

## Annexe

```

{
  "_id" : 83419,
  "contact" : {
    "GooglePlaces" : null,
    "Foursquare" : "https://foursquare.com/v/pe%C3%B1a-festayre-paris-%C
  },
  "name" : "Peña Festayre",
  "location" : {
    "city" : "Paris",
    "coord" : {
      "coordinates" : [
        2.3860357589657,
        48.896621743257
      ],
      "type" : "Point"
    },
    "address" : "80 Boulevard Macdonald"
  },
  "category" : "restaurant",
  "description" : "",
  "services" : [ "jardin", "terrasse", "journaux" ]
  "reviews" : [
    {
      "wordsCount" : 6,
      "rating" : 0,
      "language" : "ca",
      "details" : "http://tour-pedia.org/api/getReviewDetails?id=52a74",
      "source" : "Foursquare",
      "text" : "Entree + Plat (grillade a volonte) + dessert 19€",
      "time" : "2011-01-22",
      "polarity" : 0
    },
    {
      "wordsCount" : 20,
      "rating" : 0,
      "language" : "fr",
      "details" : "http://tour-pedia.org/api/getReviewDetails?id=52a74a85ae9eef5a50671b09",
      "source" : "Foursquare",
      "text" : "Tous les mercredis jusqu'en juin : Soirées Salsa... concert live puis dj ;
      "time" : "2012-01-11",
      "polarity" : 5
    }
  ],
  "likes" : {},
  "nbReviews" : 2
}

```

*Bon courage !*



*Ing2 - Info*

## Examen -Session Principale- S1 – 2024/2025

<b>Filière : Ing2_Info</b>	<b>Matière : Bases de données NoSQL et Big Data</b>		<b>Enseignante : Asma KERKENI</b>
<b>Date : 13 / 01 / 2025</b>	<b>Nbr de Crédits : 3</b>	<b>Coefficient : 3</b>	<b>Documents <u>non autorisés</u> Calculatrice <u>autorisée</u></b>
<b>Durée de l'examen : 1h30</b>	<b>Régime d'évaluation : Mixte</b>		<b>Nombre de pages : 4</b>
	<b>EX (45%) + DS (22%) + TP (33%)</b>		

## Exercice 1: QCM (4 points)

Dans le Q.C.M. suivant, chaque question peut comporter une ou plusieurs réponses correctes. Pour chaque question, veuillez indiquer sur votre feuille de réponses toutes les options exactes.

- Dans Hadoop, comment appelle-t-on le processus responsable de l'exécution d'une tâche sur un nœud Worker ?
  - TaskTracker
  - JobTracker
  - DataNode
  - ResourceManager
- Quel est l'objectif de l'étape « *shuffle and sort* » dans Hadoop ?
  - Réduire les données
  - Organiser les données pour le traitement
  - Stocker les données
  - Exécuter des tâches de map
- Dans un cluster Hadoop, quel est le nombre maximal de tâches Reduce qu'un nœud Worker peut exécuter simultanément ?
  - Une seule tâche Reduce à la fois.
  - Autant de tâches Reduce que le nombre de cœurs du nœud.
  - Autant de tâches Reduce que la mémoire totale disponible sur le nœud.
  - Un nombre illimité de tâches Reduce.
  - Autant de tâches Reduce que le nombre de slots Reduce configurés pour le nœud Worker.
- Quel type de base de données est le mieux adapté pour des données non structurées ?
  - Relationnelle
  - NoSQL
  - Graph
  - Hiérarchique

5. Quel est le principal objectif de l'indexation dans une base de données ?
  - a. Réduire la taille des données
  - b. Accélérer les requêtes
  - c. Améliorer la sécurité
  - d. Diminuer la redondance
6. Dans le contexte du théorème CAP, la disponibilité signifie :
  - a. Les données sont toujours cohérentes
  - b. Chaque requête reçoit une réponse valide
  - c. Les partitions réseau sont évitées
  - d. Chaque requête reçoit une réponse
7. Quel mécanisme est utilisé pour tolérer les pannes dans les bases NOSQL ?
  - a. Clustering
  - b. Réplication
  - c. Indexation
  - d. Transaction ACID
8. Dans le modèle BASE des bases de données NOSQL, la cohérence est :
  - a. Forte
  - b. Garantie à terme
  - c. Garantie de manière instantanée
  - d. N'est pas de tout garantie

### Exercice 2: Hadoop Map Reduce (6 points)

Vous disposez d'un fichier texte contenant des informations sur des pages web et leurs liens. Chaque ligne, composée de trois colonnes séparées par des tabulations, représente une page web avec les éléments suivants :

- **Colonne 1** : la page web source,
  - **Colonne 2** : le score attribué par la page source,
  - **Colonne 3** : une liste des pages de destination vers lesquelles la page source établit des liens.
- Le but est de développer un programme **Hadoop MapReduce** en Python Streaming pour calculer le score reçu par chaque page comme illustré par l'exemple suivant.

Entrée			Sortie	
Page A	1	page B, page C, page D	Page A	2,5
Page B	2	page A, page C	Page B	2,33
Page C	3	page A, page E	Page C	1,33
Page D	2	page B	Page D	0,33
			Page E	1,5

Détails du calcul :

- Chaque page divise son score par le nombre de destinations vers lesquelles elle pointe. Par exemple, si une page Page A avec un score de 1 pointe vers 3 destinations (Page B, Page C, Page D), elle contribuera 0.33 à chacune de ces destinations.
- Le score total reçu par une page est la somme des contributions reçues de toutes les pages sources qui pointent vers elle.

Questions :

1. Donnez le code Python du mapper.
2. Donnez le code Python du Reducer permettant d'obtenir le résultat final souhaité.

### Exercice 3 : (10 points)

La figure en annexe représente un extrait d'une collection nommée "Paris", issue d'une base de données MongoDB. Cette collection regroupe des lieux situés à Paris, agrégés à partir du site TourPedia. Elle fournit des informations détaillées sur chaque lieu, notamment leurs catégories, descriptions, et autres caractéristiques spécifiques :

- Des POI (points d'intérêts) ;
- Des restaurants ;
- Des logements (accommodation), avec les services associés ;
- Des attractions ;
- A chaque lieu sera associé des commentaires sur Internet (Facebook, Foursquare...), et des notes utilisateurs.

Ecrivez les requêtes sur la collection Paris permettant de :

1. Lister les lieux proposant un service de livraison ?
2. Donner la liste des lieux qui ne contiennent pas une information sur la catégorie.
3. Donner la liste des lieux qui ont à la fois des notes (rating) faibles (< 2) et fortes (>4).
4. Donner la liste de langues (sans doublons) utilisées dans les commentaires pour chaque source de commentaires (reviews.source).
5. Donner les adresses des lieux dont le nom contient une valeur numérique.
6. Donner la liste des lieux qui ont des commentaires écrits avant l'année 2015 (reviews.time).
7. Pour chaque langue utilisée dans les commentaires, trouver le nombre total de commentaires dans cette langue et trier les résultats par ordre décroissant de ce nombre.

Durée : 1h30	Matière :	Classe : 2 <sup>ème</sup> ING E-µE
Documents autorisés : Non	Systèmes Numériques	Enseignant : Abdesslem Ben Abdelali
Date : 13 / 01 / 2025	Complexes : µ-architecture avancée des processeurs	Nombre de pages : 3 (3 + 2 annexe)
Nom : .....	Prénom : .....	Matricule : .....

NOTE : Répondre directement sur les feuilles de l'examen  
Pas de questions à poser en aucun cas → en cas de problème estimé, vous le mentionnez sur la copie de l'examen et vous continuez à travailler avec la supposition que vous faites.

/20

### Exercice 1: (3 pts)

On suppose embarquer le code C suivant dans une plateforme à base d'un microprocesseur MIPS multi-cycles. On donne le code assembleur MIPS équivalent (à compléter). Sachant que la fréquence d'horloge est de 200 MHz, déterminez le temps d'exécution du programme (Donnée : l'instruction "slt" nécessite 4 cycles d'horloge)

# Code C

```
int i;
int sum = 0;
```

```
For (i=1 ; i < 128 ; i = i*2)
```

```
Sum = Sum+i;
```

```
addi $s0, $0, $1    # i = 1
add  $s1, $0, $0     # sum = 0
addi $t0, $0, 128    # $t0 = 128
```

```
loop:
.....             # if (i < 128), $t1 = 1, else $t1 = 0
beq  $t1, $0, done  # if $t1 == 0 (i >= 128, branch to done)
add  $s1, $s1, $s0  # sum = sum + i
.....             # i = i * 2 (utiliser l'instruction sll)
done:
```

*Ne rien écrire ici*

### Exercice 2 : (7 pts)

1. Donner le code machine (en binaire) de l'instruction « beq \$t0, \$s1, Loop » du programme suivant :

```
0x00401000 beq $t0, $s1, Loop
0x00401004 ...
0x00401008 ...
0x0040100C Loop: ...
```

beq \$t0, \$s1, Loop: →

Op-code	Rs	Rt	I16

2. Donner le code machine (en binaire) de l'instruction « beq \$t7, \$s4, done » du programme suivant :

```
0x00401000 beq $t7, $s4, done
...
0x00402040 done: ...
```

beq \$t7, \$s4, done: →

Op-code	Rs	Rt	I16

3. Donner le code machine (en binaire) de l'instruction « beq \$t9, \$s7, back » du programme suivant :

```
0x0040310C back: ...
...
0x00405000 beq $t9, $s7, back
```

beq \$t9, \$s7, back: →

Op-code	Rs	Rt	I16

4. Donner le code machine (en binaire) de l'instruction « jal proc » du programme suivant :

```
0x00403000 jal proc
...
0x0041147C proc: ...
```

jal proc: →

Op-code	Adresse cible sur 26 bits (I26)

5. Donner le code machine (en binaire) de l'instruction « j back » du programme suivant :

```
0x00403004 back: ...
...
0x0040400C j back
```

j back: →

Op-code	Adresse cible sur 26 bits (I26)

6. On suppose que \$t0 contient l'adresse (de base) du l'élément numéro 0 d'un tableau d'octets (8bits) et \$t1 contient la valeur de l'index du tableau (n). Ecrivez une courte séquence d'instruction MIPS permettant de stocker la valeur 1 dans la case n (Tab[n]).

.....

.....

.....

.....

7 - Ecrivez un code assembleur MIPS permettant d'échanger le contenu de deux registres, \$t0 et \$t1. Vous ne devez utiliser aucun registre supplémentaire et en particulier le registre \$0.

.....

.....

.....

.....

.....

### Exercice 3 : (5 pts)

La procédure « strcpy » suivante permet de copier le tableau de caractères X dans Y

```
void strcpy(char X[], char Y[])
{
    int i = 0;
    while (X[i] != 0)
    {
        Y[i] = X[i];
        i = i + 1;
    }
}
```

L'appel de cette fonction se fait en transférant les pointeurs sur les tableaux (adresses de bases) en paramètre de la fonction puis l'appel à l'instruction Jal pour le saut vers la fonction.

(a) Donnez la partie appel à la fonction dans le programme principal (main) et implémentez la procédure « strcpy » en code assembleur MIPS. L'adresse de base du tableau X est ("1522FFF0"), et l'adresse de base du tableau Y est ("1444FFF0"). Utilisez \$s0 pour i.

Main : ...

# Ecrire les adresse de base des tableaux X et Y dans \$a0 et \$a1 et faire appel à la fonction

.....

.....

.....

.....

.....

.....

...

# La procédure strcpy

# Les registres à utiliser :

# \$s0 = i, # \$t0 = adresses d'une case du tableau X, # \$t1 = adresse d'une case du tableau Y

# \$t2 / Valeur du tableau X (X[i])



# Annexe

## MIPS register Set

Name	Number	Use
\$0	0	the constant value 0
\$at	1	assembler temporary
\$v0-\$v1	2-3	procedure return values
\$a0-\$a3	4-7	procedure arguments
\$t0-\$t7	8-15	temporary variables
\$s0-\$s7	16-23	saved variables
\$t8-\$t9	24-25	temporary variables
\$k0-\$k1	26-27	operating system (OS) temporaries
\$gp	28	global pointer
\$sp	29	stack pointer
\$fp	30	frame pointer
\$ra	31	procedure return address

## MIPS instructions

R-type instructions (add, sub, and, or, slt):  $rd \leftarrow rs \text{ funct } rt$

0	rs	rt	rd	shamt	funct
31-26	25-21	20-16	15-11	10-6	5-0

RI-type instructions (addiu):  $rt \leftarrow rs \text{ funct (Immidiat 16)}$

	rs	rt	I16
31-26	25-21	20-16	15-0

Load:  $rt \leftarrow \text{Mem}[rs + I16]$  Store:  $\text{Mem}[rs + I16] \leftarrow rt$

35 or 43	rs	rt	I16
31-26	25-21	20-16	15-0

Branch equal:  $PC \leftarrow (rs == rt) ? PC + 4 + I16 \ll 2 : PC + 4$

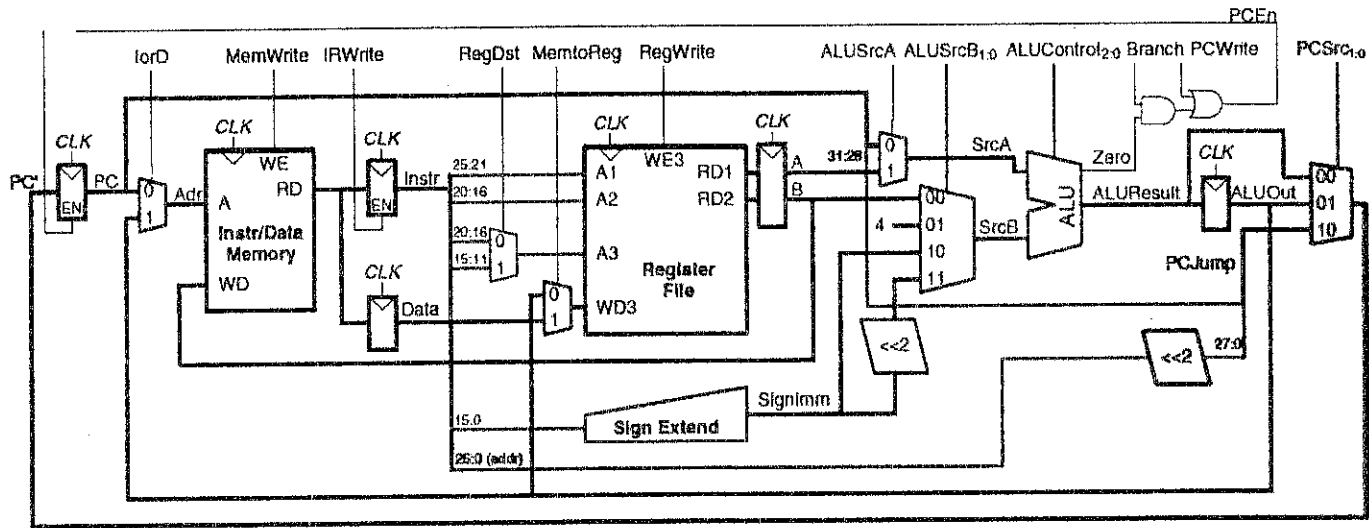
4	rs	rt	I16
31-26	25-21	20-16	15-0

J instruction (J, Jal) :  $PC \leftarrow PC_{31-28} IR_{25-0} 00$

2	I26
---	-----

## Exercice 4 : (5 pts)

Soit le schéma suivant d'un  $\mu P$  MIPS multi-cycle



1.

