TD Codage et Cryptographie

Exo 1 Pour un k et n donnés soit Γ et Δ les fonctions:

- $\Gamma : \{0, 1, \dots k-1\}^n \to \{0, 1, \dots k-1\}^n$ définie par: si $s = s_1 s_2 \dots s_n$ alors $t = t_1 t_2 \dots t_n = \Gamma(s)$ est donnée par
  - $t_1 = s_1$, et
  - $t_i = t_{i-1} + s_i \mod k$ pour $1 < i \leq n$.
- $\Delta : \{0, 1, \dots k-1\}^n \to \{0, 1, \dots k-1\}^n$ définie par: si $s = s_1 s_2 \dots s_n$ alors $t = t_1 t_2 \dots t_n = \Delta(s)$ est donnée par
  - $t_1 = s_1$, et
  - $t_i = s_i - s_{i-1} \mod k$ pour $1 < i \leq n$.
- $\Lambda : \{0, 1, \dots k-1\}^n \to \{0, 1, \dots k-1\}^n$ définie par: si $s = s_1 s_2 \dots s_n$ alors $t = t_1 t_2 \dots t_n = \Lambda(s)$ est donnée par
  - $t_n = s_n$, et
  - $t_i = s_i - s_{i+1} \mod k$ pour $1 \leq i < n$.

Pour $n = 6$ et $k = 8$, calculer

- $\Gamma(363000)$, $\Delta(314444)$, $\Gamma(353000)$.
- $\Gamma(\Delta(163401))$
- $\Gamma(\Lambda(250613))$ et $\Gamma(\Lambda(350613))$.

Exo 2

1. Soit la suite pseudo-aléatoire k_n définie par :

$$k_n = a \cdot k_{n-1} + b \cdot k_{n-2} + c \cdot k_{n-3}$$

   pour $n \geq 4$, et avec le *secret* :

   (i) la graine $k_1 = 0$, $k_2 = 1$, $k_3 = 1$, et
   (ii) $a = 1$, $b = 0$ et $c = 1$.

   Donner la periode de k_n.

2. Une suite pseudo-aléatoire e_n définie par :

$$e_n = a \cdot e_{n-1} + b \cdot e_{n-2} + c \cdot e_{n-3} + d \cdot e_{n-4}$$

   a huit termes consécutives : 10011010. Donner la suite.

Exo 3 Chiffrer le message $m = 101011$ et $m = 101001$ par la méthode de Feistel à trois etapes qui utilise la fonction f_1 définie ci-dessous et la clé k_n définie dans l'exo. 2. pt 1. Tracer le diagramme correspondent. Même question avec la fonction f_2.

entrée	sortie f_1
000	011
001	111
010	100
011	000
100	101
101	001
110	010
111	110

entrée	sortie f_2
000	110
001	001
010	101
011	000
100	100
101	111
110	010
111	011