Aurélien DUVAL

TP1 : Cryptographie et sécurité informatique

Exercice 2 : Modes de chiffrement

Pour les modes de chiffrement CBC, CFB, OFB la colonne c_0 n'est pas renvoyée concaténée au message de sortie mais est donnée sous le nom de vecteur d'initialisation. Afin de décrypter un message dans ces modes, merci de replacer le vecteur d'initialisation comme si il s'agissait d'un chiffrement et de ne pas le placer dans le message à déchiffrer.