TP N° 1
Cryptographie Artisanale

TP à rendre au plus tard le **28 / 11 / 2021** à l'adresse : crypto.qi.bc@gmail.com

N.B Écrire les solutions proposées en langage Python.

Exercice 1: Chiffre de César

1. Écrire une fonction qui prend en paramètre une chaine de caractère **ch** ainsi qu'un nombre de décalage **k** (entre 1 et 25) et retourne la chaine ch cryptée par le chiffre de César de décalage k.
2. En déduire un programme qui lit une chaine de caractères ch et lui applique le cryptage et le décryptage en affichant à chaque étape le résultat.
3. Écrire un programme qui cryptanalyse un message intercepté en supposant que ce dernier a été crypté par le chiffre de César.

Exercice 2: Chiffrement par Substitution Mono-Alphabétique

1. Écrire une fonction qui génère aléatoirement une table de substitution mono-alphabétique **Tab** (Attention : éviter les répétitions)
   Ex :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
F	Q	B	M	X	I	T	E	P	A	L	W	H	S	D	O	Z	K	V	G	R	C	N	Y	J	U

2. Écrire un programme qui lit un fichier texte (.txt) et crypte son contenu par un chiffrement par substitution mono-alphabétique via la table Tab et range le résultat dans un autre fichier text.
3. Écrire une fonction qui calcule la fréquence d'apparition des lettres dans un text et range le résultat pour un traitement ultérieur. (Ne pas compter les espaces)
4. En se basant sur la table de fréquences de la langue utilisée pour la rédaction du texte, tenter de cryptanalyser un fichier intercepté en supposant qu'il a été crypté par substitution mono-alphabétique.

   Exemple approximatif pour la langue française :

E	S	A	I	N	T	R	U	L	O	D
14.69%	8.01%	7.54%	7.18%	6.89%	6.88%	6.49%	6.12%	5.63%	5.29%	3.66%

Exercice 3 : Chiffrement de Vigenère

Écrire l'algorithme de Vigenère tel que :

- La clé et le texte à chiffrer seront passés en paramètres.
- Mettre le résultat du chiffrement dans un fichier texte.
- Ecrire un programme permettant le déchiffrement d'un texte chiffré.

Exercice 4: Chiffre Homophone

1. Écrire une fonction qui génère aléatoirement un tableau de substitution **Tab** de 0 à 99 (voir cours). Attention : éviter les répétitions.
2. Écrire une fonction qui crypte un texte par un chiffre homophone en se basant sur la table Tab. Cette fonction doit choisir d'une manière uniforme les choix de substitution.

   i.e : ne pas choisir un nombre une deuxième fois avant que tous les autres nombres soient choisis au moins une fois.

   Dans l'exemple du cours pour la lettre D, les choix possibles sont 01, 03, 45, 79
3. Refaire les questions 1. et 2. :
   a. En utilisant un carré de Polybe (initialisé manuellement ou aléatoirement)
   b. En utilisant l'alternative 2 (voir cours)

Exercice 5: Chiffre de Hill (m = 2)

1. Écrire une fonction qui retourne l'inverse d'un nombre n dans Z/26Z s'il existe et 0 sinon.
2. Écrire une fonction qui génère une matrice Q inversible Z/26Z.
3. Écrire une fonction qui crypte un texte via le chiffre de Hill basé sur la matrice Q.
4. Écrire une fonction qui décrypte un texte via le chiffre de Hill basé sur la matrice Q.
5. Écrire un programme qui illustre les questions de 1. à 4.