D. E. S. S. sécurité des systèmes d'information
UNIVERSITÉ DE TOULON ET DU VAR
Année universitaire 2000/2001

Codage

Aucun document autorisé

Exercice 1 **:** (5 points)

1) On considère le corps à 3 éléments $\mathbb{F}_3$ ($\mathbb{Z}/3\mathbb{Z}$), construire les tables d'addition et de multiplication de ce corps.

Soit G une matrice génératrice d'un code sur $\mathbb{F}_3$.

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{pmatrix}$$

2) Quel est le nombre de mots du code ?

3) Ecrire tous les mots du code.

4) Quelle est la capacité de correction du code ?

5) Qu'est-ce qu'un code parfait ?

6) Le code est-il parfait ?

Exercice 2 **:** (10 points) On veut construire un code binaire cyclique linéaire C de longueur 15 ayant une distance minimale d au moins égale à 6 et comportant plus de dix mots. Pour cela, on désire utiliser un code BCH au sens strict (avec b=1). Dans la suite, α désigne une des racines du polynôme $P(X) := X^4 + X + 1$ qui (admettons-le) est irréductible et primitif sur F_2. On note $g(X)$ le polynôme générateur du code cherché.

0) Donner la définition d'un code BCH.

1) Calculer les puissances successives de α en fonction de α^0, α^1, α^2 et α^3.

2) Donner une condition suffisante sur le degré de $g(X)$ pour que C contienne au moins 10 mots.

3) Déterminer les classes cyclotomiques modulo 15.

4) Quels sont les polynômes minimaux de α^1 et α^5.

5) Montrer que $\beta \neq 1$ est une racine de $X^4 + X^3 + X^2 + X + 1$ si et seulement si $\beta^5 = 1$. En déduire que $X^4 + X^3 + X^2 + X + 1$ est le polynôme minimal de α^3.

6) Quel est le polynôme minimal de α^7 ?

7) Déterminer $g(X)$.

8) Montrer que $d \geq 7$ et donner la dimension du code.

9) On considère le mot $f(X) = 1 + X + X^3 + X^4 + X^7 + X^9$. Calculer $f(\alpha^1)$. En déduire que le mot $f(X)$ n'est pas dans le code.

x) Décoder $f(X)$ sachant qu'il y a une seule erreur.

Exercice 3 **:** (5 points)

RSA

On pose $p = 13$ et $q = 7$ et $n = pq$. On attribue a Bob la clé publique $e = 5$. Alice envoie a Bob un message secret $1 < m < n$ en effectuant m^e modulo n.

1. Rappeler comment Bob déchiffre.
   Définir sans chercher à la calculer la clé secrète de Bob d.
2. Calculer $\phi(n) := (p-1)(q-1)$.
   Pourquoi a-t-on pris $PGCD(e, \phi(n)) = 1$?
3. Trouver des entiers r, s tels que $re + s\phi(n) = 1$
4. En déduire d en fonction de r, s.

Partage de secrets

On donne un code $q-$aire C par sa matrice de contrôle H de taille m par n et qu' on suppose de rang m.

1. Donner, en fonction des paramètres précédents une borne sup sur la distance minimale d de C.

2. On suppose que chacun des mineurs m par m de H est de rang m. Que dire de d?

3. Construire un exemple de tel H pour $m = 2$ et $n = q = 4$. On notera ω une racine de $x^2 + x + 1$. On rappelle que $F_4 = \{0, 1, \omega, \omega^2\}$.

4. Rappeler ce qu' est un système de cryptographie à seuil (N, K). Donner les plus grands N et K que l'on peut construire avec le code de l'exemple.