Suite de l'exercice 1 :

Etape annexes : chiffrement des clés secrètes avec algorythme asymétrique

Une étape clé de mon projet, visant à désidentifier les acteurs concernés, consiste à sécuriser les clés AES générées en les chiffrant à l'aide de l'algorithme asymétrique RSA. Un fichier texte est créé par le code pour stocker les clés AES, chiffrées à l'aide de la clé publique du destinataire prévu. Celui-ci pourra ensuite les déchiffrer à l'aide de sa clé privée, garantissant ainsi la confidentialité des clés AES partagées entre l'expéditeur et le destinataire. Ce processus repose sur un échange préalable des clés publiques entre les parties.

Remarque & axes d'amélioration :

Dans ce projet, la question de l'intégrité et de l'authenticité des contenus n'est pas abordée de manière explicite. Bien que certains pseudonymes soient hachés (notamment les plus sensibles), les données elles-mêmes ne sont que chiffrées en AES.

Une amélioration possible serait de mettre en place un mécanisme de signature électronique. Cela pourrait consister à hacher l'ensemble des données (par exemple avec SHA-256), puis à chiffrer ce hash avec une clé privée RSA (2048 bits). Ainsi, le destinataire serait en mesure de recalculer le hash des données reçues en utilisant le même hachage, puis de vérifier leur intégrité (contenu n'a pas été changé ou falsifié) et l'authenticité de la signature à l'aide de la clé publique de l'expéditeur.

Pour renforcer la sécurité, il serait judicieux de chiffrer la clé privée RSA de chaque utilisateur, par exemple à l'aide de l'algorithme 3DES.

Une alternative intéressante serait de s'appuyer sur un service de PKI (Infrastructure à Clés Publiques) pour gérer les certificats et garantir la fiabilité des échanges.