

Cryptographie Symétrique

Intervenant : Michael FRANÇOIS (francois@esiea.fr)

TDO4 -- AES

Pendant tout ce TDO on utilisera l'AES-128 et la fonction classique `ShiftRows()` a été remplacée par une autre fonction `ShiftRows2()`. La clé à utiliser est la suivante : j'adore l'AES :)

EXERCICE 1 : (Déchiffrement d'un bloc de 128 bits depuis un fichier -- 10 pts) \Rightarrow 1h30

Pour cette partie il faut remplir le corps de la fonction `InvShiftRows2()` (resp. `InvCipher()`), qui est la fonction inverse associée à `ShiftRows2()` (resp. `Cipher()`). Concernant `ShiftRows2()`, il faut comprendre d'abord comment fonctionne concrètement cette fonction, avant de l'inverser. Une fois les fonctions inverses écrites, déchiffrer le fichier "chiffre1" en utilisant le choix 2 dans le menu proposé.

EXERCICE 2 : (Déchiffrement d'un fichier en fonction du mode -- 10 pts) \Rightarrow 1h30

- 1. Remplir le corps de la fonction `InvCipher_Mode_1()` puis déchiffrer le fichier "chiffre2" en utilisant le choix 6 du menu. Quel est le mode opératoire employé dans `Cipher_Mode_1()` ?
- 2. Remplir le corps de la fonction `InvCipher_Mode_2()` puis déchiffrer le fichier "chiffre3" en utilisant le choix 6 du menu. Quel est le mode opératoire employé dans `Cipher_Mode_2()` ?