Master Spécialisé SIS
Semestre 1
17/11/2021

ESIEA Paris/Ivry-sur-Seine
Année 2021/2022

Cryptographie Symétrique

Intervenant : Michael FRANÇOIS (francois@esiea.fr)

TDO1 -- Chiffrement de Vigenère

EXERCICE 1 : (Chiffrement/Déchiffrement de Vigenère -- 10 pts) ⇒ 1h30

L'objectif pour cet exercice est de remplir quelques fonctions de base déjà données, puis d'essayer de chiffrer (resp. déchiffrer) un message dont la clé est connue et donnée dans le fichier "cle1.txt" (resp. "cle2.txt").

- **1.** Remplir les corps des fonctions se trouvant dans le fichier "FONCTIONS_COMMUNES.c". Le plus simple est d'isoler ces fonctions dans un nouveau fichier .c, les remplir puis les tester, et si tout est ok, les copier dans le fichier principal "FONCTIONS_COMMUNES.c".
- **2. Chiffrement :** remplir le code de la fonction `Chiffrement_vigenere` dans le fichier "CHIFFREMENT_VIGENERE.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 code de la fonction `Dechiffrement_vigenere` du fichier "CHIFFREMENT_VIGENERE.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 de Vigenère -- 10 pts) ⇒ 1h30

Le but ici est de déchiffrer le message contenu dans le fichier "chiffre3.txt". Évidemment, on ne possède pas la clé (*i.e.* "cle3.txt") qui a été utilisée lors du chiffrement, donc à vous de la trouver. On va utiliser un outil qui aide à l'analyse d'un texte chiffré via la méthode de Vigenère.

- **1.** Remplir le corps des fonctions :
  `compter_lettre`, `indice_coincidence` et `extraction_sous_texte`. Ces fonctions se trouvent dans le fichier "CRYPTANALYSE_VIGENERE.c".
- **2.** Lancer la cryptanalyse (choix C) et suivre les instructions, afin de retrouver la clé et le message original liés au fichier chiffré "chiffre3.txt".