Licence première année 2011-2012

M1MI2016 Codes et Cryptologie : DS 2

– Exercice 1.

1. On représente l'alphabet latin par les entiers entre 0 et 25 avec la convention $A = 0, B = 1, C = 2, \ldots$. Un chiffrement affine $x \mapsto ax + b \bmod 26$ transforme le message 'CRYPTO' en le cryptogramme 'ROXEYZ'. Trouver la clé (a, b) correspondante.
2. Le message clair 'CRYPTO' a cette fois été chiffré deux fois de suite par un chiffre affine de clé (a', b') (c'est-à-dire qu'on a chiffré le chiffré) pour donner en sortie 'NGBAMX'.
   (a) Montrer que 'NGBAMX' est le chiffré de 'CRYPTO' par un chiffre affine de clé (a'', b''). Trouver (a'', b'').
   (b) Trouver les deux valeurs possibles de la clé (a', b').

– Exercice 2. Le code ASCII encode les entiers de 0 à 9 par des octets de la manière donnée par la table suivante :

0	00110000	5	00110101
1	00110001	6	00110110
2	00110010	7	00110111
3	00110011	8	00111000
4	00110100	9	00111001

Un nombre entier X à deux chiffres décimaux est encodé en ASCII, puis les deux octets résultants sont chiffrés par un chiffrement de Vernam. La clé du chiffrement de Vernam est engendrée par un LFSR de longueur 5 et de fonction de transition :

$$x_{i+5} = x_{i+2} + x_i.$$

le chiffré de X est :

11101001 01110000.

Trouver X.

– Exercice 3. Soit $X = (x_0, x_1, \ldots, x_i, \ldots)$ une suite engendrée par le générateur linéaire congruentiel à valeurs dans $\mathbb{Z}/17\mathbb{Z}$ et donné par la récurrence linéaire :

$$x_{i+1} = 3x_i. \tag{1}$$

1. Montrez que, pour tout $x_0 \neq 0 \bmod 17$, la suite X est de période exactement 16. Qu'en est-il pour $x_0 = 0 \bmod 17$?
2. Maintenant $X = (x_0, x_1, \ldots, x_m, \ldots)$ est engendrée par un générateur linéaire congruentiel donné par une récurrence linéaire du type :

$$x_{i+1} = 3x_i + b \bmod 17.$$

   (a) Pour quelle valeur $\alpha(b)$ de l'initialisation x_0 la suite engendrée par ce générateur est-elle de période 1 ?

   (b) Montrez que la suite $Y = (y_1, y_2, \ldots, y_i, \ldots)$ définie par $y_{i+1} = x_{i+1} - x_i$ pour $i \geq 0$ est engendrée par le générateur (1).

   (c) Montrer que, si X n'est pas une suite constante, alors elle ne prend jamais la valeur $\alpha(b)$.

   (d) Déduire de ce qui précède que X est périodique et donner la valeur de sa période en fonction de x_0 et b.

– Exercice 4. On considère de nouveau le générateur pseudo-aléatoire de type LFSR à valeurs dans $\mathbb{Z}/2\mathbb{Z}$ de longueur 5 donné par la relation de transition :

$$x_{i+5} = x_{i+2} + x_i,$$

et $X = (x_0, x_1, \ldots, x_i, \ldots)$ une suite engendrée par ce LFSR.

1. Calculez la valeur de la période T de la suite X, pour une initialisation $(x_0, x_1, x_2, x_3, x_4) \neq 00000$ de votre choix.
2. Vérifiez que tous les éléments de $(\mathbb{Z}/2\mathbb{Z})^5$ différents de 00000 apparaissent comme mots extraits de votre suite X. Rappelez pourquoi c'est le cas. En déduire que T est aussi la période de toutes les suites engendrées par ce LFSR, quelle que soit leur initialisation (différente de 00000).
3. Montrez que, si $X = (x_0, x_1, \ldots, x_i, \ldots)$ et $Y = (y_0, y_1, \ldots, y_i, \ldots)$ sont engendrées par ce LFSR, alors leur somme

$$Z = X + Y = (x_0 + y_0, x_1 + y_1, \ldots)$$

   est aussi une suite engendrée par ce LFSR.
4. Soit $(a_i)_{i=0..T-1}$ une suite non nulle issue de ce générateur et restreinte à sa période, et soit $(a_{i+k \bmod T})_{i=0..T-1}$ une décalée circulaire de (a_i) pour un $k \neq 0 \bmod T$, c'est-à-dire

$$(a_{i+k \bmod T})_{i=0..T-1} = (a_k, a_{k+1}, \ldots, a_{T-1}, a_0, a_1, \ldots, a_{k-1}),$$

   Montrez que la somme $(a_i + a_{i+k})_{i=0..T-1}$ est encore une décalée circulaire de $(a_i)_{i=0..T-1}$.
5. Trouver la valeur du décalage de $(a_i + a_{i+2})_{i=0..T-1}$, c'est-à-dire la valeur de $k \bmod T$ telle que $a_{i+k} = a_i + a_{i+2}$.
6. Trouver la valeur de k telle que $a_{i+k} = a_i + a_{i+4}$.
7. Trouver la valeur de k telle que $a_{i+k} = a_i + a_{i+1}$.