# **Programme de Chiffrement Hybride**

## **Présentation Générale**

Ce programme de chiffrement a pour but de renforcer la confidentialité et la sécurité des fichiers sensibles. Il peut notamment être utilisé pour protéger des documents tels que les dossiers médicaux de patients ou encore des fichiers confidentiels dans un cabinet juridique, ou simplement le stockage de fichier sensible

## **Objectif du Projet**

L’objectif principal de ce projet est de chiffrer des fichiers de manière sécurisée, de façon à ce qu’ils ne puissent être déchiffrés qu’à l’aide d’une clé privée.  
 Une fois le chiffrement effectué, il devient pratiquement impossible d’accéder au contenu du fichier sans disposer de cette clé.

## **Public Cible**

* Établissements hospitaliers
* Cabinets juridiques
* Infrastructures gouvernementales
* Entreprises manipulant des données sensibles

## **Analyse des Besoins**

Le programme devra :

* Être capable de chiffrer un fichier texte (.txt) fourni par l’utilisateur.
* Générer un fichier chiffré en sortie (resultat.txt).
* Chiffrer séparément la clé de chiffrement, stockée dans un fichier à part (key.txt).

️ En raison de la complexité et du nombre d’opérations effectuées, il est possible que le programme présente des ralentissements selon la taille des fichiers traités.

**Fontionnalité du programme**

1. **Chiffrement du fichier texte (chiffrement asymetrique)**
2. **Génération d’une clé de chiffrement aléatoire (clé de session)**
3. Chiffrement de la clé de session via un chiffrement asymétrique
4. Stockage séparé des résultats

## **Technologies et Outils Utilisés**

* **Langage de programmation** : Python
* Ui design: pyqt5, qt designer, css and html