Travaux pratiques #3 — Le chiffre de Vigenère

Introduction — *Chiffrement par substitution*

Le *chiffrement par substitution* est une méthode de chiffrement consistant à remplacer une lettre du message non chiffré par une autre lettre de l'alphabet. Il existe de nombreuses méthodes de chiffrement par substitution, notamment mono (une lettre donnée est *toujours* remplacée par une même lettre) ou polyalphabétiques.

Chiffrement monoalphabétique — chiffre de César

Le chiffre de César fonctionne en décalant chaque lettre d'un nombre donné de lettres dans l'alphabet (modulo 26). Ce nombre est la **clé** du chiffrement.

Texte en clair CHIFFREDECESAR
Texte chiffré INOLLXKJKIKYGX

Phrases non ponctuées — EN MAJUSCULES

Seules des phrases **sans accent**, **sans ponctuation**, **sans espace** et **en majuscules** seront considérées.

$\mathcal{Q}_1$. Écrire une fonction `cesar` prenant en paramètre une chaîne de caractères, une clé de chiffrement et retournant la chaîne chiffrée.

La question

Chiffre de Vigenère. Un tel chiffrement n'est pas vraiment sécurisé. Si le message est intercepté -et que la personne sait qu'il a été chiffré avec cette méthode, 25 tests suffisent à trouver le message originel. Le **Chiffre de Vigenère** est une méthode de chiffrement polyalphabétique décrite par Blaise de Vigenère en 1586 et permettant d'augmenter la sécurité du chiffre de César. Dorénavant, une même lettre peut être chiffrée par différentes lettres. Le principe repose sur les deux objets suivants :

- la *table de Vigenère*, qui associe pour **toute** lettre de l'alphabet une substitution différente ;
- une **clé** plus grande que dans le chiffre de César, et permettant de chiffrer une même lettre différemment selon sa position dans le texte en clair.

La table de Vigenère consiste simplement à décaler l'alphabet d'un cran vers la droite. On obtient ainsi :

	Lettre en clair																								
	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
Clé	Lettres chiffrées (au croisement de la colonne Lettre en clair et de la ligne Clé)																								
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
...																										

La taille de la clé

La clé doit *nécessairement* être au moins aussi grande que le texte à chiffrer pour que cette méthode fonctionne. Il n'est cependant pas nécessaire d'avoir une clé plus longue que le texte : la répéter suffisamment de fois permet de faire fonctionner la méthode.

Chiffre de Vigenère — clé KRAFTWERK

Texte en clair	IMTHEOPERATORWITHMYPOCKETCALCULATOR
Clé	KRAFTWERKKRAFTWERKKRAFTWERKKRAFTWER
Texte chiffré	SDTMXKTVBKKOWPEXYWIGOHDAXTKVTUQTPSI

Implémentation

Dans un premier temps, l'objectif est de coder les méthodes de (dé)chiffrage de la méthode du chiffre de Vigenère. Une structure de code est proposée ci-dessous, mais en aucun cas imposée. Afin de simplifier la gestion de la table de Vigenère, l'alphabet sera considéré comme un ensemble de valeurs entières de 0 à 25.

$\mathcal{Q}_3$. Écrire une fonction `table_vigenere` construisant (et retournant) une table de Vigenère.

$\mathcal{Q}_4$. Écrire une fonction `chiffrer` prenant en paramètre une chaîne de caractères à coder, la table de Vigenère et la clé de chiffrement et retournant la chaîne de caractères chiffrée.
Remarque. Une fonction `generer_cle` *peut s'avérer utile*

$\mathcal{Q}_5$. Écrire une fonction `dechiffrer` prenant en paramètre une chaîne de caractères, la table de Vigenère et la clé de chiffrement et retournant la chaîne de caractères déchiffrée.

Structure du code — une proposition

Calcul de la chaîne (dé)chiffrée — `chaine`

Est-il réellement nécessaire de passer la table de Vigenère en paramètre ? Un jeu de modulo (en se souvenant que l'alphabet contient 26 éléments) peut permettre de l'éviter.

Il est possible d'augmenter la sécurité du chiffrement en utilisant une table aléatoire -seule la clé est nécessaire pour (dé)chiffrer le chiffre de Vigenère.

$\mathcal{Q}_5$. Modifier la méthode de chiffrement en faisant en sorte que expéditeur et destinataire possèdent tous deux une table de subsitution générée aléatoirement.

Modification.