

INSTITUT SUPÉRIEUR D'INFORMATIQUE ISI الجامعة العليا للعلوم	Ministère de l'enseignement supérieur et de la recherche scientifique ****	
Classe : CS 3	Institut Supérieur d'Informatique <i>Examen - Session principale</i> <i>Architecture Orientée services</i> *****	Durée : 1h30 Documents et calculatrices non autorisés

Exercice 1 :

On désire créer une encyclopédie de personnes Tunisiennes dans le domaine scientifique. Chaque personne possède un nom, un prénom et au moins une publication. Une personne peut aussi être caractérisée par son pays et son genre : homme ou femme. Une publication est soit dans un journal soit dans une conférence. Dans les deux cas, elle possède un titre.

Rédiger une DTD adaptée à cette description.

Exercice 2 :

Soit le document WSDL suivant :

```

1 <?xml version="1.0"?>
2 <definitions name="contacts"
3   targetNamespace="http://example.com/contacts.wsdl"
4   xmlns:tns="http://example.com/contacts.wsdl"
5   xmlns:types="http://example.com/contacts.xsd"
6   xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
7   xmlns="http://schemas.xmlsoap.org/wsdl/">
8
9   <types>
10  <xsd:schema targetNamespace="http://example.com/contacts.xsd"
11    xmlns:xsd="http://www.w3.org/2001/XMLSchema">
12    <xsd:element name="contact">
13      <xsd:complexType>
14        <xsd:sequence>
15          <xsd:element name="id" type="xsd:integer" minOccurs="0"/>
16          <xsd:element name="first_name" type="xsd:string"/>
17          <xsd:element name="last_name" type="xsd:string"/>
18          <xsd:element name="projects" type="xsd:string"
19            minOccurs="0" maxOccurs="unbounded"/>
20        </xsd:sequence>
21      </xsd:complexType>
22    </xsd:element>
```

```

23   <xsd:element name="id">
24     <xsd:complexType>
25       <xsd:sequence>
26         <xsd:element name="id" type="xsd:integer"/>
27       </xsd:sequence>
28     </xsd:complexType>
29   </xsd:element>
30 <xsd:element name="LocaleOptions">
31   <xsd:complexType>
32     <xsd:sequence>
33       <xsd:element name="language" type="xsd:string" minOccurs="0"/>
34       <xsd:element name="localizeErrors" type="xsd:boolean" minOccurs="0"/>
35     </xsd:sequence>
36   </xsd:complexType>
37   </xsd:element>
38   <xsd:element name="DebuggingHeader">
39     <xsd:complexType>
40       <xsd:sequence>
41         <xsd:element name="debugLevel" type="xsd:integer"/>
42       </xsd:sequence>
43     </xsd:complexType>
44   </xsd:element>
45 </xsd:schema>
46 </types>
47
48 <message name="store">
49   <part name="body" element="████:id"/>
50 </message>
51
52 <message name="store_response">
53   <part name="body" element="████:id"/>
54 </message>
55
56 <message name="retrieve">
57   <part name="body" element="████:id"/>
58 </message>
59
60 <message name="retrieve_response">
61   <part name="body" element="████:contact"/>
62 </message>
63
64 <message name="Header">

```

```

65 <part element="xxx:DebuggingHeader" name="DebuggingHeader"/>
66 <part element="xxx:LocaleOptions" name="LocaleOptions"/>
67 </message>
68
69 <portType name="contacts_port_type">
70 <operation name="store">
71 <input message="yyy:store"/>
72 <output message="yyy:store_response"/>
73 </operation>
74 <operation name="retrieve">
75 <input message="yyy:retrieve"/>
76 <output message="yyy:retrieve_response"/>
77 </operation>
78 </portType>
79
80 <binding name="contacts_binding" type="tns:contacts_port_type">
81 <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
82 <operation name="store">
83 <soap:operation soapAction="store"/>
84 <input>
85 <soap:header use="literal" message="tns:Header" part="LocaleOptions"/>
86 <soap:header use="literal" message="tns:Header" part="DebuggingHeader"/>
87 <soap:body use="literal"/>
88 </input>
89 <output>
90 <soap:body use="literal"/>
91 </output>
92 </operation>
93 <operation name="retrieve">
94 <soap:operation soapAction="retrieve"/>
95 <input>
96 <soap:body use="Literal"/>
97 </input>
98 <output>
99 <soap:body use="Literal"/>
100 </output>
101 </operation>
102 </binding>
103
104 <service name="contacts_service">
105 <port name="contacts_port" binding="tns:contacts_binding">
106 <soap:address location="http://localhost:8080"/>

