M1MI2016 Codes et Cryptologie

DS Terminal.

14 juin 2012, durée 3h

Documents interdits, calculatrices autorisées

EXERCICE 1 (5 points) Alice veut transmettre à Bob son numéro de téléphone portable sans qu'Oscar puisse en prendre connaissance. Pour cela, elle se met d'accord avec Bob sur le choix d'un registre à décalage linéaire de longueur 4 et de son initialisation $(s_0, s_1, s_2, s_3) \in \{0,1\}^4$. Puis elle transforme son numéro de portable en une suite binaire x de longueur 40 obtenue en concaténant l'écriture binaire sur 4 bits de chacun des chiffres (par exemple un 3 de son numéro devient 0011). Puis elle chiffre x avec la suite s de longueur 40 engendrée par le registre à décalage et l'initialisation choisis, en posant $c = x \oplus s$ (comme dans le cours, $\oplus$ est la somme modulo 2 coordonnée par coordonnée). Elle envoie c à Bob.

Oscar intercepte c :

$$c = 1101\ 0001\ 1010\ 1011\ 1111\ 1010\ 0000\ 0000\ 1100\ 1001$$

et bien sûr il veut calculer x. Il sait qu'Alice a chiffré x avec un registre à décalage de longueur 4 dont il ne connait ni les coefficients ni l'initialisation. Il vous demande de l'aider.

1. Déterminez les huit premiers bits de s en utilisant une particularité des numéros de téléphones portables.
2. Déduisez-en un système d'équations linéaires vérifiées par les coefficients du registre.
3. Résolvez ce système afin de déterminer ces coefficients.
4. Calculez les quinze premiers termes de s.
5. Calculez x.

EXERCICE 2 (8 points) Alice souhaite maintenant utiliser le système de chiffrement RSA. Pour créer sa clé RSA, Alice choisit les nombres premiers $p = 29$ et $q = 41$, et $e = 3$ comme exposant de chiffrement.

1. Calculez l'exposant de déchiffrement d.
2. Précisez la clé publique et la clé privée d'Alice.
3. Bob veut transmettre le message $x = 20$ à Alice. Calculez son chiffré.
4. Alice a reçu le chiffré $c = 2$. Que doit-elle calculer pour obtenir le clair x ? (on ne demande pas dans cette question d'exécuter le calcul).

Maintenant vous allez aider Alice à déchiffrer $c = 2$ en utilisant le théorème des restes chinois.

5. Calculez une relation de Bezout entre p et q.
6. Montrez que $2^d = 2^{19} \bmod p$ (indication : utilisez le petit théorème de Fermat).
7. Calculez $2^{19} \bmod p$ (indication : utilisez le moins possible de multiplications et réduisez modulo p à chaque fois..)
8. Suivez le chemin des questions (f) et (g) pour calculer $2^d \bmod q$.
9. Utilisez le théorème chinois pour déduire des questions précédentes la valeur de $2^d \bmod 1189$ et en déduire x.

EXERCICE 3 (7 points sur les 7 premières questions + bonus pour les questions 8 et 9) Soit C le code linéaire de matrice de parité

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

1. Déterminez la longueur et la dimension de C.
2. Montrez que $d(C) = 3$.
3. Quel est le nombre maximum d'effacements que C peut corriger, quelle que soit leur position ? et d'erreurs ?
4. 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) $y = 11010{*}{*}01$
   (b) $y = {*}010{*}{*}000$
5. 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) $y = 111111110$ et on suppose que le nombre d'erreurs est inférieur ou égal à 1.
   (b) $y = 101101110$ et on suppose que le nombre d'erreurs est inférieur ou égal à 2.
6. Donnez une matrice génératrice G de C.
7. Soit G' la matrice obtenue en rajoutant à G une colonne supplémentaire, de sorte que les lignes de G' soient de poids pair et soit C' le code de matrice génératrice G'. Explicitez G', et montrez que les paramètres de C' sont $[10, 5, 4]$.
8. Montrez que le mot $z = 1111111111$ appartient à $C'^{\perp}$ et en déduire que tous les mots de C' sont de poids pair.
9. Un mot du code C' a été transmis mais il a subi simultanément un effacement **et** au plus une erreur. Retrouvez ce mot à partir du mot reçu y :

$$y = 00 * 1011100$$