

# Cryptographie Symétrique

Intervenant : Michael FRANÇOIS ([francois@esiea.fr](mailto:francois@esiea.fr))

## TDO2 -- Chiffrement par Substitution

### EXERCICE 1 : (Chiffrement/Déchiffrement par substitution -- 10 pts) ⇒ 1h30

C'est un chiffrement par substitution dont les lettres sont substituées par paire, exemple : a est substituée par h, et h est substituée par a, b par m et m par b, etc. Avant de déchiffrer un message dont la clé est connue et donnée dans le fichier "cle1.txt", il faudra d'abord remplir le corps de certaines fonctions.

- 1. Remplir le corps des fonctions `Determination_long_texte`, `Lire_et_charger_texte`, `Ecrire_chiffre` et `Lire_cle` se trouvant dans le fichier "FONCTIONS\_COMMUNES.c".
- 2. **Chiffrement** : remplir le corps de la fonction `Chiffrer_substitution` dans le fichier "CHIFFREMENT.c". Chiffrer le fichier "clair1.txt" en utilisant la clé contenue dans le fichier "cle1.txt". Pour cela, il suffit juste de suivre les instructions (choix E) du programme et de répondre au fur et à mesure.
- 3. **Déchiffrement** : remplir le corps de la fonction `Dechiffrer_substitution` du fichier "CHIFFREMENT.c". Déchiffrer le fichier "chiffre2.txt" en utilisant la clé contenue dans le fichier "cle2.txt". Pour cela, il suffit juste de suivre les instructions (choix D) du programme et de répondre au fur et à mesure.

NB : si le texte clair obtenu n'a aucun sens, ce que le déchiffrement s'est mal passé, dans ce cas revoyez votre code.