Cryptographie Symétrique

(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 :** decommenter puis remplir les "`??????`" se trouvant dans 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 :** decommenter puis remplir les "`??????`" se trouvant dans 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.

EXERCICE 2 : (Cryptanalyse - - 10 pts) ⇒ 1h30

Le but ici est de déchiffrer le message contenu dans le fichier "`chiffre3.txt`". Évidemment, on ne possède pas la clé qui a été utilisée lors du chiffrement, donc à vous de la trouver.

► **1.** Remplir le corps des fonctions `Compter_lettre`, `Compter_bigramme`, `Affiche_clair` se trouvant dans le fichier "`CRYPTANALYSE.c`".

► **2.** Remplir également les `??????` dans la fonction `Cryptanalyse` après avoir decommenté la ligne correspondante.

► **3.** Lancer la cryptanalyse (choix C) et suivre les instructions afin de retrouver la clé et le message original, liés au fichier chiffré "`chiffre3.txt`".
Pour vous aider sur la cryptanalyse : voici un exemple sur 10000 lettres, du nombre d'apparition de quelques bigrammes :

es	⇒	305	le	⇒	246	en	⇒	242	de ⇒ 215	re	⇒	209
nt	⇒	197	on	⇒	164	er	⇒	163	...	...		