Pour mercredi 11/19

Devoir maison d'arithmétique sur le chiffrement affine

Le chiffrement ou cryptage consiste à transformer un message en un message codé (ou chiffré). Le déchiffrement est le procédé inverse, il consiste à décoder un message codé.

Partie A : Procédé de chiffrement

Afin de coder un message on assimile chaque lettre de l'alphabet à un nombre entier entre 0 et 25 comme l'indique le tableau ci-dessous.

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

Un chiffrement affine utilise une fonction affine f, dans cette partie on prend comme chiffrement affine la fonction $f : x \mapsto 11x + 8$

Pour chaque lettre du message :

- On associe l'entier x entre 0 et 25 correspondant à cette lettre d'après le tableau
- On calcule $f(x)$ et on détermine le reste y de la division de $f(x)$ par 26
- On associe ensuite au nombre y la lettre correspondante à l'aide du tableau

Exemple : codage de la lettre G : $G \to 6 \to f(6) = 11 \times 6 + 8 = 74 \to 74 \equiv 22(26) \to W$

1. Coder la lettre W
2. Le but de cette question est de déterminer la fonction de décodage notée f^{-1}
   a) Montrer que pour tous entiers relatifs x et z, on a : $11x \equiv z(26) \Leftrightarrow x \equiv 19z(26)$
   b) En déduire que la fonction de décodage f^{-1} est $f^{-1}(y) = 19y - 22$

Parie B : Casser un chiffrement affine

On peut facilement casser un chiffrement affine si on connait la langue dans laquelle il est écrit car une lettre est toujours codée de la même façon.

On a reçu le message : « $FMEYSEPGCB$ »

Une étude statistique de la fréquence d'apparition des lettres sur un passage plus important, montre que **la lettre E est chiffrée en E et que la lettre J est chiffrée en N.**

On note cette fois-ci g la fonction de chiffrage définie par $g(x) = ax + b$ où a et b sont des entiers entre 0 et 25

1. Montrer que a et b vérifient le système suivant $\begin{cases} 4a + b \equiv 4(26) \\ 9a + b \equiv 13(26) \end{cases}$
2. a) Montrer que : $5a \equiv 9(26)$ puis que $a \equiv 7(26)$
   b) En déduire que $b \equiv 2(26)$ et que g est définie par : $g(x) = 7x + 2$
   c) Démontrer que pour tous entiers relatifs x et z, on a : $7x \equiv z(26) \Leftrightarrow x \equiv 15z(26)$
   d) En déduire que la fonction de décodage g^{-1} est définie par : $g^{-1}(y) = 15y + 22$
   e) Décoder le message