**PRES Sorbonne-Paris Cité.**
**Université Paris 13**
**Institut Galilée**
Licence Informatique Semestre 4 **feuille TD n° 6**

---

# cryptographie I

---

**exercice 1** – Soient $A$ un alphabet à 33 caractères que l'on identifiera à $\mathbf{Z}_{33}$ et $f, g : \mathbf{Z}_{33} \to \mathbf{Z}_{33}$ les fonctions $f(x) := 19x + 6 \pmod{33}$ et $g(x) := 21x + 3 \pmod{33}$, respectivement.

(*i*) Les fonctions $f$ et $g$ sont-elles des fonctions de codage affine ?

(*ii*) Si $f$ (resp. $g$) est un codage affine, donner sa fonction de décodage et déchiffrer 9 et 17.

(*iii*) Si $f$ (resp. $g$) n'est pas un codage affine, trouver $x, y \in \mathbf{Z}_{33}$, $x \neq y$, tels que $f(x) = f(y)$ (resp. $g(x) = g(y)$).

Plus généralement, soient $A$ un alphabet à $n$ caractères que l'on identifiera à $\mathbf{Z}_n$ et $f : \mathbf{Z}_n \to \mathbf{Z}_n$ une application de la forme $f(x) := ax + b \pmod{n}$ où $a, b \in \mathbf{Z}$.

(*iv*) Donner des conditions nécessaires et suffisantes sur $a$ et $b$ pour que $f$ soit une fonction de codage.

(*v*) Si $f$ est une fonction de codage, donner sa fonction de décodage.

(*vi*) Quel est le nombre de fonctions de codage affines distinctes sur un alphabet à $n$ caractères ?

**exercice 2** – Soient $f : \mathbf{Z}_{209} \to \mathbf{Z}_{209}$ la fonction $f(x) := 18x+1 \pmod{209}$ et $g : \mathbf{Z}_{221} \to \mathbf{Z}_{221}$ la fonction $g(x) := 12x + 7 \pmod{221}$.

(*i*) Montrer que $f$ et $g$ sont des fonctions de codage et donner leurs fonctions de décodage.

(*ii*) Donner une fonction de codage affine $h : \mathbf{Z}_{46189} \to \mathbf{Z}_{46189}$ telle que $h \equiv f \pmod{209}$ et $h \equiv g \pmod{221}$.

(*iii*) Donner la fonction de décodage associée à $h$.

**exercice 3** – Chiffrement de Hill

Ce chiffrement a été publié par le mathématicien américain Lester Hill en 1929 et amélioré en 1931. C'est un chiffre polygraphique. Nous allons travailler sur un exemple bigraphique, c'est-à-dire que les lettres sont traitées par paquet de deux. Lester Hill avait fabriqué une machine permettant de chiffrer par groupe de six.

Principe : chaque lettre est remplacée par son rang, selon le tableau

| 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 |

Le message est découpé en block de deux lettres, le dernier block est complété aléatoirement. Un block de deux lettres correspond à un couple $(x_1, x_2)$ de $\mathbb{Z}/26\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$. On se donne quatre éléments de $\mathbb{Z}/26\mathbb{Z}$ (a,b,c,d) qui constituent la clé du chiffrement. On associe à $(x_1, x_2)$ le couple $(y_1, y_2)$ tel que

$$\begin{cases} y_1 = a\,x_1 + bx_2 \\ y_2 = cx_1 + dx_2 \end{cases}$$

(*i*) Quels sont les (a,b,c,d) qui permettent un codage ?

(*ii*) On utilise (11, 3, 7, 4). Est-ce une clé de codage ?
Si oui,

(*iii*) Coder PALACE et RAPACE.

(*iv*) Trouver le système de décodage.

(*v*) Décoder PFXXKNUW.