INSTITUT PRÉPARATOIRE AUX ÉTUDES D'INGÉNIEURS DE TUNIS
ANNÉE UNIVERSITAIRE 2020 - 2021
FILIÈRES : SM-SP

Simulation Numérique
Cryptographie : Algorithmes de César et Vigenère

Partie 1 :

En cryptographie, le code de César est une méthode de chiffrement très simple utilisée par Jules César dans ses correspondances secrètes et basée sur le principe de décalage. Il s'agit de décaler les lettres de l'alphabet vers la gauche ou vers la droite d'une ou plusieurs positions. Le texte chiffré s'obtient en remplaçant chaque lettre du texte clair original par une lettre à distance fixe, toujours du même côté, dans l'ordre de l'alphabet. Pour les dernières lettres (dans le cas d'un décalage à droite), on reprend au début. Par exemple avec un décalage de 2 vers la droite, A est remplacé par C, B devient D, et ainsi jusqu'à W qui devient Y, puis Y devient A etc. Il s'agit d'une permutation circulaire de l'alphabet. La longueur du décalage constitue la clé du chiffrement.

Exemple :
Le texte ELEVE INGENIEUR devient GNGXG KPIGPKGWT (décalage de 2 vers la droite).

Dans la suite, nous allons considérer une variable globale intitulée alphabet contenant la chaîne "ABCDEFGHIJKLMNOPQRSTUVWXYZ" et représentant l'alphabet considéré. Les fonctions que nous allons implémenter laisseront inchangés les caractères hors de l'alphabet (espaces, ponctuation, minuscules etc).

1. Écrire une fonction PYTHON position(c) qui retourne la position du caractère c dans la chaîne alphabet. Dans le cas où le caractère n'existe pas, la fonction retourne la valeur 99.

2. Écrire une fonction PYTHON cesar_car(c,d) qui retourne le caractère c chiffré avec un décalage d selon l'alphabet considéré. Si le caractère c ne fait pas partie de l'alphabet, la fonction le laissera inchangé.

3. Écrire une fonction cesar(m,d) qui chiffre les caractères d'un texte m selon un décalage d

4. Écrire une fonction decesar_car(c,d) qui déchiffre un caractère c codé avec le décalage d.

5. Écrire une fonction decesar(m,d) qui déchiffre un texte m codé avec le décalage d.

Partie 2 :

Dans la suite du problème, nous allons réaliser le déchiffrement d'un texte chiffré ne connaissant pas la clé. Pour cela, il faudra déterminer la valeur de la clé automatiquement. L'approche la plus couramment employée, pour déterminer cette clé, se base sur l'hypothèse que la lettre 'E' est la lettre la plus fréquente dans un texte suffisamment long en français. Autrement dit, la lettre 'E' dans un texte clair correspond à la lettre la plus fréquente dans un texte chiffré. Ainsi, il suffit de calculer le nombre d'occurrence de chaque lettre dans le texte chiffré et d'en déduire la lettre la plus fréquente qui correspondra à la lettre 'E'.

1. Écrire une fonction PYTHON frequence(m) où m est un texte. Cette fonction doit retourner une liste L composée de tuples de deux éléments. Le premier élément du tuple représente un caractère de m et où le deuxième élément représente le nombre d'apparition du caractère dans m. On ne considérera que les caractères faisant partie de l'alphabet.

2. Écrire une fonction PYTHON lettre_frequente(L) où L est une liste de tuples de deux éléments (caractère et nombre d'apparition du caractère). Cette fonction doit retourner la lettre la plus fréquente de L.

3. Écrire une fonction PYTHON chercher_clef(m) qui cherche la clé d'un texte chiffré.

4. Écrire une fonction decesar_version2(m) qui déchiffre un mot m chiffré avec un code de César dont on ignore la clé.

Partie 3 :

Au XVII siècle, Blaise de Vigenère a modernisé le codage de César de la manière suivante : au lieu de décaler toutes les lettres du texte de la même manière, on utilise cette fois un texte clef qui va indiquer une suite de décalages. Prenons par exemple la clef CONCOURS. Pour chiffrer un texte, on code la première lettre en utilisant le décalage qui envoie la lettre 'A' sur la lettre 'C' (la première lettre de la clef). Pour la deuxième lettre, on prend le décalage qui envoie le 'A' sur 'O' (la deuxième lettre de la clef) et ainsi de suite. Lorsque la clef est totalement épuisée, on reprend la clef à partir de sa première lettre.

Exemple :

La première ligne du tableau suivant donne le texte à chiffrer. La deuxième ligne représente la clef utilisée et la troisième ligne représente le texte déchiffré selon la méthode de Vigenère.

E	L	E	V	E	I	N	G	E	N	I	E	U	R
C	O	N	C	O	U	R	S	C	O	N	C	O	U
G	Z	R	X	S	C	E	Y	G	B	V	G	I	L

1. Écrire une fonction vigenere(m,clef) qui chiffre un texte m avec la clef clef selon la méthode de Vigenère.

2. Écrire une fonction devigenere(m,clef) qui déchiffre un texte m codé avec la clef clef selon la méthode de Vigenère.