

Université de Valenciennes et du Hainaut-Cambrésis
Institut des Sciences et Techniques ISTV

Master 2 TNSI – FA

TD/TP de Cryptographie

2016 – 2017

Consignes :

- Langage libre **MAIS** dans tous les cas il n'est pas autorisé de réutiliser des fonctions prédéfinies du langage répondant à certaines questions.
- Les fichiers sources des TP seront à déposer sur Moodle (avec un ReadMe indiquant comment générer l'exécutable).
- Les énoncés ne rentrent volontairement pas trop dans les détails, vous laissant une certaine liberté sur les situations que vos algorithmes permettent de gérer. Le niveau de détail de vos algorithmes ainsi que les fonctionnalités offertes influenceront sur la notation du TP. Hypothèse la plus réductrice autorisée : le texte est formé uniquement de lettres majuscules (pas de ponctuation, d'accents, de symboles, de chiffres, ...) et regroupé par blocs de 5 lettres.
- Dans tous les cas il faudra veiller à bien indiquer dans un mémo, ou à défaut dans les commentaires de vos fonctions, quels sont les cas gérés par vos méthodes.

Exercice 1 : chiffrement de César

1. Ecrire une fonction permettant de chiffrer un texte fourni, avec une clé donnée.
2. Ecrire une fonction permettant de déchiffrer un texte chiffré, connaissant la clé.
3. Ecrire une fonction permettant de décrypter un texte chiffré.

Exercice 2 : chiffrement par permutation

1. Ecrire une fonction permettant de chiffrer un texte fourni, avec une clé donnée.
2. Ecrire une fonction permettant de déchiffrer un texte chiffré, connaissant la clé.
3. Ecrire une fonction qui permet de calculer la fréquence d'apparition des lettres dans un texte donné.
4. Ecrire une fonction dont le but est de décrypter un texte chiffré, en utilisant la technique vue en cours et utilisant la fréquence d'apparition des lettres.

Exercice 3 : Vigenère

1. Ecrire une fonction permettant de chiffrer un texte fourni, avec une clé donnée.
2. Ecrire une fonction permettant de déchiffrer un texte chiffré, connaissant la clé.