(a) Si nous supposons exécuter l'instruction « add \$t3,\$s0,\$s1 », quelles sont alors les valeurs de A1, A2, A3 et RegDst?

A1	A2	A3	RegDst

(b) Supposons exécuter l'instruction « lw \$t2,-4(\$s4) » et que le registre \$s4 contient la valeur 0x0000ff08 et \$t2 = 0xFFFFFFF5. Quelles sont alors les valeurs utiles des signaux de commande suivants pour réaliser l'instruction: Jump, RegWrite, RegDst, ALUSrc, ALUControl, Branche, MemWrite et MemToReg ? Aussi, quelles valeurs ont le le signal d'adresse A et le signal d'écriture de données WD de la mémoire de données ?

RegWrite,	RegDst	ALUSrc	ALUControl	Branche	MemWrite	MemToReg

A	WD

(c) Si le code machine actuel qui s'exécute est 0x214bffff et les valeurs des registres dans le processeur sont comme indiqué ci-dessous, quelle est alors la valeur de l'entrée WD3 ? Répondre sous forme de valeur hexadécimale de 32 bits.

\$at = 0x00011021	.....
\$v0 = 0x5234f1a0	.....
\$v1 = 0x1114f111	.....
\$a0 = 0xff001231	.....
\$a1 = 0xffffffff	.....
\$a2 = 0x32252341	.....
\$a3 = 0xff1245ee	.....
\$t0 = 0xffff12ff	.....
\$t1 = 0xffffffff	.....
\$t2 = 0xffffffff5	.....
\$t3 = 0xffffffff67f	.....
\$t4 = 0x0121ffff	.....

\$t5 = 0x55f7fff5

2. Pour chacun des déclarations suivantes, répondez si la déclaration est vraie ou fausse.

(a) Le signal de contrôle RegWrite doit être 0 lorsque MemToReg est 0, car WD3 peut (en ce cycle), obtenir une valeur erronée.

(b) Le signal de commande Branch doit toujours être à 1 lorsqu'une instruction beq est exécutée.

(c) Le signal de commande RegDst ne dépend que des 6 bits de poids fort du code machine d'une instruction MIPS.

(d) Le signal de commande ALUControl ne dépend que des 6 bits de poids faible du code machine d'une instruction MIPS.

(e) les variables globales sont adressées en utilisant le registre \$gp. Aussi il y'a un registre spécifique pour pointer sur les variables normales dans la zone mémoire « Dynamic Data »

3. Répondez aux questions suivantes

(a) Lors de démarrage (à l'état initial) d'un système à base de µP MIPS, quel est l'adresse contenu dans le registre PC.

(b) Pour quoi les deux bits de poids faibles de l'adresse d'une instruction sont toujours à « 00 »

(c) Expliquez ce que se passe à l'étape "Fetch" dans le fonctionnement d'un processeur MIPS.

(d) Expliquez pourquoi le calcul de  $PC+4+Ix4$  doit précéder la soustraction pour la comparaison des registres RS et RT dans l'exécution de l'instruction branche (Beq) en ayant lieu à l'étape Decode.

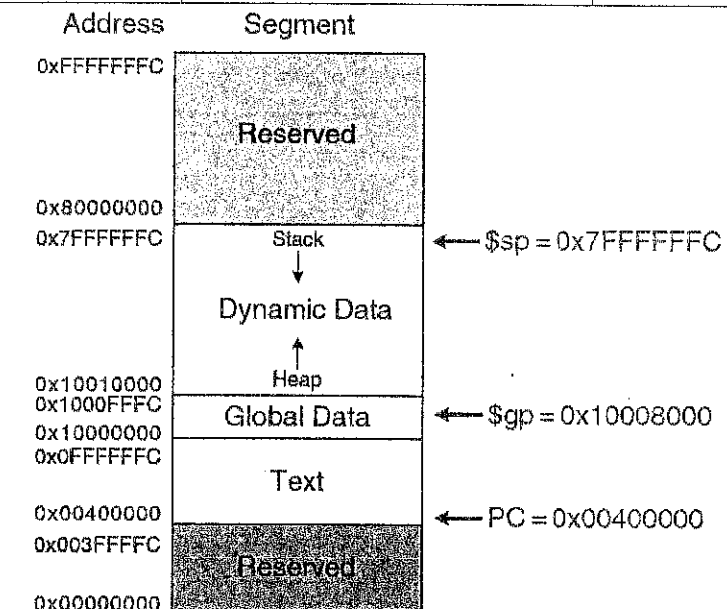
(e) Si une donnée globale est stockée dans l'adresse 10000004H. que doit être l'offset en hexa par rapport à \$gp

(f) L'instruction machine est composé du code opération et du code opérande. Dans le processeur MIPS, le code opérande peut être composé de (deux réponses sont à cocher)

- ☐ Adresses mémoire seulement
- ☐ Registres ou registres et valeur immédiate
- ☐ Registres ou registres et valeur immédiate ou registres et adresse mémoire
- ☐ Adresse mémoire, registre et valeurs immédiates à la fois
- ☐ Registres ou registres et valeur immédiate ou registres et offset adresse mémoire
- ☐ Registre et adresse mémoire ou adresses mémoires seules
- ☐ Registres ou registres et valeur immédiate ou adresse mémoire et valeur immédiate

### Code opération et code fonction de quelques instructions :

Instruction	Code opération	Code fonction
Addi (RI type)	001000 (8)	X
Sll (R type)	000000 (0)	000000 (0)
Or (R type)	000000 (0)	100101 (37)
Add (R type)	000000 (0)	100000 (32)
Sub (R type)	000000 (0)	100010 (34)
slt (R type)	000000 (0)	101010 (42)
beq	000100 (4)	x
bne	000101 (5)	x
J	000010 (2)	x
Jal	000011 (3)	X
SW	101011 (43)	X
LW	100011 (35)	x
Jr	000000 (0)	001000 (8)



### Control Unit: ALU Decoder

ALUOp <sub>1:0</sub>	Meaning
00	Add
01	Subtract
10	Look at Funct
11	Not Used

ALUOp <sub>1:0</sub>	Funct	ALUControl <sub>2:0</sub>
00	XXXXXX	010 (Add)
X1	XXXXXX	110 (Subtract)
1X	100000 [add]	010 (Add)
1X	100010 [sub]	110 (Subtract)
1X	100100 [and]	000 (And)
1X	100101 [or]	001 (Or)
1X	101010 [slt]	111 (SLT)

### EXERCICE 3 (10 pts)

Soient l'image  $I$  et le filtre  $F$  de Prewitt caractérisé par les masques  $H1$  et  $H2$  suivants:

0	0	0	0	0
0	0	0	100	100
0	100	100	100	100
100	100	200	200	100
100	200	200	200	100

$H1 \quad 1 \ 6 \ *$

-1	0	1
-1	0	1
-1	0	1

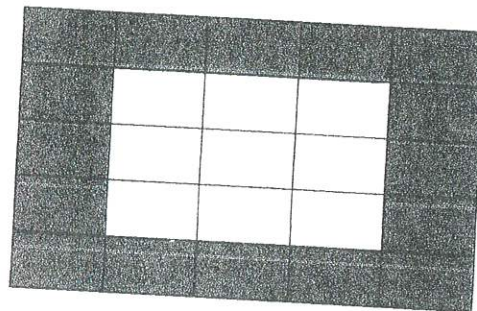
$H2 \quad 1 \ 6 \ *$

-1	-1	-1
0	0	0
1	1	1

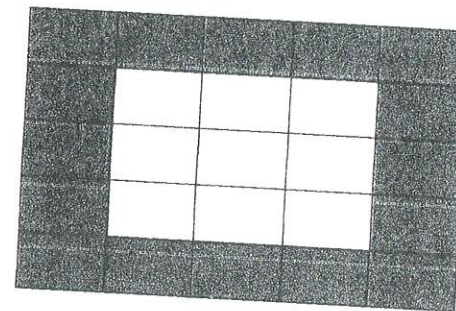
2.1 De quelle famille est ce filtre ? Quel est l'effet du filtre  $F$  sur l'image ?

2.2 Appliquer ce filtre sur la partie P de l'image allant de : ligne 2 à ligne 4, colonne 2 à colonne 4 (c'est-à-dire  $I[2:4, 2:4]$ )

Application du masque  $H1$  sur  $I$

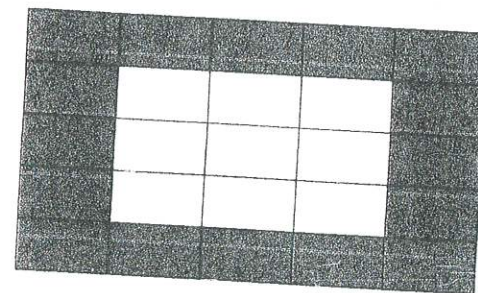


Application du masque  $H2$  sur  $I$



2.3 Calculer la norme de la dérivée de l'image  $I$ . Utiliser la formule ci-après

$$|\nabla I| = \left| \frac{\partial I}{\partial x} \right| + \left| \frac{\partial I}{\partial y} \right|$$



2.4 Quelle est la relation entre contour et gradient?

2.5 Déterminer les pixels candidats appartenant au contour dans la partie  $P$  de l'image par utilisation du gradient (PS : donner les coordonnées des pixels)

Nombre de  
Doubles feuilles :

Numéro  
double feuille :

Signature du surveillant

Examen : Traitement d'images et Reconnaissance de Formes

Master-Pro, GL-1

Session Principale

Enseignante : A. Ben Abdallah Bedoui

Janvier 2025, Documents : Non autorisés, Calculatrice : Autorisée

Nombre de doubles feuilles : 2

Nom Etudiant : ..... NCIN:..... Section :.....

Prénom Etudiant : ..... NCE :..... N° de salle :.....

N° de place :.....

Signature du correcteur

Note

### EXERCICE 1 (5 pts)

Instructions : Entourer la ou les bonnes réponses pour chaque question.

1. L'étirement d'histogramme a pour but principal de :

- a) Réduire le bruit dans l'image.
- b) Augmenter le contraste de l'image en élargissant la plage dynamique des niveaux de gris.
- c) Rendre l'histogramme de l'image uniforme.
- d) Détecter les contours dans l'image.

2. L'égalisation d'histogramme vise à :

- a) Uniformiser la distribution des niveaux de gris dans l'image.
- b) Assombrir l'image.
- c) Éclaircir l'image.
- d) Augmenter la netteté de l'image.

3. Un filtre passe-bas :

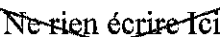
- a) Laisse passer les hautes fréquences et atténue les basses fréquences.
- b) Atténue les hautes fréquences et laisse passer les basses fréquences.
- c) Augmente le contraste de l'image.
- d) Détecte les contours.

4. L'étirement d'histogramme est particulièrement utile pour les images :

- a) Très bruitées.
- b) Avec un contraste élevé.
- c) Avec un faible contraste.
- d) En couleur.

5. Un filtre passe-bas peut être utilisé pour :

- a) Réduire le bruit dans l'image.
- b) Accentuer les détails fins.
- c) Détecter les contours.
- d) Augmenter le contraste.



- a) Réduire le bruit.
- b) Amplifier le bruit.
- c) Ne pas modifier le contraste.
- d) Rendre l'image plus floue.

- a) L'égalisation d'histogramme.
- b) L'étirement d'histogramme.
- c) L'addition d'une constante à tous les pixels.
- d) La multiplication de tous les pixels par une constante.

- a) Le bruit gaussien.
- b) Le bruit impulsif (ou bruit "sel et poivre").
- c) Le flou.
- d) Les contours.

