TP : Introduction à la Cryptographie en python

Rushed Kanawati

11 juin 2024

Résumé

L'objectif de ce TP est de comprendre le fonctionnement des algorithmes de chiffrement symétriques et asymétrique et leusr utilisation dans des programmes python.

Chiffrement symétrique

1. Donner une fonction python `cesar_chiffre(t)` qui permet de chiffrer le message `t` en appliquant l'algorithme de chiffrement de césar.
2. Donner une fonction python `cesar_dechiffre(m)` qui permet de déchiffrer un message chiffré avec le code de césar.
3. Donner une fonction python `vigenere_chiffre(t)` qui permet de chiffrer le message `t` en appliquant l'algorithme de chiffrement de Vigenère.
4. Donner une fonction python `vigenere_dechiffre(t)` qui permet de déchiffrer un message `M` chiffré avec le code de Vigenère.

Chiffrement asymétrique

1. Donner une fonction python `sign(t)` qui permet de signer un message t en utilisant l'algorithme `RSA`.
2. Donner une fonction `sig_valide(c)` qui permet de vérifier si un document signé est valide.