Université Côte d'Azur 2023–2024
Licence 3 Info, L3 Math-Info, L3 Sc. & Techn.

Cryptographie & calcul symbolique

Partiel du 27 octobre

Nom :
Prénom :

Durée : 1h30
Une feuille manuscrite recto autorisée

Note :

Exercice 1 : (4 points) Compression Lempel-Ziv

Je chante, tu chantes, il chante, nous chantons, vous chantez ...

Compressez ce texte avec l'algorithme LZ77, les fenêtres de recherche et de lecture étant de tailles 31 et 7.

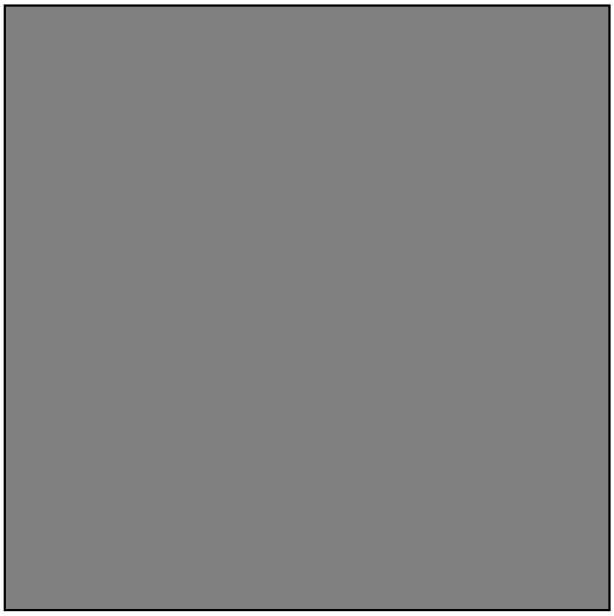
(0, 0, 'J')	(0, 0, 'e')	(0, 0, ' ')	(0, 0, 'c')	(0, 0, 'h')	(0, 0, 'a')	(0, 0, 'n')
(0, 0, 't')	(7, 1, ',')	...	...	...	...	...
...	...	...	...	...	...	...
...	...	...	...	...		

Exercice 2 : (4 points) Codes d'Hufmann

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

Symbole	Proba. d'apparition	Code
a	0,10	...
b	0,10	...
c	0,25	...
d	0,15	...
e	0,35	...
f	0,05	...

1. Donnez la formule générale de l'entropie puis calculez celle de la source probabilisée (Ω, p).



2. Dessinez au-dessus à droite l'arbre d'Huffman obtenu en vue d'attribuer à chaque symbole son mot de code *(on demande en prime que la probabilité des fils gauches n'excède pas celle des fils droits)*.
3. Remplissez la dernière colonne de la table précédente avec les mots du code obtenus.
4. Calculez la longueur moyenne pondérée du code obtenu. Commentez.

Exercice 3 : (3 points) Transformée de Burrows-Wheeler Voici la colonne de lettres triée **F** et le vecteur de transformation **H** permettant de retrouver un mot tel qu'il était avant sa transformation :

F	**H**	**L**
E	3	...
E	0	...
I	1	...
N	7	...
O	5	...
P	2	...
R	4	...
T	6	...

1. Commencez par retrouver la colonne **L** à partir de la colonne **F** et du vecteur **H** sachant que :
$$\forall j \quad L[\,H[j]\,] = F[j]$$
2. Rappelez l'algorithme pour reconstruire le mot initial à partir de **L**, de **H** et de l'index primaire ip.

3. Décodez le mot initial sachant que l'index primaire $ip = 3$ ici.

Exercice 4 : (5 points) Codes de Hamming

On considère le code de Hamming entièrement spécifié par la matrice génératrice G suivante :

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

1. Comment coderait-on le message $\mathcal{M}_1 = 1001$ par ajout de redondance avant de l'envoyer dans un canal ?

2. Calculez la matrice de contrôle H de sorte que le produit $H.{}^tG = [0]_{3,4}$.

3. Le récepteur reçoit un message $\mathcal{R} = 1100011$. En supposant qu'une seule erreur au maximum peut se produire, indiquez si le message $\mathcal{R}$ est altéré ou pas.

4. Le cas échéant, proposez une correction de $\mathcal{R}$ qui corresponde au message codé $\mathcal{C}_2$ réellement transmis et déduisez-en le message $\mathcal{M}_2$ d'origine, c'est-à-dire avant ajout de redondance.

5. Quelle est la distance minimale $d_{min}(C)$ de ce code de Hamming ? Combien d'erreurs permet-elle de détecter ? Combien d'erreurs permet-elle de corriger ?

Exercice 5 : (4 points) Questions de cours Vous commenterez brièvement chacune de vos réponses.

1. Quelles sont les trois techniques à la base de la plupart des algorithmes de chiffrement à clef secrète, utilisées afin de rendre l'information de départ inintelligible.

2. Voici un LFSR représenté sous la forme du polynôme $\Pi(X) = X^5 - X^4 - X^2 - 1$. Calculez les 5 bits pseudo-aléatoires suivants produits à partir des valeurs initiales $(x_0, x_1, x_2, x_3, x_4) = (0, 0, 1, 1, 0)$.

3. Considérons le code CRC de polynôme générateur $P_g = x^2 + x + 1$. Le message 01001011 reçu est-il correct ? (*vous poserez la division*).

4. Le codage arithmétique permet de compresser un texte en un réel. Retrouvez la compression des 5 premières lettres du mot COCCINELLE.