M1MI2016 Codes et Cryptologie

DS Terminal.

10 juin 2013, durée 3h

Documents interdits, calculatrices autorisées

EXERCICE 1 (6 points)

Alice doit transmettre confidentiellement à Bob des nombres entiers N de 4 chiffres décimaux. Ils se mettent d'accord sur la méthode suivante : N est remplacé par la concaténation x des écritures binaires sur quatre bits de ses chiffres (par exemple $N = 1234$ est remplacé par $x = 0001\ 0010\ 0011\ 0100$). Puis Alice chiffre x en $c = x \oplus s$ où s est une suite binaire engendrée par le LFSR de longueur 5 et de coefficients 10100 (c'est-à-dire de relation de récurrence $s_{i+5} = s_{i+2} + s_i$). Enfin Alice transmet c à Bob. L'initialisation est changée à chaque transmission et est connue seulement d'Alice et Bob.

1. Si $N = 1111$ et si le LFSR a pour initialisation 10000, explicitez les étapes de la communication (calcul de x, de s, de c, et procédure de déchiffrement de Bob).
2. Au cours d'une nouvelle session de communication, Bob reçoit d'Alice le message chiffré $c = 1111110101010101$. Hélas, il se rend compte au moment de procéder au déchiffrement, qu'il a perdu une partie des paramètres du LFSR : il se rappelle bien la relation de récurrence $s_{i+5} = s_{i+2} + s_i$ mais il lui manque le troisième bit d'initialisation : il sait seulement que $s_0 = 1, s_1 = 1,\ s_3 = 1,\ s_4 = 1$. Qu'est-ce que Bob peut conclure en ce qui concerne N ?
3. Paniqué, Bob envoie un message à Alice pour lui expliquer qu'il lui manque une valeur d'initialisation. Alice lui répond en lui affirmant que le mot binaire x qui représente N est de poids impair. Bob peut-il alors déterminer N ?
4. Au cours de cette même communication, Oscar a intercepté c et il a entendu Alice affirmer que x est de poids impair. Il ne sait bien sûr rien de l'initialisation du LFSR, mais il connait sa longueur et ses coefficients. D'autre part, il pense savoir que N est plus petit que 3000. Vous allez montrer que Oscar peut retrouver la valeur de N :
   (a) Listez les possibilités pour s sous l'hypothèse $N < 3000$.
   (b) Montrez que x est de poids impair si et seulement si $\sum_{i=0}^{15} s_i = 0 \bmod 2$.
   (c) Pour les valeurs de s restantes calculez x et conclure.

EXERCICE 2 (6 points) Bob et Alice utilisent pour communiquer le système de chiffrement RSA. Bob publie sa clé publique $(N, e) = (5183, 11)$. Alice lui transmet le message chiffré $c = 3$.

1. Sachant que Bob a l'habitude de prendre pour nombres premiers (p, q) des nombres premiers *jumeaux* c'est-à-dire tels que $q = p + 2$, calculez p et q.
2. Calculez l'exposant de déchiffrement d.
3. Que devez-vous calculer pour obtenir le clair x ? (on ne demande pas dans cette question d'exécuter le calcul).

Maintenant vous allez calculer x en utilisant le théorème des restes chinois.

4. Calculez une relation de Bezout entre p et q.
5. Calculez $3^d \bmod p$ et $3^d \bmod q$ en utilisant le petit théorème de Fermat.
6. Utilisez le théorème chinois pour déduire des questions précédentes la valeur de x.

EXERCICE 3 (8 points sur les questions 1 à 6 et 2 points bonus sur la 7) Soit C le code linéaire de matrice génératrice

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

1. Calculez une matrice génératrice G' de C qui soit échelonnée réduite.
2. En déduire une matrice de parité H de C.
3. Déterminez les paramètres $[n, k, d]$ de C, où n est sa longueur, k sa dimension et d sa distance minimale.
4. Combien C peut-il corriger d'effacements ? d'erreurs ?
5. Lors de la transmission d'un mot $x \in C$, ce mot subit des effacements. On note y le mot reçu. Déterminez l'ensemble des possibilités pour x dans les cas suivants :
   (a) $y = ***01000$
   (b) $y = ***0*0000$
6. Lors de la transmission d'un mot $x \in C$, ce mot subit des erreurs. On note y le mot reçu. Déterminez l'ensemble des possibilités pour x dans les cas suivants :
   (a) $y = 11001110$ et on suppose que le nombre d'erreurs est inférieur ou égal à 1.
   (b) $y = 10010110$ et on suppose que le nombre d'erreurs est inférieur ou égal à 2.
7. Dans cette question, on va montrer que, à une permutation près des coordonnées, un code de paramètres $[8, 4, 4]$ est égal à C. Soit donc D un code quelconque de paramètres $[8, 4, 4]$.
   (a) Expliquez pourquoi D possède une matrice de parité P dont les colonnes contiennent les quatre colonnes de la matrice identité I_4.
   (b) Montrez que les quatre autres colonnes sont nécessairement de poids 3 ou 4.
   (c) Montrez qu'il est impossible que P contienne une colonne de poids 4.
   (d) Conclure qu'à l'ordre près des colonnes, il y a une seule possibilité pour P.