Examen terminal de MAT239 (2 heures)

Documents et calculatrices interdits. Les téléphones portables doivent rester éteints.
Chaque partie doit être rédigée sur une copie distincte *; le barème est approximativement de 10 points pour chaque partie.*

---

1 Partie I

Exercice 1

Soit $C \subset \mathbb{F}_2^7$ un code linéaire dont une matrice génératrice est $G' = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$.

1. Montrer que C admet la matrice génératrice standard $G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$.
2. Montrer que C est un code polynomial, de polynôme générateur $g = X^3 + X^2 + X + 1$.
3. Combien ce code permet-il de détecter d'erreurs ? et d'en corriger ?
4. En expliquant brièvement comment vous procédez,
   (a) coder systématiquement les mots 1001 et 0011 ;
   (b) corriger (si nécessaire) et décoder les mots 0110110 et 1101111.

Exercice 2

Soit $C \subset \mathbb{F}_2^n$ un code linéaire donné par une application de codage (linéaire, injective) $\phi : \mathbb{F}_2^q \to \mathbb{F}_2^n$; ainsi, en tant que sous-espace vectoriel de $\mathbb{F}_2$, C est de dimension q. On note d sa distance minimale.

1. On souhaite montrer l'inégalité de Singleton,
$$d + q \leq n + 1.$$
On définit l'application (linéaire) $\pi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ par
$$\forall w = w_1 \dots w_n \in \mathbb{F}_2^n, \quad \pi(w) = w_1 \dots w_{q-1} 0 \dots 0.$$
   (a) Quelle est la dimension de l'image $\pi(\mathbb{F}_2^n)$ de π ?
   (b) En déduire que la dimension de $\pi(C)$ est inférieure ou égale à $q-1$, et qu'il existe $w \in C \setminus \{0_n\}$ tel que $\pi(w) = 0_n$.
   (c) Montrer que le poids $p(w)$ du mot $w \in C$ de la question précédente (tel que $w \neq 0_n$ et $\pi(w) = 0_n$) vérifie
$$d \leq p(w) \leq n - q + 1,$$
   et conclure.
2. (a) Écrire l'inégalité de Hamming pour le code C.
   (b) Si $n = 7$ et $q = 4$, quelle borne sur d implique l'inégalité de Hamming ?
   (c) Toujours avec $n = 7$ et $q = 4$, quelle borne sur d implique l'inégalité de Singleton ?

2 Partie II

Question de cours

Expliquer comment fonctionne le système de chiffrement RSA. Montrer pourquoi et grâce à quel théorème le déchiffrement est correct.

Problème

Le chiffrement de Goldwasser-Micali, proposé en 1982, est un des premiers cryptosystèmes à clé publique probabiliste et "probablement sûr". Son fonctionnement est le suivant :

— Génération de clés : Alice choisit deux grands nombres premiers p et q et calcule $n = pq$. Elle prend ensuite un élément $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ qui n'est un résidu quadratique ni modulo p ni modulo q, c'est-à-dire tel que $\left(\frac{x}{p}\right) = \left(\frac{x}{q}\right) = -1$. La clé publique d'Alice est alors (x, n) et sa clé privée est (p, q).

— Chiffrement : pour envoyer un message, Bob le transcrit en une suite de bits $b_0 \dots b_N$ et chiffre chaque bit indépendamment (autrement dit, l'espace des messages clairs est $\{0, 1\}$). Pour chiffrer un bit $b \in \{0, 1\}$, Bob choisit au hasard un élément $y \in (\mathbb{Z}/n\mathbb{Z})^\times$ et transmet le chiffré $c = y^2 x^b \mod n$.

— Déchiffrement : pour trouver le message clair b' correspondant à un chiffré reçu $c \in (\mathbb{Z}/n\mathbb{Z})^\times$, Alice calcule le symbole de Legendre $\left(\frac{c}{p}\right)$; s'il vaut 1 alors $b' = 0$, sinon $b' = 1$.

1. Alice choisit $p = 13$ et $q = 17$ (en réalité bien sûr, p et q doivent être nettement plus grands), et donc $n = 221$. Montrer que $x = 5$ convient. Plus généralement, si Alice tire un entier aléatoirement entre 1 et $n - 1$, quelle est la probabilité que cet entier soit un choix convenable pour x ?
2. Montrer que le système de Goldwasser-Micali est correct (c'est-à-dire que $b' = b$; le déchiffrement fonctionne).
3. Alice reçoit le chiffré $c = 184$ (toujours avec $n = 221$). Donner le message clair correspondant.
4. Pourquoi est-il nécessaire d'utiliser un aléa y dans l'étape de chiffrement ? Que se passe-t-il si Bob utilise plusieurs fois une même valeur de y pour communiquer avec Alice ?
5. Soit c_1 un chiffrement de b_1, c_2 un chiffrement de b_2 et z un élément quelconque de $(\mathbb{Z}/n\mathbb{Z})^\times$. Montrer que $c = c_1 c_2 z^2 \mod n$ est un chiffrement de $b_1 + b_2 \mod 2$.
6. Pour simplifier la génération des clefs, on se propose dans cette question de modifier le protocole en demandant juste que l'élément $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ vérifie $\left(\frac{x}{p}\right) = -1$.
   (a) Quelle est la probabilité qu'un élément x tiré aléatoirement vérifie cette condition ?
   (b) Montrer que le déchiffrement tel que décrit ci-dessus fonctionne toujours.
   (c) On suppose que le x choisi vérifie $\left(\frac{x}{q}\right) = 1$. Expliquer comment Charlie qui écoute la communication entre Alice et Bob peut facilement déchiffrer la conversation.
7. Rappeler la définition du problème de résiduosité quadratique. Montrer qu'un adversaire qui est capable de résoudre le problème de la résiduosité quadratique modulo n peut décrypter n'importe quel message chiffré.
8. Réciproquement, montrer qu'un adversaire capable de retrouver le message clair correspondant à n'importe quel chiffré peut résoudre le problème de la résiduosité quadratique modulo n.
9. Comparer la taille des messages clairs et des messages chiffrés.