- a) Une opération de multiplication pixel par pixel entre deux images.
- b) Une opération de glissement d'un noyau (filtre) sur l'image, calculant une somme pondérée des pixels voisins.
- c) Une transformation géométrique de l'image.
- d) Une méthode de compression d'image.

- a) Locale.
- b) Globale.
- c) Linéaire.
- d) Non linéaire.

Soit l'image I suivante :

220	220	100	20	20
220	220	100	255	20
220	255	0	20	20
220	220	100	255	20
220	0	100	0	20
220	220	100	20	20

[illegible]


1  
 2  
 3  
 4  
 5  
 6  
 7  
 8  
 9  
 10  
 11  
 12  
 13  
 14  
 15  
 16  
 17  
 18  
 19  
 20  
 21  
 22  
 23  
 24  
 25  
 26  
 27  
 28  
 29  
 30  
 31  
 32  
 33  
 34  
 35  
 36  
 37  
 38  
 39  
 40  
 41  
 42  
 43  
 44  
 45  
 46  
 47  
 48  
 49  
 50  
 51  
 52  
 53  
 54  
 55  
 56  
 57  
 58  
 59  
 60  
 61  
 62  
 63  
 64  
 65  
 66  
 67  
 68  
 69  
 70  
 71  
 72  
 73  
 74  
 75  
 76  
 77  
 78  
 79  
 80  
 81  
 82  
 83  
 84  
 85  
 86  
 87  
 88  
 89  
 90  
 91  
 92  
 93  
 94  
 95  
 96  
 97  
 98  
 99  
 100  
 101  
 102  
 103  
 104  
 105  
 106  
 107  
 108  
 109  
 110  
 111  
 112  
 113  
 114  
 115  
 116  
 117  
 118  
 119  
 120  
 121  
 122  
 123  
 124  
 125  
 126  
 127  
 128  
 129  
 130  
 131  
 132  
 133  
 134  
 135  
 136  
 137  
 138  
 139  
 140  
 141  
 142  
 143  
 144  
 145  
 146  
 147  
 148  
 149  
 150  
 151  
 152  
 153  
 154  
 155  
 156  
 157  
 158  
 159  
 160  
 161  
 162  
 163  
 164  
 165  
 166  
 167  
 168  
 169  
 170  
 171  
 172  
 173  
 174  
 175  
 176  
 177  
 178  
 179  
 180  
 181  
 182  
 183  
 184  
 185  
 186  
 187  
 188  
 189  
 190  
 191  
 192  
 193  
 194  
 195  
 196  
 197  
 198  
 199  
 200  
 201  
 202  
 203  
 204  
 205  
 206  
 207  
 208  
 209  
 210  
 211  
 212  
 213  
 214  
 215  
 216  
 217  
 218  
 219  
 220  
 221  
 222  
 223  
 224  
 225  
 226  
 227  
 228  
 229  
 230  
 231  
 232  
 233  
 234  
 235  
 236  
 237  
 238  
 239  
 240  
 241  
 242  
 243  
 244  
 245  
 246  
 247  
 248  
 249  
 250  
 251  
 252  
 253  
 254  
 255  
 256  
 257  
 258  
 259  
 260  
 261  
 262  
 263  
 264  
 265  
 266  
 267  
 268  
 269  
 270  
 271  
 272  
 273  
 274  
 275  
 276  
 277  
 278  
 279  
 280  
 281  
 282  
 283  
 284  
 285  
 286  
 287  
 288  
 289  
 290  
 291  
 292  
 293  
 294  
 295  
 296  
 297  
 298  
 299  
 300  
 301  
 302  
 303  
 304  
 305  
 306  
 307  
 308  
 309  
 310  
 311  
 312  
 313  
 314  
 315  
 316  
 317  
 318  
 319  
 320  
 321  
 322  
 323  
 324  
 325  
 326  
 327  
 328  
 329  
 330  
 331  
 332  
 333  
 334  
 335  
 336  
 337  
 338  
 339  
 340  
 341  
 342  
 343  
 344  
 345  
 346  
 347  
 348  
 349  
 350  
 351  
 352  
 353  
 354  
 355  
 356  
 357  
 358  
 359  
 360  
 361  
 362  
 363  
 364  
 365  
 366  
 367  
 368  
 369  
 370  
 371  
 372  
 373  
 374  
 375  
 376  
 377  
 378  
 379  
 380  
 381  
 382  
 383  
 384  
 385  
 386  
 387  
 388  
 389  
 390  
 391  
 392  
 393  
 394  
 395  
 396  
 397  
 398  
 399  
 400  
 401  
 402  
 403  
 404  
 405  
 406  
 407  
 408  
 409  
 410  
 411  
 412  
 413  
 414  
 415  
 416  
 417  
 418  
 419  
 420  
 421  
 422  
 423  
 424  
 425  
 426  
 427  
 428  
 429  
 430  
 431  
 432  
 433  
 434  
 435  
 436  
 437  
 438  
 439  
 440  
 441  
 442  
 443  
 444  
 445  
 446  
 447  
 448  
 449  
 450  
 451  
 452  
 453  
 454  
 455  
 456  
 457  
 458  
 459  
 460  
 461  
 462  
 463  
 464  
 465  
 466  
 467  
 468  
 469  
 470  
 471  
 472  
 473  
 474  
 475  
 476  
 477  
 478  
 479  
 480  
 481  
 482  
 483  
 484  
 485  
 486  
 487  
 488  
 489  
 490  
 491  
 492  
 493  
 494  
 495  
 496  
 497  
 498  
 499  
 500  
 501  
 502  
 503  
 504  
 505  
 506  
 507  
 508  
 509  
 510  
 511  
 512  
 513  
 514  
 515  
 516  
 517  
 518  
 519  
 520  
 521  
 522  
 523  
 524  
 525

[illegible]





.....

.....

Enseignant : BRAHEM TAOUFIK	Durée : 1H	Nb Pages : 3	Filière : ING 2-Info
Examen session janvier 2025			
Nom et Prénom:.....N°d'inscription.....			

### Exercice n°1

1) Donner la définition aux termes suivants :

a) Méthode SMART

.....

.....

.....

b) Méthode QQQQCP

.....

.....

.....

2) Quels sont les objectifs de l'entreprise ?

.....

.....

.....

3) Quels sont les différents types d'immobilisations?

.....

.....

### Exercice n°2

Le 1/7/2023, la société "Progrès" a acquis un camion d'une valeur 71 400 D TTC, TVA 19%, amortissable selon le mode d'amortissement linéaire sur 5 ans.

Calculer le montant de l'amortissement au 31/12/2023 et au 31/12/2024.

.....

.....

.....

.....

### Exercice n°3

En raison d'un ralentissement des ventes pendant l'été, la société Moderne prévoit des difficultés de trésorerie dans les prochains mois. Elle tient une comptabilité prévisionnelle. Le comptable Mr Tej a établi partiellement les différents budgets, il vous invite à compléter cette étude trimestrielle vous disposez des informations suivantes:

NE RIEN ECRIRE ICI

Prévisions des achats et des ventes (Somme en dinars)

Eléments	Juin	Juillet	Aout
Ventes H TVA 19 %	200 000	180 000	150 000
Achats H TVA 19 %	250 000	270 000	300 000

- encaissements des ventes:
  - ✓ 20 % au comptant
  - ✓ 40 % dans un mois
  - ✓ 40 % dans deux mois
- règlements des achats:
  - ✓ 20 % au comptant
  - ✓ 80 % dans deux mois

**Travail à faire :**

- 1) compléter le budget de trésorerie
- 2) commenter les résultats obtenus

**Budget de Trésorerie**

Eléments	Juin	Juillet	Aout	Autres
<b>Encaissements</b>				
Ventes: Juin:.....			95 200	
Juillet : 214 200				
Aout : .....				
Autres encaissement	377 600	115 600		
<b>Total des encaissements</b>				
<b>Décaissements</b>				
Achats : juin: .....				
Juillet : .....				257 040
Aout : 357 000				
Autres décaissement	389 400	194 700		
<b>Total des décaissements</b>				
<b>Synthèses</b>				
Trésorerie initiale	1 600			
Total encaissements				
Total décaissements				
<b>Trésorerie finale</b>				

Commentaire:

.....

.....

.....

.....

.....

.....





**Examen S1**  
**Session principale**

Département :	Informatique	Date :	18 Janvier 2025
Classe :	ING2-GL	Documents :	Non autorisés
Matière :	Design patterns et conception par contrat	Durée :	1h30mn
Enseignante :	Mme Sameh HBAIEB	Nb pages :	3 pages

**Exercice 1**

Nous considérons l'application Twitter, permettant d'échanger des « Tweets » ou messages courts avec le monde entier. Par exemple, l'utilisateur @xyz peut envoyer le tweet « Aime #Design Pattern @PascalRoques » qui utilise le tag #Design Pattern et cite explicitement l'utilisateur « @PascalRoques ».

Tout utilisateur muni d'un compte est associé à un fil d'actualité, visible par tous, qui porte par ordre chronologique du plus récent au plus ancien tout tweet :

- qu'il a tweeté,
- qu'il a retweeté,
- qui le cite explicitement dans le corps du tweet,
- qu'un utilisateur auquel il est abonné à lui-même tweeté ou retweeté.

Nous allons faire plusieurs hypothèses simplifiant le problème dans cet énoncé :

- Les tweets sont du texte pur, on ne peut pas attacher d'images ou fichier.
- On ne peut pas rajouter du texte quand on « retweete » un message.
- Retweeter consiste simplement à ajouter le tweet en question à son propre fil d'actualité ainsi qu'à celui de tous ses abonnés potentiels.
- On ignore l'authentification et la création de compte (profil etc...) dans tout l'exercice

Une première version du diagramme de classe (diagramme d'analyse) modélisant ce problème est présentée en figure 1.

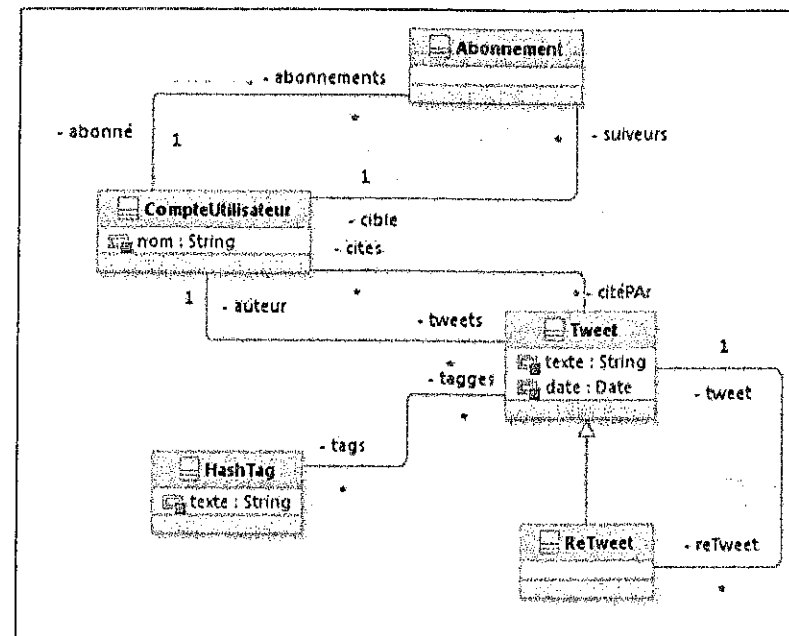


Figure 1. Diagramme de classes d'analyse

Un compte twitter (utilisateur) peut avoir un nombre arbitraire d'abonnés. A chaque fois qu'un utilisateur publie un Tweet, ses abonnés sont notifiés.

#### Questions :

1. Quel design pattern modélise le mieux cette fonctionnalité ?
2. Quels sont les principes respectés par ce design pattern ?
3. Complétez le diagramme de classes de la figure 1 pour adopter le pattern proposé (ajoutez également les méthodes nécessaires).
4. Présentez par un diagramme de séquence les interactions entre les différentes entités participantes dans ce patron.

## Exercice 2

Dans cet exercice nous allons modéliser des expressions arithmétiques sous la forme d'un arbre binaire. Seules l'addition et la soustraction devront être considérées. Un Arbre possède un Noeud racine et un nom. Un Noeud est soit un NoeudPlus, soit un NoeudMoins, soit un NoeudValeur. NoeudPlus et NoeudMoins possède chacun un noeud droit et un noeud gauche. NoeudValeur possède une valeur (un entier). Vous modéliserez Noeud sous la forme d'une interface.

#### Questions :

1. Proposez une modélisation des arbres binaires tels que spécifiés ci-dessus.
2. On souhaite introduire des visiteurs à la structure d'arbre binaire. Définissez l'objectif de ce patron. Pourquoi les méthodes accept() sont-elles nécessaires ?
3. Complétez le diagramme de classe proposé en question 1 de sorte à pouvoir appliquer le patron de conception Visiteur. En particulier, une interface Visiteur permettra de visiter tous les éléments de l'arbre.
4. Implémentez et testez un Visiteur pour calculer la valeur d'une expression arithmétique.

*Bon travail*

d) La multicollinéarité n'a aucun impact sur la régression linéaire et n'affecte pas les coefficients.

Exercice 2 (5 points)

A. Soit les paramètres de l'architecture VGG16 suivants, les images en couleurs de taille 224 × 224, Nombre de filtres=64, Taille du filtre=3, Pas de décalage=1, Padding P=1,

1. Expliquer et donner les dimensions du volume envoyé par :

a. La première couche de convolution :

b. La couche de ReLU

c. La couche de pooling, paramètres : Taille du filtre=2, Pas de décalage=2.

