurs (mot de passe, mauvais identifiant…).

6. Mesures de sécurité globales

- Confidentialité : chiffrement bout-en-bout pour les messages et images.
- Authenticité : utilisateurs identifiés par leurs clés et mots de passe hachés.
- Résilience : base protégée par des données chiffrées en LONGBLOB.