T.D. n°6

On ajoute à l'alphabet de 26 lettres 5 symboles de ponctuation (espace, virgule, point, point d'interrogation et deux points) pour arriver à 31 symboles (un nombre premier !) On associe à chaque lettre un élément de $\mathbb{Z}/31\mathbb{Z}$: a = 1, b = 2, c = 3, …, z = 26, : = 0.

1. Cryptosystème de César : le chiffre de Jules César correspond, dans ce codage, à appliquer la fonction

$$f : \mathbb{Z}/31\mathbb{Z} \to \mathbb{Z}/31\mathbb{Z}$$
$$x \mapsto x + 3 \bmod 31$$

aux blocs de 1 lettre.

   a) Montrer que *f* est bijective et que la réciproque est $f^{-1}(x) = x + 28 \bmod 31$.

   b) Le message suivant a été crypté avec ce système mais pas avec un décalage de 3 lettres ; seriez-vous capables de le décrypter ?

« khuzckl,:cqv,yzcpscach,yhcslckzcklc tpcgczvalbcwyl zecslvckvuh pe »

2. Généralisation : on peut généraliser le chiffre de Jules César en utilisant la fonction

$$f : \mathbb{Z}/31\mathbb{Z} \to \mathbb{Z}/31\mathbb{Z}$$
$$x \mapsto ax + b \bmod 31$$

avec $a, b \in \mathbb{Z}/31\mathbb{Z}$; c'est ce qu'on appelle cryptage linéaire 1-1.

   a) pour quelles valeurs de *a* et *b* la fonction *f* est-elle une bijection ?

   b) trouver la fonction réciproque de $f(x) = 16x + 5$.

   c) décrypter le message suivant qui a été crypté avec la fonction *f* du b).

3. Cryptosystème de Vigénère :

   a) utiliser la méthode de Vigénère pour crypter le message « merci beaucoup » avec la clef « oui ».

   b) montrer que cet algorithme de cryptage peut s'interpréter comme l'application de la fonction

$$f : (\mathbb{Z}/31\mathbb{Z})^3 \to (\mathbb{Z}/31\mathbb{Z})^3$$
$$X \mapsto X + B$$

qui est le vecteur B ?

   c) quelle est la réciproque de *f* ?

4. Généralisation : cryptage linéaire n-n ; on applique la fonction

$$f : (\mathbb{Z}/31\mathbb{Z})^n \to (\mathbb{Z}/31\mathbb{Z})^n$$
$$X \mapsto A \cdot X + B$$

où A est une matrice $n \times n$ d'éléments de $\mathbb{Z}/31\mathbb{Z}$.

a) à quelle condition *f* est-elle inversible ?
b) montrer que Vigénère est un cas particulier de cette situation.
c) on considère

$$f : (\mathbb{Z}/31\mathbb{Z})^2 \to (\mathbb{Z}/31\mathbb{Z})^2$$
$$X \mapsto \begin{pmatrix} 1 & 9 \\ 3 & 4 \end{pmatrix} \cdot X + \begin{pmatrix} 3 \\ 28 \end{pmatrix}$$

appliquer cette fonction de cryptage au message « attention. »
d) décrypter le message suivant, qui a été crypté avec la fonction de cryptage du point c).

« pasbc pgfytz »