Examen *théorie de l'information*
Tous documents autorisés
Le barème est donné à titre indicatif

1(3 pt)

1. Quel est le résultat de l'algorithme *Move to Front* appliqué au message : `aaacccbbc` ?
2. Calculer l'entropie du système obtenu au point 1. et donner le code de Huffman de celui-ci.
3. Donner le résultat de l'algorithme de compression LZ78 appliqué au message `aaacccbbc`.
4. Donner le résultat de l'algorithme de décompression LZ78 appliqué au message :
   (0,a) (0,b) (1,a) (3,b) (3,a) (2,a) (5,b)

2 (2 pt) Donner le codage de Elias pour le mot hexadécimal $x = 1\underbrace{00\ldots0}_{15 \text{ fois}}A2\underbrace{00\ldots0}_{63 \text{ fois}}$.

3(3 pt) Soit la matrice génératrice $G = \begin{pmatrix} 100101 \\ 010110 \\ 001011 \end{pmatrix}$ d'un code linéaire.

1. Quels sont les mots du code ?
2. Quelle est la taille et la dimension du code ?
3. Quelle est sa distance minimale?
4. Quel est son taux d'information?
5. Combien détecte-t-il et corrige-t-il d'erreurs ?

4 (2 pt) Soit le code de longueur 5 obtenu par 3 répétitions doublées par un bit de parité. Exemple : le mot 01 sera codé par 01 01 01 1. Le code ainsi obtenu est un code linaire de dimension 2 et taille 5.

1. Donner la matrice génératrice de ce code;
2. Quels sont les mots du code?
3. Quelle est sa distance minimale?
4. Quel est son taux d'information?
5. Combien corrige-t-il d'erreurs?
6. Vérifier la proposition de Hamming pour ce code.

5 (1 pt) Résoudre les équations suivantes en $\mathbb{Z}/7\mathbb{Z}$: $4x + 3 = 1$, $3x + 6 = 0$.

6 (3 pt) Le coffre-fort d'une banque s'ouvre si trois de ses quatre directeurs saisissent leur code (part du secret). Les codes sont :

$$\text{p1} : 3;\ \text{p2} : 0;\ \text{p3} : 6;\ \text{p4} : 0.$$

Soit $P : \mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}/7\mathbb{Z}$ le polynôme correspondent à ce protocole.

- Donner $P(0)$ (le secret),
- Donner P.

7 (4 pt)

1. 2 est un générateur de $\mathbb{F}_7^*$?
2. 3 est un générateur de $\mathbb{F}_7^*$?
3. 5 est un générateur de $\mathbb{F}_7^*$?
4. combien de générateurs possède $\mathbb{F}_7^*$?
5. en $\mathbb{F}_7^*$ calculer $\log_3 4$ et $\log_5 4$
6. Alice et Bob veulent appliquer le protocole de Diffie-Hellman. Ils choisissent en commun $g = 5$ et $p = 7$. Choisir des clés secrètes a (pour Alice) et b (pour Bob) et appliquer le protocole avec ces deux valeurs.

8 (3 pt) Décrire le protocole RSA avec

1. les données privées d'Alice : $p = 3$, $q = 5$,
2. la clé publique : $(n, e) = (15, 7)$