

# Mini-Projet : Système de Messagerie Chiffrée

---

Membres du groupe :

- Mohammed Abdulatef Azan
- THOLFAQAR ABDURAHMAN SAEED THABIT

Date : 18/04/2025

## 1. Sujet du projet

Le projet consiste à concevoir et développer un système de messagerie chiffrée permettant à deux utilisateurs d'échanger des messages de manière sécurisée à l'aide de l'algorithme AES.

## 2. Points de concentration du projet

- Étude et implémentation du chiffrement symétrique avec AES.
- Génération et gestion sécurisée d'une clé de chiffrement.
- Développement d'un système d'envoi/réception de messages chiffrés.
- Ajout optionnel d'une interface graphique avec Tkinter.

## 3. Méthode de travail adoptée

Le projet sera développé en plusieurs étapes selon la méthodologie incrémentale :

- D'abord une version de base en ligne de commande (CLI).
- Ensuite une version avec interface graphique Tkinter (optionnelle).
- Le développement sera découpé en modules : gestion des clés, chiffrement, échange de messages, interface.

## 4. Outils et technologies utilisés

- Langage de programmation : Python
- Bibliothèque de chiffrement : cryptography (AES-GCM)
- Interface graphique : Tkinter (optionnel)
- Environnement : VS Code, Python 3.x

- Outils de gestion des fichiers : système de fichiers local (.key, .txt)

## 5. Planning du projet

| Étape   | Tâches   |
|---------|--|
| Étape 1 | Compréhension d'AES, génération de la clé, création du module key_manager.py   |
| Étape 2 | Implémentation des fonctions de chiffrement/déchiffrement dans crypto_utils.py |
| Étape 3 | Création du système de messagerie en ligne de commande                         |
| Étape 4 | Ajout optionnel de l'interface graphique avec Tkinter                          |
| Étape 5 | Tests, finalisation, documentation et préparation à la présentation finale     |