2. Combien de paramètres VGG-16 doit apprendre pendant la phase d'entraînement pour la première couche de convolution? (les poids des filtres de convolution ainsi que les biais associés)

B. Répondez par oui ou non et expliquez brièvement :

1. La couche de pooling permet d'éviter le sur-apprentissage ?

2. La rétropropagation est-elle spécifique aux réseaux de neurones et n'est pas utilisée dans d'autres types de modèles d'apprentissage automatique?

Université de Monastir

Institut Supérieur d'Informatique et de Mathématiques de Monastir

Examen: Machine Learning avec python

Filière : ING2\_Info

Nom : .....

Prénom : .....

N°C.I.N : .....N° Inscription.....

Salle N°.....Place N°.....

Signatures des  
surveillants

Identifiant Secret

Note/20	<b>Examen: Machine Learning avec python</b>		Identifiant Secret
	Nombre de pages : 4		
	Durée : 1:30h	Documents <b>non</b> autorisés	
	Enseignante : M. SEKMA	Filière : ING2_Info	

Exercice 1 (15 points) : Entourez la bonne réponse.

- Quelle est la principale différence entre la normalisation et la standardisation dans le contexte du Feature Scaling ?
  - La normalisation rend les données centrées autour de zéro avec un écart type de 1, tandis que la standardisation ajuste les données entre 0 et 1.
  - La normalisation ajuste les données entre 0 et 1, tandis que la standardisation rend les données centrées autour de zéro avec un écart type de 1.
  - La normalisation et la standardisation sont des termes interchangeables, sans différence significative.
  - La normalisation rend les données plus interprétables, tandis que la standardisation améliore les performances des modèles.
- Comment sélectionner toutes les lignes d'un DataFrame où la valeur dans la colonne 'Score' est supérieure à 90?
  - df[Score > 90]
  - df[df['Score'] > 90]
  - df.select\_rows('Score > 90')
  - df.filter('Score > 90')
- Quelle fonction d'activation est utilisée dans une couche Dense pour introduire une non-linéarité?
  - activation='sigmoid'
  - activation='tanh'
  - activation='relu'
  - activation='softmax'

**NE RIEN ECRIRE ICI**

4. Que devez-vous ajouter comme paramètre manquant à cette ligne de code pour configurer le modèle afin d'effectuer une classification binaire?

```
model.compile(optimizer=optimizers.Adam(lr=1e-4), _____, metrics=['accuracy'])
```

- a) `loss='mean_squared_error'`
  - b) `loss='huber_loss'`
  - c) `loss='binary_crossentropy'`
  - d) `loss='loss_binary_crossentropy'`
5. Quel est le rôle de la méthode de régularisation (**dropout**) dans l'apprentissage des réseaux neuronaux?
- a) Augmenter le surajustement
  - b) Accélérer la convergence
  - c) Prévenir le surajustement
  - d) Réduire la précision du modèle
6. Quel est l'avantage principal d'ElasticNet par rapport à Ridge et Lasso ?
- a) ElasticNet est plus efficace lorsque les données sont fortement corrélées.
  - b) ElasticNet est plus rapide à entraîner que Ridge et Lasso.
  - c) ElasticNet ne nécessite pas d'hyperparamètre de régularisation.
  - d) ElasticNet ne fait pas de sélection de variables, contrairement à Lasso.
7. Quelle fonctionnalité est activée par le paramètre `include_top` dans la création d'un modèle **VGG16** à l'aide de la ligne de code suivante ?
- ```
model = VGG16(weights='imagenet', include_top=True)
```
- a) Exclure les couches `fully connected` à la fin du réseau.
  - b) Utiliser des poids pré-entraînés provenant d'ImageNet.
  - c) Inclure les couches `fully connected` à la fin du réseau.
8. Quelle stratégie est mise en œuvre lorsqu'on ajuste seulement quelques couches du modèle pré-entraîné tout en laissant les autres figées pour l'apprentissage ?
- a) `fine-tuning total`
  - b) Extraction des features
  - c) Les couches `fully connected`
  - d) `fine-tuning partiel`
9. Dans quel cas serait-il avantageux d'appliquer la stratégie du "fine-tuning total" ?
- a) Lorsque la nouvelle collection d'images est petite, pour éviter le surajustement.

- b) Lorsque l'on souhaite uniquement extraire les caractéristiques du modèle pré-entraîné.
  - c) Lorsque l'on souhaite réentraîner uniquement quelques couches du modèle pré-entraîné.
  - d) Lorsque la nouvelle collection d'images est grande, pour éviter le surajustement.
10. Pourquoi l'ajout du poids de l'élément de **biais** rend-il le nœud plus flexible dans un réseau de neurones?
- a) Il augmente la complexité du modèle en introduisant une non-linéarité.
  - b) Il permet au nœud de prendre en compte les variations dans les données d'entrée.
  - c) Il régularise le modèle en évitant le surajustement.
  - d) Il simplifie la tâche d'optimisation en facilitant la convergence du modèle.
11. Les hyperparamètres dans l'apprentissage automatique sont :
- a) Des paramètres qui n'ont pas d'impact sur l'apprentissage et la structure du modèle.
  - b) Les caractéristiques d'entrée du modèle.
  - c) Des paramètres qui sont appris à partir des données.
  - d) Des paramètres définis avant l'apprentissage et externes au modèle.
12. Quelle interprétation est correcte pour une valeur de RMSE de 96 dans le contexte de la prédiction des prix en dinars ?
- a) La valeur prédite est, en moyenne, 96 dinars plus élevée que la valeur réelle.
  - b) La valeur prédite est, en moyenne, 96 dinars plus basse que la valeur réelle.
  - c) La valeur prédite peut varier, en moyenne, de +/- 96 dinars par rapport à la valeur réelle.
  - d) La moyenne entre la valeur prédite et la valeur réelle est égale à 96.
13. Quelle est la formule correcte pour calculer la racine de l'erreur quadratique moyenne (RMSE)?
- a)  $RMSE = \sqrt{(\sum(y - \hat{y})^2 / n)}$
  - b)  $RMSE = \sqrt{(\sum(y - \hat{y}) / n)}$
  - c)  $RMSE = \sqrt{(\sum(y - \hat{y})^2) / n}$
  - d)  $RMSE = \sum(\sqrt{(y - \hat{y})^2}) / n$
14. Vous analysez des données sur les dépenses mensuelles des clients en fonction de revenu, l'âge et la localisation géographique. L'objectif est de prédire si un client effectuera un achat important, défini par une dépense mensuelle dépassant un seuil spécifique. Quelle méthode serait la plus appropriée pour résoudre ce problème?
- a) Régression simple
  - b) Régression logistique
  - c) Classification
  - d) Segmentation
15. Quel est l'impact de la multicolinéarité sur les coefficients dans un modèle de régression linéaire ?
- a) La multicolinéarité rend les coefficients du modèle plus stables et moins sensibles aux changements dans les données.
  - b) La multicolinéarité entraîne des coefficients instables,
  - c) La multicolinéarité améliore la précision des prédictions en réduisant l'erreur de prédiction.





Devoir Surveillé– S1 – 2024/2025

|                                    |                                    |                            |
|------------------------------------|------------------------------------|----------------------------|
| Classe : 2 <sup>ème</sup> Ing Info | Matière :<br>Sécurité Informatique | Enseignant :<br>Zied Jaoua |
| Date : 23 / 11 / 2024              | Calculatrices autorisées : Oui     |                            |
| Durée de l'examen : 1h             | Nombre de pages : 04               |                            |

6) Soient A et B deux entités utilisant le procédé de chiffrement décrit dans cet exercice. La clé K doit être échangée d'une façon sécurisée et authentifiée. Pour cela A et B font appel au chiffrement asymétrique. A calcule la clé K, la chiffre pour obtenir KC et l'envoi à B.

- Avec quelle clé A doit chiffrer K ?
- Avec quelle clé B déchiffre KC ?
- Expliquer pourquoi cette méthode n'est pas authentifiée et proposer une solution ?

Exercice 3 (Cryptographie RSA et authentification).

Un professeur envoie ses notes au secrétariat de l'école par mail. La clef publique du professeur est  $(e_p, n_p) = (3, 55)$ , celle du secrétariat  $(e_s, n_s) = (3, 33)$ .

- Déterminer la clé privée du professeur et du secrétariat de l'école.
- Pour assurer la confidentialité de ses messages, le professeur chiffre les notes avec la clef RSA du secrétariat. Quel message chiffré correspond à la note 10 ?
- Pour assurer l'authenticité de ses messages, le professeur signe chaque note avec sa clé privée et chiffre le résultat avec la clef RSA du secrétariat. Le secrétariat reçoit ainsi le message 23. Quelle est la note correspondante ?

Exercice 4

Expliquez par un schéma le fonctionnement du protocole d'échange de Diffie-Hellman. Et donnez la formule de la clef secrète résultant en fonction des valeurs publiques et privées?

Exercice 1 : QCM (Plusieurs choix sont corrects) Ne pas répondre directement sur cette feuille

- Quels sont les objectifs principaux de la cryptographie à clé publique ?
  - Garantir l'intégrité des données
  - Garantir l'authenticité des données
  - Garantir la confidentialité des données
  - Permettre un chiffrement rapide et efficace
- Lequel des éléments suivants est un exemple de méthode de hachage cryptographique ?
  - SHA-256
  - RSA
  - Diffie-Hellman
  - MD5
- Parmi les attaques suivantes, laquelle utilise une méthode de "force brute" pour trouver une clé secrète ?
  - Attaque par dictionnaire
  - Attaque par canal auxiliaire
  - Attaque de type "Man-in-the-middle"
  - Attaque par force brute
- Quelle est la différence principale entre un algorithme de chiffrement symétrique et un algorithme de chiffrement asymétrique ?
  - Le chiffrement symétrique utilise la même clé pour le chiffrement et le déchiffrement, tandis que le chiffrement asymétrique utilise une paire de clés (publique et privée).
  - Le chiffrement asymétrique est plus rapide que le chiffrement symétrique.
  - Le chiffrement symétrique est utilisé pour le chiffrement des emails, tandis que l'asymétrique est utilisé pour les fichiers.
  - Le chiffrement symétrique garantit mieux la confidentialité que le chiffrement asymétrique.

5. Dans le cadre de l'algorithme RSA, que représente la clé privée dans une paire de clés ?
- La clé utilisée pour signer numériquement les messages.
  - La clé utilisée pour chiffrer les messages.
  - La clé utilisée pour vérifier la signature du message.
  - La clé utilisée pour déchiffrer les messages chiffrés avec la clé publique.
6. Quelle est la principale différence entre le chiffrement de type "stream cipher" et "block cipher" ?
- Un chiffrement de type stream chiffre un bit ou un octet à la fois, tandis que le block cipher chiffre un bloc de données (par exemple, 128 bits) à la fois.
  - Les "block ciphers" sont plus vulnérables aux attaques par canal auxiliaire que les "stream ciphers".
  - Un chiffrement de type stream est généralement plus rapide que le chiffrement de type block pour des volumes de données plus importants.
  - Les "block ciphers" peuvent utiliser des modes comme ECB, CBC ou CTR pour améliorer la sécurité.
7. Quelle(s) attaque(s) peuvent affecter les systèmes de cryptographie symétrique utilisant un mode de chiffrement ECB (Electronic Codebook) ?
- Attaque par substitution de blocs.
  - Attaque par analyse de fréquence.
  - Attaque par injection de texte clair.
  - Attaque par modification de texte chiffré.
8. Parmi les affirmations suivantes sur le chiffrement symétrique, lesquelles sont correctes ?
- Une clé symétrique peut être utilisée pour chiffrer plusieurs messages.
  - Tous les systèmes de chiffrement symétrique nécessitent des clés aussi longues que les messages à chiffrer.
  - Le chiffrement symétrique peut être très rapide en termes de performances.
  - La longueur des clés dans le chiffrement symétrique doit être assez grande pour éviter la recherche exhaustive des clés.
9. Pourquoi AES est-il considéré comme une amélioration majeure par rapport à DES ?
- Il utilise des clés plus longues et des blocs de données plus grands.
  - Il n'a aucune vulnérabilité connue même avec le mode ECB.
  - Il consomme plus de ressources pour garantir une meilleure sécurité.
  - Il inclut des fonctions comme SubByte, ShiftRows et MixColumns pour complexifier l'algorithme.
10. Quelle est une faiblesse critique de l'algorithme RC4 ?
- Il est trop lent pour les flux de données en temps réel.
  - Les premiers octets générés par le flux de clés sont biaisés.
  - Il nécessite une clé aussi longue que le flux de données.
  - Il ne peut pas utiliser de vecteur d'initialisation (IV).

11. Quel facteur a permis de casser le chiffrement de la machine Enigma ?
- Une faible longueur des clés.
  - Une utilisation répétée de courtes séquences de messages.
  - L'analyse fréquentielle des cryptogrammes.
  - Une permutation insuffisante des rotors.
12. Pourquoi le mode ECB (Electronic Codebook Mode) est-il considéré comme peu sûr ?
- Il utilise des clés trop courtes.
  - Il produit des cryptogrammes identiques pour des blocs identiques de message clair.
  - Il est vulnérable à la cryptanalyse fréquentielle.
  - Il n'est pas compatible avec des clés multiples.
13. Quelles sont les étapes impliquées dans la création et la vérification d'une signature numérique ?
- Créer une empreinte du message en utilisant une fonction de hachage.
  - Crypter l'empreinte avec une clé publique.
  - Vérifier la signature en comparant l'empreinte recalculée avec celle reçue.
  - Utiliser une clé privée pour crypter l'empreinte lors de la création de la signature.
14. Pourquoi Triple-DES (3DES) est-il plus sûr que DES standard ?
- Il utilise trois clés différentes pour augmenter la complexité.
  - Il utilise deux clés différentes et un chiffrement/déchiffrement supplémentaire.
  - Il allonge la taille des blocs pour éviter la répétition.
  - Il intègre des permutations aléatoires pour chaque bloc.

