Compléments au TP4 : le chiffre de Vigenère 1.

L'idée de Vigenère est d'utiliser un chiffre de César, mais où le décalage utilisé change de lettres en lettres. Pour cela, on utilise une table composée de 26 alphabets, écrits dans l'ordre, mais décalés de ligne en ligne d'un caractère. On écrit encore en haut un alphabet complet, pour la clé, et à gauche, verticalement, un dernier alphabet, pour le texte à coder :



Pour coder un message, par exemple cryptographie de vigenere, on choisit une clé qui sera un mot de longueur arbitraire; prenons mathweb. On écrit ensuite cette clé sous le message à coder, en la répétant aussi souvent que nécessaire pour que sous chaque lettre du message à coder, on trouve une lettre de la clé :

c	r	у	р	t	О	g	r	a	р	h	i	е	d	е	v	i	g	е	n	е	r	е
m	a	t	h	W	e	b	m	a	t	h	W	е	b	m	a	t	h	W	е	b	m	a

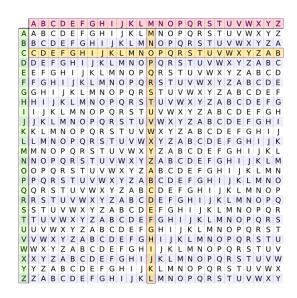
Pour coder, on regarde dans le tableau l'intersection de la ligne de la lettre à coder avec la colonne de la lettre de la clé.

Dans notre exemple, on commence par coder la lettre c; la clé est donnée par la lettre m.

On regarde dans le tableau l'intersection de la "ligne" C et de la "colonne" M : ainsi ce sera codé par o.

Ensuite, on code la lettre \mathbf{r} , dont la clé est \mathbf{a} ; la lecture du tableau donne la lettre \mathbf{r} (ligne \mathbf{R} et colonne \mathbf{A}).

Ainsi de suite : notre message sera codé par orrwpshdaioei eq vbnarfde.



^{1.} la présentation est issue du site bibmath.net

L'intérêt par rapport au codage de César est qu'une même lettre sera codée par plusieurs lettre différentes; par exemple ici e est codé par i, q, a, f et e. En conséquence, l'analyse des fréquences d'apparition n'a plus aucune utilité et ne permet pas de décoder le texte.

Remarques:

- ★ Dans la suite, on supposera que les textes sont sans espaces, sans majuscules, sans accents et sans ponctuation.
- ★ Récupérer le fichier vigenere.py disponible sur le site delphine.sembely.free.fr/tp.html et le stocker dans le dossier TP04. Ouvrir vigenere.py puis copier-coller son contenu dans le ficher TP04.py à la suite de votre travail sur le code de César.
- ★ On pourra bien sûr se servir avec profit des fonctions développées pour le décodage automatique de César.
- 1°) Écrire une fonction codage_vigenere d'arguments une clé (chaîne de caractères) cle et un message en clair texte. Cette fonction renverra le message codé selon Vigenère avec la clé cle.
- 2°) Écrire une fonction decodage_vigenere d'arguments une clé (chaîne de caractères) cle et un message codé texte (selon Vigenère avec la clé cle). Cette fonction renverra le message décodé.
- 3°) Écrire une fonction decodage_vigenere_ameliore d'arguments la longueur de la clé longueur et un message codé texte (selon Vigenère et une clé inconnue de taille longueur). Cette fonction renverra la clé et le message en clair.
- **4°)** Décoder message_vigenere qui a été codé avec la méthode de Vigenère, sachant que la clé possède 11 lettres.