

Sécurité et Cryptographie :

TP SDES

L'objectif du TP est d'implémenter une version simplifiée de DES.

Dans un langage de votre choix développez

- Une fonction qui prends en entré un bloc de 8 bits (un octet) et une clé de 10 bits et qui retourne 8 bits chiffrés.
- Une fonction de déchiffrement
- Une fonction main qui montre l'utilisation en chiffrant et déchiffrant un texte.
- Vos sous-fonctions doivent être optimales. Utilisez des opérations sur les bits.