## Exercice 2 :

Soit  $M$  un message divisé en blocs  $\{x_1, x_2, x_3, \dots, x_p\}$  chacun de taille  $n$  bits et soit  $K$  une clé de même taille que les blocs ( $n$  bits). Soit  $\{c_1, c_2, c_3, \dots, c_p\}$  les cryptogrammes des blocs obtenus en appliquant la clé  $K$  aux blocs. Le chiffrement des blocs se fait selon le schéma suivant:  
 $C_0 = IV$  (valeur initiale) ; pour  $i$  de 1 à  $p$ ,  $c_i = E_K(C_{i-1} \oplus x_i)$

- La fonction  $E_K$  est inversible et son inverse est  $D_K$ . Montrer que l'opération de déchiffrement est  $x_j = C_{j-1} \oplus D_K(C_j)$  (rappel :  $A \oplus A = 0$  ;  $A \oplus 0 = A$ ,  $A \oplus B = B \oplus A$ )
- Peut-on chiffrer un bloc quelconque du message  $M$  sans chiffrer les blocs qui le précèdent ? Expliquer ?
- Peut-on déchiffrer un bloc quelconque ci sans déchiffrer les blocs qui le précèdent ? Expliquer ?
- Peut-on déchiffrer un bloc  $c_j$  en l'absence des autres blocs chiffrés ? Expliquer ?
- Prenons le cas où  $E_K(x) = D_K(x) = K \oplus x$ . Supposons qu'un attaquant a pu récupérer deux blocs consécutifs  $(x_{j-1}, x_j)$  ainsi que leurs cryptogrammes correspondants  $(c_{j-1}, c_j)$ . Montrer que cet attaquant peut en déduire la clé de chiffrement  $K$ .

b) Si le **revenu annuel** d'un client augmente de 1 000 dinars, quel impact cela aura-t-il sur le **montant d'emprunt approuvé**, en supposant que les autres caractéristiques restent constantes ?

.....

.....

.....

.....

c) Interprétez le coefficient de l'**historique de crédit** : que signifie un coefficient négatif dans ce cas ?

.....

.....

.....

.....

d) Quel rôle joue l'**âge** du client dans la prédiction du montant d'emprunt approuvé, en fonction de son coefficient ?

.....

.....

.....

.....

*Bon travail !*

Nom : .....

Prénom : .....

N°C.I.N : .....N° Inscription.....

Salle N°.....Place N°.....

Signatures des  
surveillants

Identifiant Secret

|         |                                         |                                |                    |
|---------|-----------------------------------------|--------------------------------|--------------------|
| Note/20 | <b>DS: Machine Learning avec python</b> |                                | Identifiant Secret |
|         | Nombre de pages : 4                     |                                |                    |
|         | Durée : 1h                              | Documents <b>non</b> autorisés |                    |
|         | Enseignante : M. SEKMA                  | Filières : ING_2_INFO          |                    |

- Le barème est donné à titre indicatif et peut subir éventuellement quelques modifications.
- Vous pouvez inclure des exemples ou des illustrations pour appuyer vos explications.

**Exercice 1 (4 points) Brièvement :**

1. Citez un exemple d'algorithme basé sur une instance et un autre basé sur un modèle.  
Expliquez brièvement comment chacun effectue ses prédictions.

.....

.....

.....

.....

.....

2. Expliquez la décomposition de l'erreur totale en biais, variance et bruit. En quoi ces trois composantes influencent-elles la performance d'un modèle ?

.....

.....

.....

.....

.....

NE RIEN ECRIRE ICI

## Exercice 2 (16 points)

Vous disposez d'un ensemble de données nommé **montants\_emprunt\_tnd.csv** contenant des informations sur les clients d'une banque.

```
Client_ID;Rev_ann;Age;Hist_cr;Nb_déf;Type_emp;Durée_remb;Montant_appr
C001;25000;32;1;0;1;60;45000
C002;50000;45;2;1;2;36;70000
.....
```

L'objectif est d'utiliser la **régression linéaire** pour prédire le **montant d'emprunt approuvé** en fonction des caractéristiques des clients.

**Client\_ID** : Identifiant unique pour chaque client  
**Rev\_ann (TND)** : Revenu annuel du client (en dinars).  
**Age** : Âge du client (en années).  
**Hist\_cr** : Historique de crédit du client (1 = Bon, 2 = Moyen, 3 = Mauvais).  
**Nb\_déf** : Nombre de paiements en retard ou défauts constatés.  
**Type\_emp** : Type d'emprunt demandé (1 = Immobilier, 2 = Personnel, etc.).  
**Durée\_remb** : Durée prévue pour le remboursement (en mois).  
**Montant\_appr (TND)** : Montant d'emprunt approuvé.

### 1. Compléter le code suivant selon les commentaires :

```
import ....
.....
.....
.....

# Lire le fichier et le stocker dans un DataFrame df
.....

# Afficher les deux premières lignes du DataFrame
.....

# Obtenir des informations sur les colonnes
```

.....  
# Explorer les valeurs manquantes pour chaque colonne  
.....

.....  
# Remplacer les valeurs manquantes par la moyenne  
.....

.....  
# Normalisation des colonnes numériques pour mettre à l'échelle (0 à 1)  
.....  
.....

.....  
# Diviser les données en caractéristiques (X) et cible (y)  
.....  
.....

.....  
# Diviser les données en ensembles d'entraînement et de test (80% / 20%)  
.....  
.....

.....  
# Instancier et entraîner le modèle de régression linéaire  
.....  
.....

.....  
# Prédire les montants approuvés sur l'ensemble de test  
.....

.....  
# Calculer le MSE et le RMSE  
.....  
.....

.....  
# Afficher les coefficients du modèle  
.....  
.....

2. Après avoir entraîné le modèle de régression linéaire pour prédire le montant d'emprunt approuvé, vous avez obtenu les coefficients suivants pour les caractéristiques du modèle :

**Rev\_ann: 500**  
**Age : 2000**  
**Hist\_cr: -3000**  
**Nb\_déf : -1500**  
**Type\_emp: 3000**  
**Durée\_remb: 250**

a) Que signifient ces coefficients dans le contexte du modèle ?  
.....  
.....  
.....





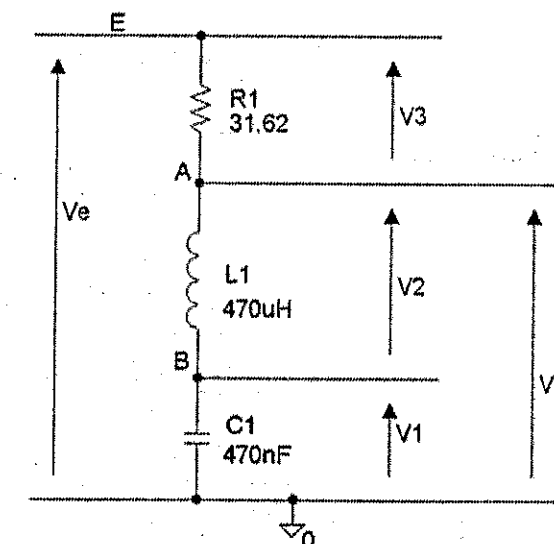
|                                      |                                         |               |                                |
|--------------------------------------|-----------------------------------------|---------------|--------------------------------|
| Filière :<br>Cycle d'Ingénieur .ING2 | Matière :<br><b>Filtrage Analogique</b> |               | Enseignant :<br>Ben Nasr Nejib |
| Date : 18/ 11/ 2024<br>Séance 4      | Nbr de Crédits :                        | Coefficient : | Documents autorisés : Non      |
| Durée de l'examen : 1h               | Régime d'évaluation : Mixte / CC        |               | Nombre de pages : 03           |

L'examen n'est pas une course de vitesse. Faites le maximum de ce que vous pouvez faire bien.

### DS Filtrage Analogique

#### Exercice1

Soit le filtre passif représenté à la Figure suivante :



Calculer les fonctions de transfert suivantes, et donner le type de filtre ainsi réalisé.

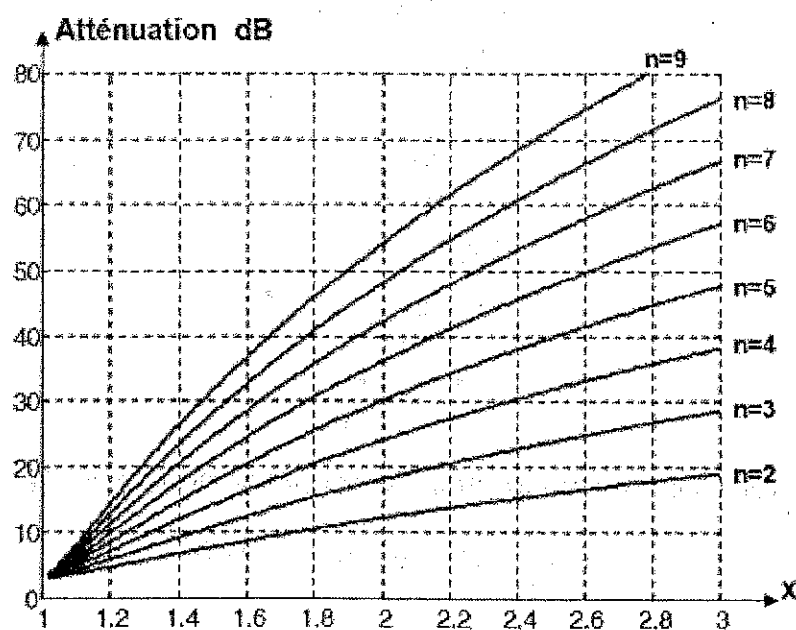
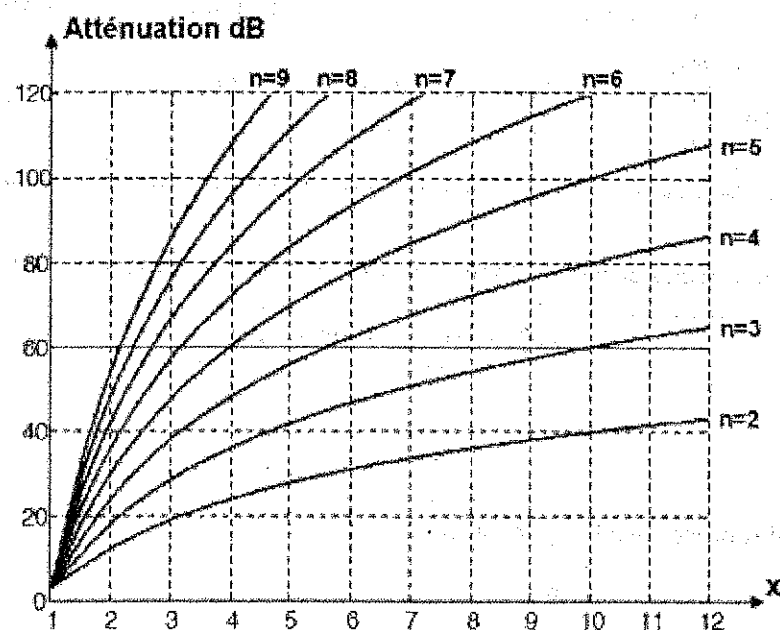
$$H_1 = \frac{V_1}{V_E}, H_2 = \frac{V_2}{V_E}, H_3 = \frac{V_3}{V_E} \text{ et } H_4 = \frac{V_4}{V_E},$$

Calculer littéralement et numériquement  $m$  et  $\omega_0$  pour pouvoir écrire les fonctions de transfert sous la forme générale d'un filtre du 2<sup>ème</sup> ordre

## Exercice 2 : Synthèse filtre

Dans le cadre d'un équipement audio pour une scène de spectacle on souhaite réaliser un filtre audio passe bas dont la fréquence de coupure est fixée à 16kHz. La proximité d'une alimentation à découpage induit un signal parasite à la fréquence de 48kHz que l'on souhaite supprimer en apportant une atténuation d'au moins 35dB.

1- Représenter le gabarit du filtre passe bas et en déduire l'ordre nécessaire pour une fonction d'approximation de type Butterworth à partir de l'abaque fournie ci-dessous (x est la sélectivité du filtre). Vous expliquerez votre démarche.



