Université Côte d'Azur 2022–2023
Licence 3 Info, L3 Math-Info, L3 Sc. & Techn.

Cryptographie & calcul symbolique

Partiel du 28 octobre

Nom :

Prénom :

Durée : 1h30
Une feuille manuscrite recto autorisée

Note :

Exercice 1 : (3 points) Codes CRC
Voici un code CRC de degré $r = 3$ défini par son polynôme générateur $P_g = x^3 + x^2 + 1$.

1. On souhaite coder le message $m = 100101$. Commencez par mettre le message m sous la forme du polynôme P_m. Calculez le polynôme P_c obtenu par division de polynômes et déduisez-en le message codé c obtenu par ajout de redondance à m *(détaillez les étapes du calcul dont la division)*.

2. On reçoit le message codé $c' = 1100101$. Contrôlez si c' est valide ou non ? Si oui, ôtez lui sa redondance afin de retrouver le message m' initial.

Exercice 2 : (4 points) Code d'Huffman

Voici la distribution de probabilités d'une source Ω que l'on se propose de coder en binaire :

Symbole	Proba. d'apparition	Mot de code
a	0,25	...
b	0,20	...
c	0,05	...
d	0,20	...
e	0,25	...
f	0,05	...

1. Calculez l'entropie de cette source Ω en rappellant la formule au préalable.

2. Construisez et dessinez (en haut à droite de cette page) un arbre d'Huffman afin d'attribuer à chaque symbole son mot de code. *(on demande en prime ici que la probabilité des fils gauches n'excède pas celle des fils droits)*.
3. Remplissez la dernière colonne de la table en attribuant à chaque symbole de la source Ω le mot de code lui correspondant.
4. Calculez la longueur moyenne pondérée des mots du code puis prouvez l'optimalité de votre code d'Huffman.

5. A quelle famille de codes appartiennent les codes d'Huffman ? Pourquoi ?

Exercice 3 : (5 points) Code de Hamming On considère le code de Hamming entièrement spécifié par la matrice de contrôle H suivante :

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

1. Le récepteur reçoit le message $\mathcal{R} = 1100001$. Vérifiez si le message reçu $\mathcal{R}$ est bien celui qui a été transmis.

2. Le cas échéant, proposez une correction de $\mathcal{R}$ qui corresponde au message $\mathcal{T}$ réellement transmis.

3. Trouvez la matrice génératrice G de ce même code de Hamming qui est entièrement conditionné par la matrice de contrôle H.

4. Déduisez-en la valeur du message $\mathcal{M} = x_1x_2x_3x_4$ codé en le message $\mathcal{T}$ par ajout de redondance.

5. Expliquez en quoi un tel $(7, 4)$-code de Hamming est un code linéaire *parfait*.

Exercice 4 : (5 points) Chiffrement symétrique

1. **Le rail de chemin de fer** Le plus simple est d’illustrer le principe de ce petit chiffre par un exemple. Le cryptogramme `CIEL?EHFESIBNCRTO` est ici obtenu pour une hauteur de $n = 2$:

$$\begin{array}{ccccccccccccccccc}
C & & & & I & & & & E & & & & L & & & & ? \\
 & E & & H & & F & & E & & S & & I & & B & & N & \\
 & & C & & & & R & & & & T & & & & O & &
\end{array}$$

   Déchiffrez le cryptogramme `AAELCMH?OSACRR` obtenu pour une hauteur de 3 puis indiquez la nature et la clef de cet algorithme de chiffrement.

2. Dites quels sont les avantages et les inconvénients communs à la plupart des chiffrements à clef secrète. Vous donnerez 3 exemples connus de tels chiffres.

3. Le stockage des mots de passe sur un serveur UNIX utilise la cryptographie à clef secrète. Décrivez comment.

Exercice 5 : (3 points) Compression Lempel-Ziv

Décompressez la séquence de triplets suivante, la compression a été faite avec l’algorithme LZ77 *(le texte est en anglais)* :

(0, 0, ’o’)	(0, 0, ’n’)	(0, 0, ’ ’)	(0, 0, ’a’)	(3, 1, ’d’)	(4, 1, ’o’)	(7, 2, ’t’)	(0, 0, ’h’)	(0, 0, ’e’)	(11, 1, ’r’)	(12, 1, ’i’)
…	…	…	…	…	…	…	…	…	…	…
(16, 2, ’w’)	(4, 1, ’l’)	(1, 1, ’ ’)	(0, 0, ’f’)	(22, 1, ’l’)	(5, 2, ’l’)	(14, 1, ’k’)	(20, 2, ’t’)	(23, 1, ’a’)	(23, 1, ’s’)	(16, 2, ’r’)
…	…	…	…	…	…	…	…	…	…	…
(0, 0, ’o’)	(0, 0, ’m’)	(31, 1, ’a’)	(28, 1, ’s’)	(14, 1, ’a’)	(13, 1, ’ ’)	(23, 6, ’e’)	(23, 6, ’o’)	(23, 6, ’a’)	(23, 2, ’.’)	(1, 1, ’.’)
…	…	…	…	…	…	…	…	…	…	…