Devoir maison

La qualité et la précision des raisonnements entreront de façon importante dans la notation. Vous devez justifier vos calculs ou affirmations.

Problème Cryptologie : chiffrement affine

La cryptologie est la "science du secret", et regroupe **deux branches** : d'une part, la **cryptographie**, qui permet de **coder les messages**, et d'autre part, la **cryptanalyse**, qui permet de les **décoder.**

La cryptographie, ou **art de chiffrer**, coder les messages, est devenue aujourd'hui une science à part entière. Au croisement des **mathématiques**, de l'**informatique**, et parfois même de la **physique**, elle permet ce dont les civilisations ont besoin depuis qu'elles existent : le maintien du secret.
Pour éviter une guerre, protéger un peuple, il est parfois nécessaire de cacher des choses...

Le but de cet exercice est le cryptage et le décryptage d'un message à l'aide d'une fonction affine.
Cette méthode de codage consiste à décaler les lettres de y rangs dans l'alphabet (vers la droite ou la gauche suivant que l'on veut coder ou décoder).

PARTIE 0 : Présentation

Pour faciliter le cryptage et le décryptage, il vaut mieux utiliser un tableau de chiffrage. Voici comment :
On numérote les lettres de l'alphabet de 0 à 25 :

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Il suffit de calculer l'image par une fonction affine du nombre correspondant à une lettre à crypter et de chercher à quelle lettre correspond le nombre obtenu.

Exemple : avec la fonction affine f(x) = 3x + 1.

Si on veut crypter la lettre C,

- Le nombre correspondant à C est 2
- f(2) = 3x2 + 1 = 7
- La lettre correspondant à 7 est H
- « C » est donc codé par la lettre « H »

Si on veut crypter la lettre M,

- Le nombre correspondant à M est 12
- f(12) = 3x12 + 1 = 37
- Le problème est que 37 est plus grand que le nombre des 26 lettres de l'alphabet et ne correspond à aucune lettre mais 37 = 26 + 11 donc le nombre qui code M est 11
- La lettre correspondant à 11 est L
- « M » est codé par la lettre « L »

1/ Coder le message suivant avec la clé de cryptage de l'exemple précédent : *CLASSE DE SECONDE CINQ*.

PARTIE 1 : Fonction affine

Une personne souhaitant coder un message donne des nombres à trois personnes. A Jason BOURNE[1] elle donne -1 et -4, à Ethan HUNT[2] elle donne 2 et 17 et à Evelyn SALT[3] elle donne -3 et -18.

2/ Déterminer la fonction $f(x) = ax + b$ définie par ces nombres correspondant pour chaque personne aux coordonnées d'un point du plan.

L'intérêt d'avoir trois personnes ou plus, est soit de pouvoir vérifier avec un troisième point que c'est la bonne équation de droite, soit de pouvoir quand même décrypter si un des agents meurt en mission ! Il faut au moins deux agents pour pouvoir déterminer l'équation de la droite qui permet de décrypter le message.

PARTIE 2 : Cryptage affine

3/ Recopier et compléter le tableau de chiffrage suivant avec la clé affine de la partie I :

Alphabet 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
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Alphabet codé	3														23											
	D														X											

4/ Coder le message suivant :

«Le plus beau sentiment du monde, c'est le sens du mystère. Celui qui n'a jamais connu cette émotion, ses yeux sont fermés.»

Albert Einstein - ***Comment je vois le monde*** (*Mein Weltbild* ; *The World As I See It*) – 1934.

PARTIE 3 : Décryptage

5/ Déterminer x en fonction de y et donner une méthode qui permet de décrypter un message codé.

6/ Décrypter le message suivant :

> Lndqy o'dh rxnsz dufr uxnz o'dh adgf yf uxnz sfgsxnufs. hc p d ydqz uxz pfni, fq radrnq yf uxnz, yf c'fqgaxnzhdzjf, yf c'djxns fg yf cd oxhf. Lnf yfjdqyfw yf ecnz ? uxnz fgfz nqf cfrxq yf uhf. Uxnz fgfz Cd Uhf.

7/ Imaginer que vous n'avez pas la clé (les coefficients a et b de la fonction affine) de cryptage pour décrypter un message. Comment procéder ?

---

[1] Personnage de fiction, héros de la série littéraire créée par Robert Ludlum et incarné par Matt Damon dans les adaptations cinématographiques.

[2] Personnage principal de la série Mission impossible au cinéma. Il est interprété par l'acteur Tom Cruise.

[3] Agent de la CIA et espion triple incarné au cinéma par l'actrice Angelina Jolie.