2- Montrer alors que le problème de filtrage précédent peut être résolu en utilisant un circuit LTC1563 dont vous préciserez la référence. En déduire la valeur de la résistance R qu'il convient de choisir



LTC1563-2/LTC1563-3

Active RC, 4th Order Lowpass Filter Family

## FEATURES

- Extremely Easy to Use—A Single Resistor Value Sets the Cutoff Frequency ( $256\text{Hz} < f_c < 256\text{kHz}$ )
- Extremely Flexible—Different Resistor Values Allow Arbitrary Transfer Functions with or without Gain ( $256\text{Hz} < f_c < 256\text{kHz}$ )
- Supports Cutoff Frequencies Up to 360kHz Using FilterCAD™
- LTC1563-2: Unity-Gain Butterworth Response Uses a Single Resistor Value, Different Resistor Values Allow Other Responses with or without Gain
- LTC1563-3: Unity-Gain Bessel Response Uses a Single Resistor Value, Different Resistor Values Allow Other Responses with or without Gain
- Rail-to-Rail Input and Output Voltages
- Operates from a Single 3V (2.7V Min) to  $\pm 5\text{V}$  Supply
- Low Noise:  $36\mu\text{V}_{\text{RMS}}$  for  $f_c = 25.6\text{kHz}$ ,  $60\mu\text{V}_{\text{RMS}}$  for  $f_c = 256\text{kHz}$
- $f_c$  Accuracy  $< \pm 2\%$  (Typ)
- DC Offset  $< 1\text{mV}$
- Cascadable to Form 8th Order Lowpass Filters
- Available in Narrow SSOP-16 Package

## APPLICATIONS

- Discrete RC Active Filter Replacement
- Antialiasing Filters
- Smoothing or Reconstruction Filters
- Linear Phase Filtering for Data Communication
- Phase Locked Loops

## DESCRIPTION

The LTC®1563-2/LTC1563-3 are a family of extremely easy-to-use, active RC lowpass filters with rail-to-rail inputs and outputs and low DC offset suitable for systems with a resolution of up to 16 bits. The LTC1563-2, with a single resistor value, gives a unity-gain Butterworth response. The LTC1563-3, with a single resistor value, gives a unity-gain Bessel response. The proprietary architecture of these parts allows for a simple resistor calculation:

$$R = 10\text{k} (256\text{kHz}/f_c); f_c = \text{Cutoff Frequency}$$

where  $f_c$  is the desired cutoff frequency. For many applications, this formula is all that is needed to design a filter. By simply utilizing different valued resistors, gain and other responses are achieved.

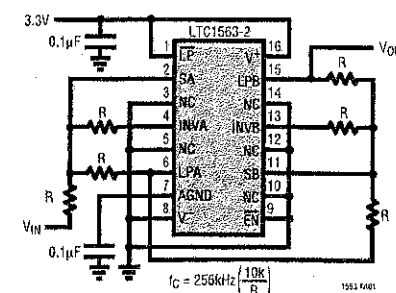
The LTC1563-X features a low power mode, for the lower frequency applications, where the supply current is reduced by an order of magnitude and a near zero power shutdown mode.

The LTC1563-Xs are available in the narrow SSOP-16 package (Same footprint as an SO-8 package).

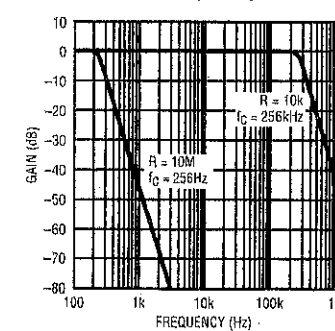
LT, LTC and LT are registered trademarks of Linear Technology Corporation. FilterCAD is trademark of Linear Technology Corporation. All other trademarks are the property of their respective owners.

## TYPICAL APPLICATION

Single 3.3V, 256Hz to 256kHz Butterworth Lowpass Filter



Frequency Response



1563231a

Devoir Surveillé S1

|               |                                           |             |               |
|---------------|-------------------------------------------|-------------|---------------|
| Département : | Informatique                              | Date :      | Novembre 2024 |
| Master :      | ING2 GL                                   | Documents : | Non autorisés |
| Matière :     | Design patterns et conception par contrat | Durée :     | 1h            |
| Enseignante : | Mme Sameh HBAIEB                          |             |               |

Etude de cas : Gestion des événements

Une équipe de développement désire créer une plateforme pour la gestion des événements. Cette plateforme permet d’offrir différents services aux utilisateurs (gestion d’agenda, l’envoi des emails d’invitation, gestion des contacts et profils, etc). L’accès aux différents services de la plateforme sera conditionné par l’authentification de l’utilisateur et chaque utilisateur étant défini par un profil, est géré par un annuaire notamment LDAP (Light Directory Access Protocol). LDAP est un serveur d’annuaire qui permet de sauvegarder des informations sur les utilisateurs (nom, prénom, etc.), et les données d’authentification ce qui permet la définition des droits d’accès à la plateforme.

Dans cet exercice, on se concentre sur le service gestion d’agenda. La figure présentée ci-dessous fournit une vue fonctionnelle de ce service.

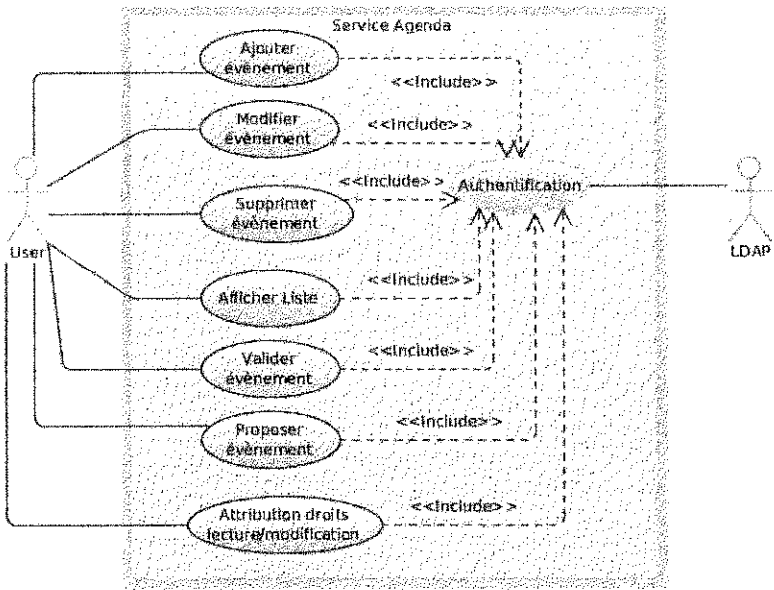


Figure 1. Service Agenda



Les événements peuvent prendre plusieurs formats. Exemple :

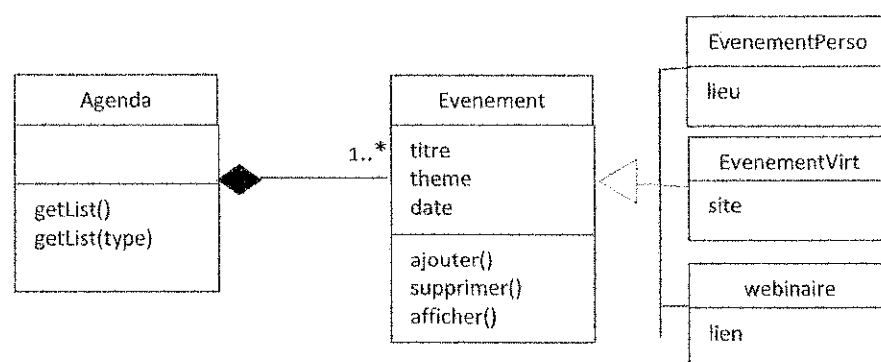
- Événements en personne tels que les conférences, salon de l'emploi, événements d'entreprise, etc
- Événements virtuels/hybrides tels que les conférences virtuelles, salon virtuel de l'emploi, foire d'exposition virtuelle, etc
- Webinaires et les sessions

### Partie 1. Questions de cours

Q1. Qu'est-ce qu'un design pattern ?

Q2. Expliquez le principe OCP (Open Closed Principe) et comment l'appliquer

### Partie 2. Mise en œuvre des design pattern



Q3. Détaillez le processus de création d'un événement en appliquant le patron Builder  
(Implémentez la classe EventBuilder).

Voici le résultat attendu :

```

Evenement event = new EventBuilder()
    .addTitre(" ")
    .addTheme(" ")
    .addDate(" ")
    .build();
    
```



Q4. En se basant sur la description fonctionnelle de la plateforme gestion des événements, définissez le point d'entrée (la façade) de ce SI

Q5. L'équipe de développement souhaite ajouter des sponsors (en option) pour certains événements. Ainsi, l'affichage d'un événement sera accompagné par la liste de ses sponsors.

- Comment implémenter cela (choix du design pattern)?
- Apportez les modifications nécessaires au diagramme de classes
- Implémentez la méthode afficher() avec le design pattern choisi

Q6. La plateforme gestion des événements interagit avec deux systèmes tiers :

- un serveur d'annuaire LDAP pour contrôler l'accès à la plateforme, et
- un autre système qui offre à son tour des événements pouvant être consultés par les utilisateurs de la plateforme. L'idée est d'offrir plus de choix aux utilisateurs qui cherchent des événements dans une thématique particulière. Ainsi les résultats des requêtes utilisateurs sont sauvegardés dans une cache pour des utilisations similaires.

Pour répondre à de tels besoins, il s'avère nécessaire d'utiliser le modèle de procuration (patron proxy) afin de préserver les fonctionnalités existantes.

- Citez 3 situations où ce patron de conception s'avère utile
- Modifiez votre conception en intégrant le patron proxy

Bon travail



1. Illustrer une solution utilisant le modèle de programmation *MapReduce* sur l'exemple.

|                         |  |                                                 |                 |                                                              |  |
|-------------------------|--|-------------------------------------------------|-----------------|--------------------------------------------------------------|--|
| Filière : Ing2_Info     |  | Matière :<br>Bases de données NOSQL et Big Data |                 | Enseignante :<br>Asma KERKENI                                |  |
| Date : 22 / 11 / 2024   |  | Nbr de Crédits : 3                              | Coefficient : 3 | <u>Calculatrice : autorisée</u><br>Documents autorisés : Non |  |
| Durée de l'épreuve : 1h |  | Régime d'évaluation : Mixte                     |                 | Nombre de pages : 5                                          |  |
|                         |  | EX (45%) + DS (22%) + TP (33%)                  |                 |                                                              |  |
| Nom & Prénom : .....    |  |                                                 |                 | Matricule :<br>.....                                         |  |
| Signature : .....       |  | Code confidentiel :                             |                 | Classe : ..... N° Place : .....                              |  |

NOTE : Répondre directement sur les feuilles de l'examen /

Note

/ 20

Exercice 1 : (10 points)

Cet exercice nécessite des réponses concises et précises aux questions posées. Répondez uniquement dans l'espace prévu, en fournissant la réponse attendue. Évitez les explications ou définitions longues.

1. Que signifie le terme "véracité" dans le contexte du Big Data ?
2. Qu'est-ce qu'un Data Lake?
3. Quelle cause majeure a entraîné l'explosion de données à l'origine de l'émergence du Big Data ?
4. Comment le NameNode détecte-t-il les nœuds en panne dans Hadoop ?

*Ne rien écrire ici*

5. Quelle est la principale limitation qui freine la scalabilité de Hadoop dans sa version 1.

6. Quel est le rôle du Job History Server dans Hadoop 2 ?

7. Quel démon gère les ressources sur un nœud worker dans YARN ?

8. Un fichier de 256 Go doit être stocké dans un cluster Hadoop avec une politique de réplication de 2. Si chaque DataNode dispose de 50 Go de capacité libre, combien de DataNodes sont nécessaires (taille de bloc de 128 Mo) pour stocker le fichier ?

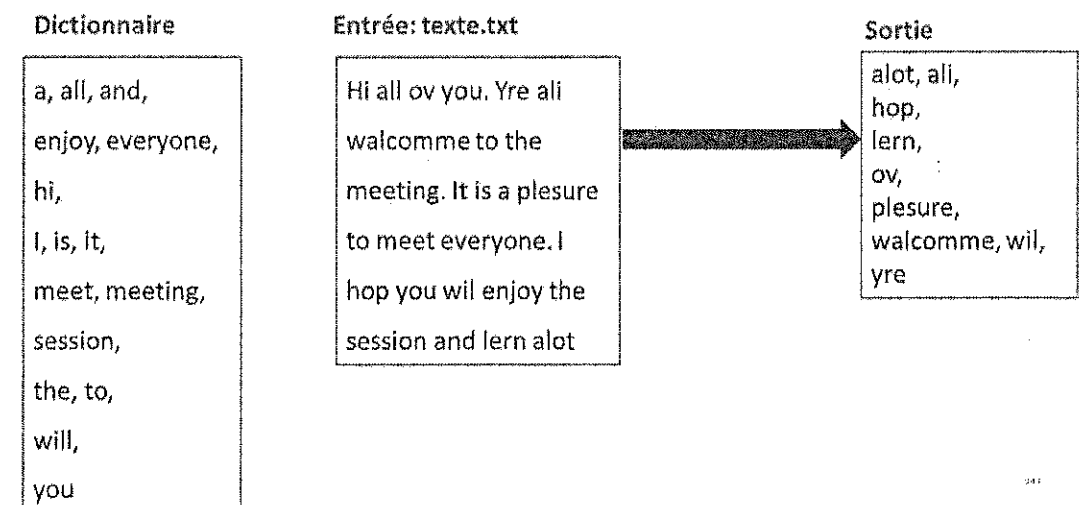
9. Le taux de parallélisme est défini comme le ratio entre les tâches simultanées et le total de tâches. Un job MapReduce contient 20 tâches Map, et le cluster dispose de 5 nœuds, chacun pouvant exécuter 3 tâches simultanément. Quel est le taux de parallélisme pour ce job ?

10. Pour traiter 512 Go de données dans un cluster Hadoop avec une taille de bloc de 128 Mo et 10 slots par nœud, combien de tâches Map seront générées, et combien de nœuds sont nécessaires pour un parallélisme optimal ?

### Exercice 2 : (10 points)

L'objectif de cet exercice est de développer un programme utilisant Hadoop MapReduce pour traiter un ensemble de fichiers contenant des textes écrits en anglais. Le but est d'extraire tous les mots qui ne figurent pas dans un dictionnaire de référence de la langue anglaise et de créer un nouveau dictionnaire, trié par ordre alphabétique, contenant uniquement les mots extraits.

