

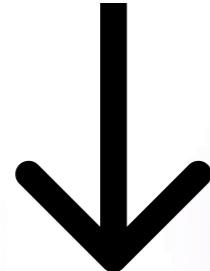
MiniRSA

Développement d'un système de **cryptographie asymétrique** avec signature numérique et génération de certificats en **Python**

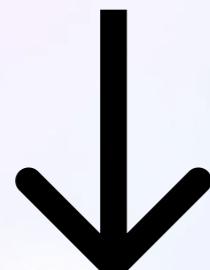
Outils / méthode



Implémentation des bases de la cryptographie asymétrique (clés publiques et privées, chiffrement, déchiffrement)



Implémentation de la signature numérique et d'un algorithme de hashage



Implémentation d'un certificat pour une clé publique, signé par une autorité de certification



Implémentation du test de primalité de Miller-Rabin.



Ajout de la prise en charge des messages textes pour le chiffrement, déchiffrement et signature.

README.md

SAÉ Mini RSA

Introduction :

Dans le cadre du module de cryptographie R3.09, nous avons développé le projet Mini RSA visant à implémenter, en Python, un chiffrement RSA pour une communication entre deux personnes (Alice et Bob), incluant une vérification via un organisme certificateur ainsi que la création d'empreintes pour authentifier les messages.

Le chiffrement RSA est une méthode de chiffrement asynchrone à clé privée/publique qui repose sur les problèmes de factorisation et de racine ième modulaire impliquent des fonctions à sens unique avec brèche secrète.

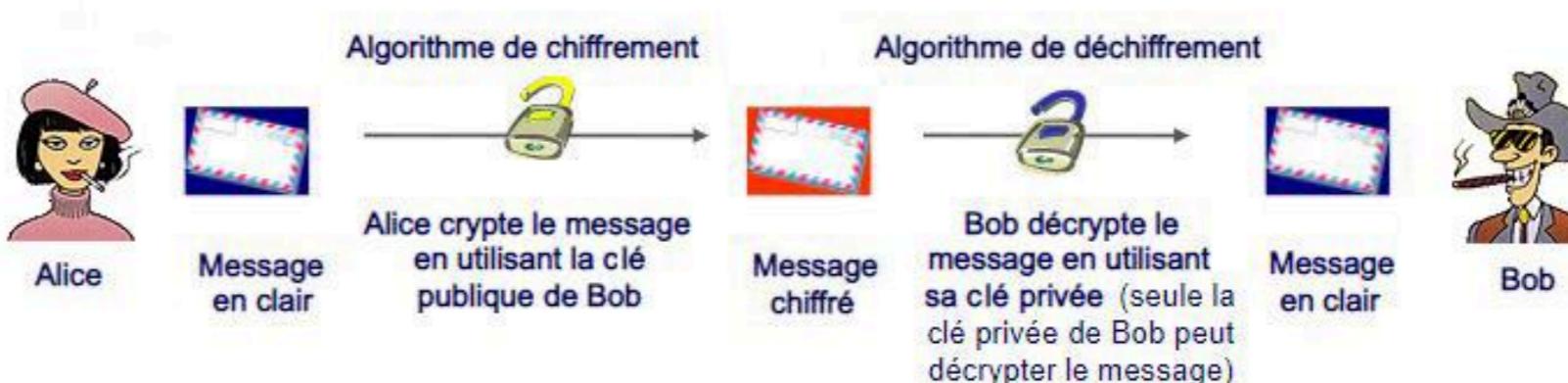


Figure : README du projet

Résultat :

Un système fonctionnel de cryptographie asymétrique capable de : chiffrer et déchiffrer des messages, générer et vérifier des signatures numériques, créer et valider des certificats publics via un organisme certificateur.

Compétences acquises :

- Maîtrise des concepts de cryptographie asymétrique et des mathématiques associées
- Gestion de projet collaboratif avec Git/Git
- Programmation orienté objet en Python
- Réalisation de tests unitaires avec Pytest

Améliorations possibles :

- Optimisation des algorithmes pour des messages de grande taille.
- Ajout d'une interface utilisateur
- Étendre le projet pour inclure des fonctionnalités réseau simulées