

## Devoir à la maison : Le chiffre affine

Le but de ce devoir est d'étudier une méthode simple de chiffrement de messages. Pour coder un mot on associe un nombre à chacune des lettres de l'alphabet. On applique ensuite un calcul (une fonction) à chaque nombre composant le mot.

Pour ce devoir, on utilisera l'association initiale suivante :

A : 0 ; B : 1 ; C : 2 ; D : 3 ; E : 4 ; F : 5 ; G : 6 ; H : 7 ; I : 8 ; J : 9 ; K : 10 ; L : 11 ; M : 12 ; N : 13 ; O : 14 ; P : 15 ;  
Q : 16 ; R : 17 ; S : 18 ; T : 19 ; U : 20 ; V : 21 ; W : 22 ; X : 23 ; Y : 24 ; Z : 25



On considère la fonction :  $f(x) = 3x + 5$  qui sera appliquée pour coder chaque lettre.

### Partie 1 : Coder un mot

1. Quelle est l'image de 0 par  $f$ ?
2. Expliquer pourquoi la lettre B sera codée par la lettre I.
3. Expliquer pourquoi la lettre H sera codée par la lettre A.
4. Par quelle lettre sera codée la lettre M? la lettre Y?
5. Expliquer pourquoi le mot ADO sera codé par le mot FOV.
6. Par quel mot sera codé le mot BUG?
7. Choisir un mot de quatre lettres et le coder.

### Partie 2 : Décoder un mot

On cherche maintenant à déchiffrer un mot c'est à dire trouver le mot de départ à partir d'un mot déjà codé.

On sait que la lettre A : 0 est codée par la lettre F : 5 et que la lettre B : 1 est codée par la lettre I : 8.

1. Déterminer une **fonction affine**  $g$  telle que  $g(5) = 0$  et  $g(8) = 1$ .
2. Expliquer pourquoi cette fonction  $g$  ne permet pas de décoder correctement toutes les lettres.
3. La lettre B est associée à la valeur 1 mais aussi à la valeur 27. Déterminer une **fonction affine**  $h$  telle que  $h(5) = 0$  et  $h(8) = 27$ .
4. En utilisant la fonction  $h$ , décoder le mot HDW.
5. De même, décoder le mot de quatre lettres que vous avez codé à la fin de l'exercice 1.