**Exemple :**



[illegible]



### Exercice 1 {11 pts}

A l'exécution, les commandes Shell suivantes affichent des erreurs. Justifier l'origine de l'erreur et corriger la commande (Les commandes ne doivent pas être lancées par l'utilisateur root):

1- {1pt} `$ unshare -n sh`  
**unshare: unshare failed: Operation not permitted**

2- {1pt} `$ unshare -fUr sh`  
`# hostname host2`  
**hostname: you must be root to change the host name**

3- {1pt} `$ unshare -Umfr sh`  
`# ps -ef`  

| UID    | PID | PPID | C | STIME | TTY | TIME     | CMD        |
|--------|-----|------|---|-------|-----|----------|------------|
| nobody | 1   | 0    | 1 | 05:27 | ?   | 00:00:04 | /sbin/init |

  
.....

4- {1,5pt} `$ unshare -umUr -p sh`  
`# ls`  
`# ls`  
**sh: 2: Cannot fork**  
`# pwd`  
`/home/ubuntu`

5- {1pt} `$ unshare -Ur sh`  
`# mkdir test`  
`# mount /dev/sda1 test`  
**mount: /home/ubuntu/test: permission denied.**

6- {1pt} `$ unshare -mipunUrf chroot rootfs /bin/bash`  
`bash-5.1# ls`  
**bash: ls: command not found**

8- {1pt} `$ runc run cont`  
**ERRO[0000] runc run failed: JSON specification file config.json not found**

7- {1,5pt} 

```
$ docker container run alpine sh
$ docker container ls -a
CONTAINER ID   IMAGE     COMMAND   CREATED   STATUS    PORTS   NAMES
db982375400e   alpine   "sh"      3 seconds ago   Exited (0) 2 seconds ago   recursing_rubin
```

- Peut-on redémarrer correctement le conteneur ? Pourquoi ?

9- {1pt} 

```
$ ip a
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d6:ac:63 brd ff:ff:ff:ff:ff:ff
    inet 192.168.250.10/24 brd 192.168.250.255 scope global enp0s8
$ docker container run --rm -d nginx:alpine
$ curl 192.168.250.10
curl: (7) Failed to connect to 192.168.250.10 port 80 after 0 ms: Connection refused
```

10- {1pt} 

```
$ docker container run curlimages/curl curl --silent https://google.com/ |
> docker container run alpine grep '<TITLE>'
write /dev/stdout: broken pipe
```

## Exercice 2 {9 pts}

- 1) Comment peut-on lancer une commande cmd1 qui partage avec un processus P2 ces NameSpaces ? {1 pt}
- 2) Décrire le contenu d'une image OCI, les fichiers de configuration qu'elle contient et les liens entre eux. {2 pts}
- 3) Quel est le rôle de l'option -P dans la commande docker container run ? Comment elle peut déterminer les ports d'écoute d'un conteneur ? {1 pt}
- 4) On dispose d'un répertoire src sous le répertoire courant contenant un fichier main.c implémentant la fonction main() d'un projet de développement en C.
  - a) Donner le fichier Dockerfile d'une image Docker permettant l'exécution de l'application dans un conteneur. {2 pts}
  - b) Comment peut-on construire l'image et lancer le conteneur. {1 pt}
  - c) Comment peut-on afficher le Image-Spec de l'image et le Run-Spec du conteneur lancé. {1 pt}
  - d) Si on modifie le code de l'application. Décrire les étapes réalisées par le serveur Docker pour reconstruire l'image ? {1 pt}





**Devoir Surveillé – S1 – 2024/2025**

|                                      |                                          |                   |                                 |
|--------------------------------------|------------------------------------------|-------------------|---------------------------------|
| Filière : 2 <sup>ème</sup> Ing. Inf. | Matière :<br>Systèmes répartis           |                   | Enseignant :<br>Malek BEN SALEM |
| Date : 21 / 11 / 2024                | Nbr de Crédits : 3                       | Coefficient : 1,5 | Documents autorisés : Non       |
| Durée de l'examen : 1h               | Régime d'évaluation : Mixte              |                   | Nombre de pages : 02            |
|                                      | EX (50%) + DS (20%) + TP (25%) + OR (5%) |                   |                                 |

**Exercice 1 (4 points):**

Répondre en mentionnant le numéro de la question suivi par **la ou les lettres correspondantes** à la ou les bonnes réponses.

- À quoi sert la classe MulticastSocket en Java ?
  - À envoyer des messages à un seul destinataire.
  - À recevoir des messages diffusés en unicast.
  - À envoyer et recevoir des messages au sein d'un groupe multicast.
- Quel est le rôle de la méthode joinGroup(InetAddress group) dans MulticastSocket ?
  - Elle envoie un message au groupe multicast spécifié.
  - Elle permet à une instance MulticastSocket de rejoindre un groupe multicast afin de recevoir les messages envoyés à ce groupe.
  - Elle envoie une demande de connexion à un autre socket.
- Dans une communication via UDP, que représente un DatagramPacket ?
  - Une connexion persistante entre le client et le serveur.
  - Une unité de données unique, avec les informations d'adresse et de contenu, envoyée ou reçue sans connexion.
  - Un canal pour transmettre plusieurs paquets en même temps.
- Dans une application Java utilisant TCP, quel objet le serveur utilise-t-il pour écouter les connexions entrantes ?
  - DatagramServerSocket
  - Socket
  - ServerSocket

5. Quelle est la principale différence entre un socket TCP et un socket UDP ?

- a) TCP est orienté connexion, tandis que UDP est sans connexion.
- b) UDP est plus fiable que TCP.
- c) TCP est plus rapide que UDP.

### **Exercice 2 (4 points)**

1. Dans une application utilisant RPC comme intermédiaire, est-il suffisant de générer un seul souche client pour tous les services ou bien on doit générer un souche client pour chaque service (procédure) ?
2. Quelles sont les différences entre les deux intermédiaires RPC et RMI ?

### **Exercice 3 (12 points)**

Un cabinet vétérinaire souhaite développer une application client-serveur en Java pour gérer les rendez-vous des clients (propriétaires d'animaux) via une communication par sockets TCP, selon cette spécification :

- Le serveur doit répondre aux requêtes du client pour consulter les informations d'un animal en fonction de son ID. Si l'animal est trouvé, le serveur renvoie ses informations. Sinon, il renvoie un message indiquant que l'animal est introuvable.
- Le serveur doit répondre aux requêtes du client pour réserver un rendez-vous pour un animal en fonction de son ID. Le client envoie une demande de prise de rendez-vous avec le nom de l'animal, la date, l'heure, et le motif (la raison ou au type de service pour lequel le rendez-vous est pris). Si l'animal est trouvé, le serveur enregistre le rendez-vous et renvoie une confirmation avec les détails de la réservation. Sinon le serveur renvoie un message indiquant que l'animal est introuvable et que le rendez-vous n'a pas pu être pris.

**Remarque :** Dans cet exercice, vous n'êtes pas censé développer la gestion des dates, la vérification des disponibilités dans le calendrier, et la validation des formats de date/heure qui seront prises en charge par un autre service.

Le serveur stocke une liste d'animaux avec les informations suivantes : **ID** de l'animal, **Nom** de l'animal, **Espèce** (ex. : chat, chien, lapin), **Age** de l'animal, et **Nom du propriétaire**

**Implémenter cette application** en permettant au serveur de servir plusieurs clients d'une **manière parallèle** en utilisant les sockets TCP ;

1. Implémenter le programme du serveur (classe Serveur + classe Service) qui doit être installé sur la machine de l'adresse **Cabinets.PetsLover.tn** sachant que le service de noms doit être activé sur le port numéro **9753**.
2. Implémenter le programme du Client



Examen Principal– S1 – 2024/2025

|                                    |                                    |                            |
|------------------------------------|------------------------------------|----------------------------|
| Classe : 2 <sup>ème</sup> Ing Info | Matière :<br>Sécurité Informatique | Enseignant :<br>Zied Jaoua |
| Date : 15 / 1 / 2025               | Documents autorisés : Non          |                            |
| Durée de l'examen : 1h30           | Nombre de pages : 02               |                            |

Exercice 1 :

- 1- Dans les modèles d'accès quelles sont les différences principales entre le modèle de Biba et celui de Bell-Lapadula ?
- 2- Quelles sont les avantages des Coupe-feu dynamiques par rapport à ceux qui sont statiques ?
- 3- Donner deux approches pour la détection de comportements suspects et quels sont les problèmes des Intrusion Detection Systems ?
- 4- Schématisez les échanges de clés SSL (grosso modo) et indiquez le type de données contenus dans les messages

Exercice 2: Étude d'un schéma de MAC basé sur le mode de chiffrement CFB

On considère un chiffrement par bloc  $E: \{0,1\}^{64} \times \{0,1\}^{64} \rightarrow \{0,1\}^{64}$  où  $E_k(x) = E(k, x)$

désigne le chiffrement du texte clair  $x$  sous la clé  $k$ . Le MAC CFB d'un message donné

$m \in \{0,1\}^*$  avec la clé  $k$  est obtenu en chiffrant  $m$  avec  $E_k$  en utilisant le mode de

chiffrement CFB, puis en combinant les blocs de sortie par un XOR. Plus précisément, pour un

message  $m = x_1 || x_2 || \dots || x_n$  on a :

$CFB-MAC_k(m) = y_1 \oplus y_2 \oplus \dots \oplus y_n$ , où  $y_i = E_k(y_{i-1} \oplus x_i)$  pour  $i = 2, \dots, n$  et  $y_1 = E_k(IV) \oplus x_1$ ,  $IV$  étant un vecteur d'initialisation constant et connu. Pour simplifier, on suppose que tous les messages ont une longueur multiple de 64 bits. Dans toutes les questions, on suppose que  $IV$  est constant et connu.

(a) Supposons que nous ayons accès à un oracle  $O$  qui calcule le MAC CFB sous une clé secrète  $k$  et un  $IV$  connu. Montrez que vous pouvez retrouver  $E_k(IV)$  en effectuant une seule requête à l'oracle.

(b) Étant donné un message  $m$  de  $n$  blocs et  $h = \text{CFB-MAC}_k(m)$ , montrez comment il est possible de générer un nouveau message  $m'$  de  $n$  blocs et un  $h' \in \{0,1\}^{64}$  tel que  $m' \neq m$  et  $\text{CFB-MAC}_k(m') = h'$ .

(c) Supposons que nous disposons de  $IV$ ,  $E_k(IV)$  et  $h \in \{0,1\}^{64}$ . Montrez comment il est possible de générer un message  $m$  de deux blocs, tel que  $\text{CFB-MAC}_k(m) = h$ .

(d) Peut-on étendre l'attaque de la question précédente à des messages  $m$  de plus de deux blocs ?

### Exercice 3

Le protocole HTTPS (HTTP sur SSL/TLS) est couramment utilisé pour sécuriser les communications entre un serveur web et un navigateur. Pour cela, une session HTTPS s'appuie sur un certificat diffusé par le serveur permettant d'effectuer une session d'authentification initiale et ensuite un chiffrement du canal de communication dans lequel transite l'échange HTTP.

1. Lors de l'authentification, le protocole utilise une clef publique contenu dans un certificat que le serveur détient et diffuse au client à l'établissement de la connexion.

Quelles sont les protections offertes par cette utilisation d'un certificat serveur ?

2. Comment l'utilisateur du navigateur peut-il être assuré que cette clef publique correspond bien à l'organisme auquel il souhaite accéder ?

3. Pourquoi de nombreux services web, utilisant pourtant HTTPS, demandent-ils en plus à l'utilisateur de fournir un nom de compte et un mot de passe pour compléter l'ouverture de session ?

4. Il est possible d'utiliser un certificat client stocké sur le navigateur pour l'échange HTTPS.

Quel est l'effet de l'utilisation d'un certificat client sur la protection de l'ensemble du service ?

5. Avec un certificat client, l'utilisateur doit quand même parfois fournir une passphrase : de quel mot de passe s'agit-il ?

6. Pensez-vous qu'il y ait une « passphrase » utilisateur sur la partie privée du certificat serveur ? Pourquoi ?

### Exercice 4

Carl M. Ellison et Bruce Schneier ont écrit un article « Tout ce que l'on ne vous dit pas au sujet des PKI ». Dans cet article, ils présentent 10 risques liés à l'utilisation des PKI. Commenter les quatre risques suivants :

1. Risque n1 : « Who do we trust, and for what ? » (A qui faisons-nous confiance et pour quoi ?). Plus précisément, la question est de savoir qui a donné à un CA l'autorité de signer des certificats et quelle est la notion de confiance. Commenter pour les scénarios : PKI au sein d'une seule entreprise ; PKI entre une entreprise et ses clients/filiales ; PKI gérée par une entreprise spécialisée (VeriSign, RSA Security, etc.) pour une entreprise tierce.

2. Risque n2 : « Who is using my key ? » (Qui utilise ma clef). Plus précisément, comment protéger les clefs secrètes ?

3. Risque n4 : « Which John Robinson is he ? » (Quel Jean Martin est-ce ?). Plus précisément, comment traiter les différents Jean Martin connus par un CA ?


4. Risque n9 : « How secure are the certificate practices ? » (Quelle est la sécurité des pratiques de certification ?). Par exemple :

(a) Sur quels critères établir des durées de validité de clefs ?

(b) Comment établir les longueurs de clefs, de hachage ?

