14X040 Securité avancé - Sujet

David Papa

March 2025

1 Description

Le but du projet est d'exploiter de l'encryption homomorphique et de réaliser :

- Differentes implémentations d'algorithmes homomorphique permettant d'effectuer des opérations simple, soit des additions soit des multiplications : Unpadded RSA, ElGamal, Goldwasser–Micali, Benaloh, Paillier.

- Utiliser une encryption homomorphe plus complexe avec la librairie `TenSEAL` de python pour pourvoir effectuer des additions et des multiplications avec la même encryption.

Ensuite, le but serait de comparer leurs performances (rapidité, mémoire) entre elles ainsi qu'avec des opérations non encryptés. Evaluer la scalabilité de ces méthodes (avec des grands nombres) et mettre en avant leur utilité.