CHIFFREMENT AFFINE

Matrices	*Travaux Pratiques*

Exercice 1

Afin de coder un message on assimile chaque lettre de l'alphabet à un nombre entier 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

Le chiffrement ou cryptage consiste à coder un message. Le déchiffrement consiste à décoder un message codé.
Un chiffrement élémentaire est le chiffrage affine. On se donne une fonction de codage affine f, par exemple : $f(x) = 11x + 8$.
À une lettre du message :

- on lui associe un entier x entre 0 et 25 suivant le tableau ci-dessus
- on calcule $f(x) = 11x + 8$ et l'on détermine le reste y de la division euclidienne de $f(x)$ par 26
- On traduit y par une lettre d'après le tableau ci-dessus

Par exemple, si l'on veut coder par exemple la lettre G par la fonction $f(x) = 11x + 8$, on procède de la façon suivante :
L correspond à $x = 11$. Par suite, $f(11) = 11 \times 11 + 8 = 129$.
Or $129 \equiv 25\ (26)$ et 25 correspond à la lettre Z.
La lettre L est donc codée par la lettre Z.

La fonction de codage est définie par la fonction f, définie par : $f(x) = 11x + 8$.

1) Coder la lettre Z.
2) Le but de cette question est de déterminer la fonction de décodage.
   a) Montrer que pour tous nombres entiers relatifs x et n, on a :
   $$11x \equiv n\ (26) \text{ équivaut à } x \equiv 19n\ (26)$$
   b) En déduire que la fonction f^{-1} de décodage est $f^{-1}(y) = 19y + 4$.
   c) Décoder la lettre F.

Point historique : Ce que l'on appelle le *chiffrement de César* est probablement l'un des plus anciens codages au monde (et plus certainement l'un des plus simples qui soient), dans la mesure où Jules César lui-même l'aurait utilisé.
Aussi appelé chiffrement par décalage, il consiste simplement en une permutation de chaque lettre par une autre, par translation d'un certain nombre de positions dans l'alphabet (toujours dans le même sens bien sûr). Si l'on fait un décalage à droite de trois positions du mot CESAR, cela donne FHVDU (car C + 3 = F dans l'alphabet).
Ce chiffrement par substitution est donc une simple permutation circulaire de l'alphabet qui peut s'exprimer à l'aide d'une congruence sur les entiers. Prenons l'entier n comme clé de cryptage :

C. Lainé

- Chiffrement : $C_n(x) \equiv x + n \ [26]$
- Déchiffrement : $D_n(x) \equiv x - n \ [26]$

Ce système de cryptage symétrique a pour inconvénient d'être particulièrement simple à casser, une soustraction permettant de remonter à la lettre substituée. Afin de connaitre la clé de cryptage, il suffit d'une petite étude statistique. En effet, certaines lettres sont plus fréquentes que d'autres : en français par exemple, c'est la lettre « e » qui revient le plus souvent. Ainsi, la lettre étant la plus fréquente dans le message à décoder peut correspondre au « e ». Il ne reste plus ensuite qu'à décrypter le reste du message.

(Source : http://omnilogie.fr/O/Le_chiffrement_de_C%C3%A9sar)

Vous pourrez voir une présentation du code de César en utilisant le code ci-contre

Exercice 2

On a reçu le message suivant : JWPNWMRCFWMY

On sait que le chiffrement est affine et que la lettre E est codée par la lettre E et que la lettre J est codée par la lettre N.

Soit la fonction affine f définie par : $f(x) = ax + b$, où a et b sont des entiers naturels compris entre 0 et 25.

1) Démontrer que a et b vérifient le système suivant : $\begin{cases} 4a + b \equiv 4 \ (26) \\ 9a + b \equiv 13 \ (26) \end{cases}$.

2) a) Démontrer que $5a \equiv 9 \ (26)$, puis que $a \equiv 7 \ (26)$.

b) En déduire que $b \equiv 2 \ (26)$ et que f est définie par $f(x) = 7x + 2$.

c) Démontrer que pour tous relatifs x et z, on a :

$$7x \equiv z \ (26) \text{ équivaut à } x \equiv 15z \ (26)$$

d) En déduire que la fonction de décodage f^{-1} de décodage est $f^{-1}(y) = 15y + 22$.

e) Décoder le message.

C. Lainé