(c) Faut-il faire des CRL (certificate revocation list) ?

(d) Plus généralement comment savoir quelles sont les pratiques de certification d'une autorité ?

|                                                                                   |                                                                                                                                                                              |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p style="text-align: center;"><b>Université de Monastir</b></p> <p style="text-align: center;"><b>Institut Supérieur d'Informatique et de Mathématiques de Monastir</b></p> |
| 2024/2025                                                                         | Epreuve : <b>Culture d'entreprise</b>                                                                                                                                        |

|                                    |            |              |                             |
|------------------------------------|------------|--------------|-----------------------------|
| Enseignant : BRAHEM TAOUFIK        | Durée : 1H | Nb Pages : 1 | Filière : <b>ING 2-Info</b> |
| <b>Examen session janvier 2025</b> |            |              |                             |

### Exercice n°1

- 1) Donner la définition aux termes suivants :
  - a) Prix
  - b) Entreprise
- 2) Quels sont les critères de segmentation d'un marché ?
- 3) Quelles sont les différentes formes juridiques des sociétés?

### Exercice n°2

Pour analyser la rentabilité économique, la société "Info-Tech" vous fournit les informations ci-dessous relatives à l'activité de l'année 2024 pour les solutions GRH et comptabilité

| Eléments                    | GRH     | Comptabilité |
|-----------------------------|---------|--------------|
| <b>Chiffre d'affaires</b>   | 217 500 | 1 340 000    |
| <b>Coût de production</b>   |         |              |
| - charges variables         | 116 250 | 628 000      |
| - charges fixes             | 45 000  | 240 000      |
| <b>Coût de distribution</b> |         |              |
| - charges variables         | 6 000   | 40 000       |
| - charges fixes             | 3 000   | 20 000       |

L'objectif fixé par la société "Info-Tech" est de réaliser un **taux de rentabilité au minimum de 25 % sur GRH et de 30 % sur comptabilité.**

### Travail à faire:

- 1) Pour chaque produit :
  - a) Calculer le coût variable total et le coût fixe
  - b) Présenter le tableau de résultat différentiel
  - c) La société a-t-elle atteint son objectif en termes de rentabilité? justifiez
  - d) Calculer le seuil de rentabilité en valeur
  - e) Déterminer la date à laquelle sera atteint le SR (la société travail 12 mois / 12)
- 2) Présenter sur le même graphique le deux SR et localiser les zones de perte et de bénéfices





**DS2**  
**Session janvier 2025**  
**ENSEIGNTE : M AWATEF GUIDARA**

|                  |                                                  |
|------------------|--------------------------------------------------|
| <b>EPREUVE :</b> | <b>Droit des données et éthiques d'ingénieur</b> |
| <b>Niveau :</b>  | <b>2<sup>ème</sup> année ING2 GL-TD1-TD2</b>     |

**Partiel 1 : QCM (10 points).**

Cocher la ou les bonnes réponses :

\*Le traitement des données personnelles doit se faire dans le cadre :

- 1- du respect de la vie privée
- 2- du respect de la dignité humaine
- 3- de la transparence et la loyauté.

\*la loi n° 63-2024 du 27 juillet 2004 portant sur la protection des données à caractère personnel est une loi :

- 1- organique
- 2- ordinaire

\*la déclaration préalable doit être effectuée par seulement :

- 1- le traitant
- 2- le sous traitant

\*La personne responsable du traitement peut être :

- 1- une personne physique
- 2- une association
- 3- une personne morale

\*la déclaration préalable du traitant des données personnelles est une condition :

- 1- facultative
- 2- obligatoire

\*Le traitant des données personnelles doit être :

- 1- un Tunisien résident en Tunisie
- 2- un Tunisien résident ou non résident en Tunisie

\*Le silence de l'instance concernant la demande d'une autorisation préalable vaut :

- 1- acceptation
- 2- refus

## المعهد العالي للإعلامية والرياضيات بالمنستير

\*la violation des dispositions de la loi n° 63-2024 du 27juillet 2004 portant sur la protection des données à caractère personnel engendre une :

- 1-responsabilité pénale
- 2-responsabilité civile
- 3- responsabilité morale

\*en cas de décès du responsable du traitement, les héritiers doivent informer l'instance dans un délai ne dépassant pas :

- 1- un mois à compter de la date de survenance du fait
- 2-trois mois à compter de la date de survenance du fait

\*le consentement de la personne dont ses données personnelles font l'objet d'un traitement doit être :

- 1- explicite
- 2-implicite
- 2-écrit

\* le traitement des données personnelles qui concerne un enfant ne peut s'effectuer qu'après l'obtention du consentement de :

- 1- son tuteur seulement
- 2- son tuteur et le juge des enfants
- 3- son tuteur et le juge de la famille.

\*en cas de faillite de la personne morale responsable du traitement, l'instance sera informé par :

- 1- les héritiers
- 2- le syndic de la faillite
- 3- le liquidateur

### **Partie2 : Questions : (10 points).**

- 1- Quels sont les droits de la personne dont ses données personnelles font l'objet d'un traitement ? (5points).
- 2- Qu'est ce que l'instance nationale de protection des données à caractère personnel ? (5 points).

### Exercice 1 : {11 pts}

- 1) Lors de la création d'une image Docker, nous cherchons à réduire le nombre d'instructions RUN. Pourquoi ? {1 pt}
- 2) Donner un exemple de conteneur où on doit mettre en place un système de persistance des données. Comment et pourquoi ? {1 pt}
- 3) Comment peut-on établir une communication entre :
  - a) L'hôte Docker et un conteneur. {0,5 pt}
  - b) Deux conteneurs. {0,5 pt}
- 4) Comment forcer plusieurs conteneurs fonctionnant sur une seule machine de partager les mêmes ressources (CPU, RAM, etc) {0,5 pt}
- 5) Quel est l'utilité d'un cluster Docker? Comment peut-on créer un cluster Docker? {1 pt}
- 6) On considère le fichier de déploiement deploy.yml suivant :

```
version: '3'

services:
  MysqlService:
    image: mysql
    deploy:
      replicas: 3
  WebService:
    image: repoweb/webapp
    deploy:
      replicas: 3
    ports:
      - 80:8081
```

- 7) Comment peut-on déployer les deux services Mysql et Web ? Pourquoi ? {1 pt}
- 8) Les instances de MysqlService et WebService peuvent-ils se connecter à un service installé à l'extérieur du cluster ? Pourquoi ? {1 pt}
- 9) Les instances WebService peuvent-ils communiquer avec les instances MysqlService? Comment ? {1 pt}

- 10) De l'extérieur, peut-on accéder au MysqlService et WebService? **{0,5 pt}**
- 11) On s'intéresse au service WebService, expliquer comment un utilisateur peut accéder à ce service ? comment le partage de charge est réalisé sur les différentes instances ? (Utiliser une figure) **{2 pts}**
- 12) Si on déploie un autre service public dans le cluster, comment le load balancer distingue entre les flux de deux services ? **{1 pt}**

## **Exercice 2 : {9 pts}**

- 1) La technologie VXLAN peut-elle étendre un réseau IPv6 ? pourquoi ? **{0,5 pt}**
- 2) Comment EVPN améliore la gestion des réseaux VXLAN traditionnelle ? **{1 pt}**
- 3) Avec les VXLAN-EVPN peut-on avoir une découverte automatique des VTEPs ? Comment ? **{1 pt}**

On considère 3 VTEPs installés dans trois sites physiques et connectés à Internet :

- VTEP1 qui étend le VXLAN 100. Dans le site1, on dispose d'une machine M1 appartenant au VXLAN100 et possédant la MAC 00-00-00-00-00-01 et l'IP 10.0.0.1/24
  - VTEP2 qui étend le VXLAN 100. Dans le site2, on dispose d'une machine M2 appartenant au VXLAN100 et possédant la MAC 00-00-00-00-00-02 et l'IP 10.0.0.2/24
  - VTEP3 qui étend deux VXLANs : le VXLAN 100 et le VXLAN 200. Dans le site3, on dispose de deux machines :
    - Une machine M3 appartenant au VXLAN100 et possédant la MAC 00-00-00-00-00-03 et l'IP 10.0.0.3/24
    - Une machine M4 appartenant au VXLAN200 et possédant la MAC 00-00-00-00-00-04 et l'IP 192.168.0.4/24
- 4) On utilise les VXLAN unicast, donner les forwarding databases initiales. **{0,5 pt}**
  - 5) Une communication se produit entre M1 et M2. Donner alors les nouvelles forwarding databases. **{1 pt}**
  - 6) M1 peut-elle communiquer avec M4 ? M3 peut-elle communiquer avec M4 ? Pourquoi ? **{1 pt}**
  - 7) Comment pour connecter M1 avec M4 avec un routage asymétrique ? **{1 pt}**
  - 8) Peut-on connecter M1 avec M4 avec un routage symétrique ? Comment ? **{1,5 pt}**
  - 9) Si on utilise les VXLAN-EVPN, donner les forwarding databases initiales et après une communication se produit entre M1 et M2 . **{1,5 pt}**



**Examen – S1 – 2024/2025**

|                                            |                                          |                   |                                         |
|--------------------------------------------|------------------------------------------|-------------------|-----------------------------------------|
| <b>Filière : 2<sup>ème</sup> Ing. Inf.</b> | <b>Matière :<br/>Systèmes répartis</b>   |                   | <b>Enseignant :<br/>Malek BEN SALEM</b> |
| <b>Date : 10/ 01 / 2025</b>                | Nbr de Crédits : 3                       | Coefficient : 1.5 | <b>Documents autorisés : Non</b>        |
| <b>Durée de l'examen : 1h30</b>            | <b>Régime d'évaluation : Mixte</b>       |                   | <b>Nombre de pages : 1</b>              |
|                                            | EX (50%) + DS (20%) + TP (25%) + OR (5%) |                   |                                         |

**Exercice 1 (8 points) :**

1. Quelles sont les étapes de développement d'une application répartis avec CORBA ?
2. Quelles sont les étapes de lancement d'une application répartie avec RMI ?
3. Quelle est la différence entre MOM, CORBA et RMI ?
4. Donner les étapes de développement d'une application répartie avec un MOM Java.

**Exercice 2 (6 points) :**

En utilisant le middleware RMI, on souhaite développer une application répartie qui permet de calculer le montant TTC (Tout Taxe Comprise) d'une commande à partir d'un montant et d'un taux de TVA (Taxe sur la Valeur Ajoutée) ;

```
double calculMontantTTC (double montant, double taux_tva)  
return montant * taux_tva;
```

1. Afin de rendre cette méthode accessible à distance, définir l'interface **CalculTVA** entre le client et le serveur.
2. Définir la classe **CalculTVAImpl** qui matérialise les opérations de **CalculTVA**.
3. Donner le programme du serveur **Serveur.java** qui doit être installé sur la machine de l'adresse **services.calcul** sachant que le service de noms est activé sur le port numéro **1357**.
4. Donner le programme du client **Client.java** en essayant d'invoquer toutes les méthodes de services de calcul de TVA.

**Exercice 3 (6 points) :**


En utilisant l'architecture CORBA, on souhaite développer la même application répartie proposée dans l'exercice 2.

1. Proposez la spécification CORBA IDL.
2. Donner l'instruction permettant de compiler cette spécification en Java tout en citant les noms des fichiers générés.
3. Proposez une implémentation du servant.
4. Décrire textuellement et brièvement le scénario du programme Serveur ainsi que celui du programme Client.

Bon travail.





|                                                                                   |                                                                                                               |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
|  | <b>Université de Monastir</b><br><br><b>Institut Supérieur d'Informatique et de Mathématiques de Monastir</b> |
| 2024/2025                                                                         | Epreuve : <b>Culture d'entreprise</b>                                                                         |

|                                    |            |              |                             |
|------------------------------------|------------|--------------|-----------------------------|
| Enseignant : BRAHEM TAOUFIK        | Durée : 1H | Nb Pages : 1 | Filière : <b>ING 2-Info</b> |
| <b>Examen session janvier 2025</b> |            |              |                             |

### Exercice n°1

- 1) Donner la définition aux termes suivants :
  - a) Prix
  - b) Entreprise
- 2) Quels sont les critères de segmentation d'un marché ?
- 3) Quelles sont les différentes formes juridiques des sociétés?

### Exercice n°2

Pour analyser la rentabilité économique, la société "Info-Tech" vous fournit les informations ci-dessous relatives à l'activité de l'année 2024 pour les solutions GRH et comptabilité

| Eléments                    | GRH     | Comptabilité |
|-----------------------------|---------|--------------|
| <b>Chiffre d'affaires</b>   | 217 500 | 1 340 000    |
| <b>Coût de production</b>   |         |              |
| - charges variables         | 116 250 | 628 000      |
| - charges fixes             | 45 000  | 240 000      |
| <b>Coût de distribution</b> |         |              |
| - charges variables         | 6 000   | 40 000       |
| - charges fixes             | 3 000   | 20 000       |

L'objectif fixé par la société "Info-Tech" est de réaliser un taux de rentabilité au minimum de 25 % sur GRH et de 30 % sur comptabilité.

### Travail à faire:

- 1) Pour chaque produit
  - a) Calculer le coût variable total et le coût fixe
  - b) Présenter le tableau de résultat différentiel
  - c) La société a-t-elle atteint son objectif en termes de rentabilité? justifiez
  - d) Calculer le seuil de rentabilité en valeur
  - e) Déterminer la date à laquelle sera atteint le SR (la société travail 12 mois / 12)
- 2) Présenter sur le même graphique le deux SR et localiser les zones de perte et de bénéfices

