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').

– **Solution.**

1. CRYPTO et ROXEYZ sont respectivement représentés par les suites d'entiers : $[2, 17, 24, 15, 19, 14]$ et $[17, 14, 23, 4, 24, 25]$. Il s'agit de résoudre le sytème :

$$\begin{aligned} 2a + b &= 17 \\ 17a + b &= 14 \end{aligned}$$

   qui a comme solution $(a, b) = (5, 7)$.
2. Si on chiffre deux fois par un chiffre affine de clé (a', b') on obtient une fonction qui à $x \in \mathbb{Z}/26\mathbb{Z}$ associe :

$$a'(a'x + b') + b' = a'^2 x + (a'b' + b').$$

   On obtient donc un chiffre affine de clé (a'', b'') avec :

$$a'' = a'^2 \quad (1)$$
$$b'' = a'b' + b' \quad (2)$$

   NGBAMX est représenté par la suite d'entiers : $[13, 6, 1, 0, 12, 23]$. La résolution du système :

$$\begin{aligned} 2a'' + b'' &= 13 \\ 17a'' + b'' &= 6 \end{aligned}$$

donne cette fois : $(a'', b'') = (3, 7)$. Suite à un mauvais choix de valeurs numériques dans l'énoncé, il n'y avait pas de valeur possible pour un couple (a', b') vérifiant (1) et (2).

– 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.

– **Solution.** Notons la suite chiffrante $(x_i)_{i=0..15}$ et les bits des deux octets de message clair par $m_0 m_1 \cdots m_{15}$. On remarque que les quatre premiers symboles $m_0 m_1 m_2 m_3$ sont fixés et égaux à 0011 ainsi que $m_8 m_9 m_{10} m_{11}$. On obtient donc $x_0 x_1 x_2 x_3 = 1101$ et $x_8 x_9 x_{10} x_{11} = 0100$. La relation de récurrence $x_{i+5} = x_{i+2} + x_i$ nous donne, de proche en proche, $x_5 = 1$, $x_6 = 0$, $x_7 = x_4$, $x_4 + x_6 = 1$ d'où $x_4 = 1$ et toute la suite (x_i) est ainsi dévoilée. On en déduit $m_0 \cdots m_{15} = 0011010000110001$ et $X = 42$.

– 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 :

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

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 $Y = (y_1, y_2, \dots, y_i, \dots)$ définie par $y_{i+1} = x_{i+1} - x_i$ pour $i \geq 0$ est engendrée par le générateur (3).

(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.

– **Solution.**

1. On a $x_i = 3^i x_0$, donc pour $x_0 \neq 0$, la période de la suite est donnée par l'ordre multiplicatif de 3, c'est-à-dire par le plus petit e, tel que $3^e = 1$. 0n calcule les puissances successives de 3 et on constate que $3^2 = 9, 3^3 = 10, 3^4 = 13, \dots, 3^{15} = 6, 3^{16} = 1$. La période de (x_i) vaut $e = 16$. Pour $x_0 = 0$, la suite est identiquement nulle et sa période vaut donc 1.
2. (a) Si la suite est de période 1 on a $x_0 = 3x_0 + b \bmod 17$, soit $2x_0 = -b$, ou $x_0 = -2^{-1}b = 8b$: $\alpha(b) = 8b$.

   (b)

$$\begin{aligned} y_{i+1} &= x_{i+1} - x_i \\ &= (3x_i + b) - 3(x_{i-1} + b) \\ &= 3(x_i - x_{i-1}) \\ &= 3y_i. \end{aligned}$$

   (c) On a constaté à la question 1. que la suite Y est soit identiquement nulle, soit ne prend jamais la valeur 0. Or si X n'est pas constante, on a $x_{i+1} \neq x_i$ pour un certain i, et $y_{i+1} \neq 0$: on a donc jamais $y_i = 0$, donc jamais $x_{i+1} = x_i$, donc jamais $x_i = \alpha(b)$.

   (d) Si $x_0 = \alpha(b)$, on a déjà vu que la période de X égale 1. Sinon, la période de X est au moins égale à celle de Y, soit 16 : comme on a vu que dans ce cas X ne peut pas prendre la valeur $\alpha(b)$, le nombre de valeurs prises par X, et par conséquent sa période, ne peut pas dépasser 16. La période égale donc 16 lorsque $x_0 \neq \alpha(b)$.

– 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 $X = (x_0, x_1, \dots, x_i, \dots)$ 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 $X = (x_0, x_1, \dots, x_i, \dots)$ et $Y = (y_0, y_1, \dots, y_i, \dots)$ sont engendrées par ce LFSR, alors leur somme
$$Z = X + Y = (x_0 + y_0, x_1 + y_1, \dots)$$
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
$$(a_{i+k \bmod T})_{i=0..T-1} = (a_k, a_{k+1}, \dots, a_{T-1}, a_0, a_1, \dots, a_{k-1}),$$
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 $a_{i+k} = a_i + a_{i+1}$.

– **Solution.**

1. On trouve $T = 31$.
2. Le quintuplet 00000 ne peut apparaître, sinon la suite est identiquement nulle. Comme la suite $(x_i)_{i \geq k}$ ne dépend que des cinq symboles précédant x_k, la période égale le nombre de valeurs distinctes de tous les quintuplets de symboles consécutifs : dans notre cas, toutes les 31 valeurs non nulles possibles de ces quintuplets doivent défiler pour que la période atteigne 31. L'initialisation ne peut donc changer la période car elle revient toujours à décaler la suite.
3. On a :
$$x_{i+5} + y_{i+5} = (x_{i+2} + x_i) + (y_{i+2} + y_i)$$
$$x_{i+5} + y_{i+5} = (x_{i+2} + y_{i+2}) + (x_i + y_i).$$
4. La suite décalée de (a_i) est aussi une suite engendrée par le LFSR, la somme de deux suites engendrées par le LFSR reste une suite engendrée par le LFSR, comme on vient de le démontrer, et toutes les suites engendrées par le LFSR sont des décalées d'une même suite (question 2.)
5. $k = 5$. C'est la définition de la récurrence $x_{i+5} = x_{i+2} + x_i$.
6. On a :
$$a_{i+5} = a_i + a_{i+2}$$
$$a_{i+7} = a_{i+2} + a_{i+4}$$
D'où, en additionnant,
$$a_{i+5} + a_{i+7} = a_i + a_{i+4}$$
$$a_{i+10} = a_i + a_{i+4}.$$
Soit, $k = 10$.

7. de $a_{i+10} = a_i + a_{i+4}$ on obtient par décalage $a_{i+14} = a_{i+4} + a_{i+8}$, et en sommant

$$a_{i+10} + a_{i+14} = a_i + a_{i+8}.$$

Comme $a_{i+10} = a_i + a_{i+4}$ peut se réécrire $a_{i+20} = a_{i+10} + a_{i+14}$, on en déduit :

$$a_{i+20} = a_i + a_{i+8}$$

et de proche en proche

$$a_{i+40} = a_i + a_{i+16}$$
$$a_{i+80} = a_i + a_{i+32}$$

soit, en réduisant les indices modulo 31,

$$a_{i+18} = a_i + a_{i+1}$$

et $k = 18$.

Commentaire. Il est en général difficile de prévoir la *valeur* du décalage de la suite obtenue comme somme de deux décalées d'une même suite.