

Objectif : Utiliser un tableur pour coder et décoder des messages à l'aide de deux méthodes de chiffrement : *chiffrement de César* et *chiffrement affine*.

Remarques sur le code ASCII :

- Chaque caractère a un code numérique qui est un nombre entier naturel compris entre 0 et 255.
- Les lettres majuscules ont un code ASCII compris entre 65 (pour A) et 91 (pour Z)
- Avec le tableur, la fonction CODE permet d'obtenir le code ASCII d'une lettre donnée (exemple : =CODE(« A ») affiche 65) et la fonction CAR donne le caractère correspondant à un code ASCII donné.(exemple : =CAR(91) affiche Z)
- Pour avoir le rang d'une lettre dans l'alphabet avec la convention : Rang 0 pour A et donc Rang 25 pour Z, on va utiliser le schéma suivant :



I) Chiffrement de César :

Principe : Chaque lettre du message en clair est remplacée par la lettre qui la suit trois rangs plus loin dans l'alphabet.

Remarque : Pour simplifier le travail, les messages à coder seront entrés sans ponctuation et sans espace.

a) Codage :

Préparer une feuille de calcul du type suivant :

	A	B	C	D
1	Texte clair :			
2	Rang de la lettre :			
3	Rang après codage :			
4	Texte chiffré :			

- En B1 C1 D1... on trouve les lettres du texte non codé
- En B2 : On tape =CODE..... (à compléter) pour avoir le rang de la lettre placée en B1
- En B3 : On tape =.....(à compléter) pour avoir le rang de la lettre après codage.
- En B4 : On tape =CAR.....(à compléter) pour obtenir la lettre codée.

Utilisation : A l'aide de cette feuille de calcul, coder le message suivant « LARITHMETIQUECESTFANTASTIQUE »

Message codé :

b) Décodage :

Préparer une deuxième feuille de calcul pour le décodage.

Utiliser cette feuille pour décoder le message suivant crypté par chiffrement de César :

ODVSHPDWKVFHVWOHSLHG

Message clair :

II) Chiffrement affine :

Principe :

- Chaque lettre du message en clair est remplacée par son rang dans l'alphabet. On note x le rang de la lettre dans le message en clair ($0 \leq x \leq 25$)
- On se donne une clé de codage : $(a;b)$, où a et b sont des entiers naturels
- On note y : le rang de la lettre codée. $y =$ reste dans la division euclidienne de $ax+b$ par 26 (ainsi, y sera compris entre 0 et 25)

1) Exemple de codage avec la clef (4;19) :

Préparer une feuille de calcul du type suivant :

	A	B	C	D	E
1	Clef de codage	$a=4$		$b=19$	
2	Texte clair :				
3	$ax+b$				
4	y				
5	Texte chiffré :				

Coder le message suivant : « LECALCULMATRICIELCESTLIDEAL »

Message codé :

Si on change la clef de codage en (30;45) que constate-t-on concernant le message codé ?

.....

En fait, $30 = 1 \times 26 + 4$ et $4 = 0 \times 26 + 4$ d'où 30 et 4 **ont le même reste dans la division euclidienne par 26**

Même chose pour les nombres 19 et 45 : $19 = 26 \times 0 + 19$ et $45 = 26 \times 1 + 19$

Définition : On dit que 30 est congru à 4 modulo 26 . **Notation :** $30 \equiv 4 [26]$

De même : $45 \equiv 19 [26]$