```

107 </ports>
108 </service>
109

110 </definitions>

- ✓ 1. Une partie du fichier a été remplacée par XXX et YYY. Que désignent-ils ? Justifier
- ✓ 2. Tous les fils directs de l'élément « definitions » dans un fichier WSDL sont obligatoires. A l'exception d'un seul élément. Citer le et expliquer dans quels cas peut-on l'omettre.
- ✓ 3. Citer les messages échangés entre le client et le service (spécifier le sens de l'échange et l'ordre de transmission de message). Justifier
- ✓ 4. Soit le message incomplet suivant envoyé :

```
<?s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
<s:Body>
<?som:contact xmlns:son="http://example.com/contacts.xsd">
<?s:contact>.....</s:contact>
</s:Body>
</s:Envelope>
```

- ✓ a) Quel standard est-il utilisé pour formuler ce message ? Expliquer
- ✓ b) S'agit-il d'un message d'entrée ou de sortie ? Justifier
- ✓ c) Chaque message porte un nom, comment s'appelle ce message ?
- ✓ d) Compléter les points de suspension par un exemple de message.

- ✓ 5. a) Est-ce que les messages SOAP représentent l'unique moyen pour échanger des données entre services Web ? Justifier votre réponse.
- ✓ b) Où est ce que cette information est indiquée par le fournisseur de service ?

- ✓ 6. Le service est considéré comme une boîte noire. Comment les consommateurs de service peuvent interagir avec ?

Exercice 3:

Soit un service Web RESTful qui gère les employés d'une entreprise. Il met à la disposition

- des client la ressource « /employees » qui contient la liste des employés.
1. Donner deux différences entre les services Web de type REST et ceux de type WS-* (qui reposent sur SOAP).
 - ✓ 2. Expliquer la différence entre le verbe « POST » et le verbe « PUT »
 - ✓ 3. Un client désire consulter la liste des employés.
Donner la requête HTTP correspondante.
 - ✓ 4. Le client désire consulter l'employé « 21 ».
Donner la requête HTTP correspondante.

✓ 4. Donner deux triplets :

INSTITUT SUPÉRIEUR INFORMATIQUE الجامعة العليا للإنformatique	Ministère de l'enseignement supérieur et de la recherche scientifique ****	
Classe : CS 3	Institut Supérieur d'informatique	Durée : 1h30
Date : 06 janvier 2023	Examen - Session principale Web Sémantique et Web de Données *****	Documents et calculatrices non autorisés
Nbre pages : 2		

Exercice 1:

On désire construire une ontologie légère en RDFS qui décrit la structure d'une entreprise.

Cette ontologie organisera les notions suivantes :

- A. Les Documents dans l'entreprise : les documents publics (PublicDoc), tous les types de rapports (Report) et les documents internes et privés (InternalDoc). On trouve aussi les rapports secrets (SecretReport), les mémos ou notes internes (InternalMemo), les communiqués de presse (PressRelease) et les rapports d'activité annuels (AnnualReport),

- B. L'ensemble des Agents qui se divise en l'ensemble des personnes (Person) et l'ensemble des groupes (Group).

- C. Des propriétés pour les documents : un titre (hasTitle), un auteur (hasAuthor) et des liens de citations (makesReferenceTo)

- D. Des propriétés pour les agents : un nom (hasName), l'appartenance d'une personne à un groupe (isMemberOf)

Travail à faire :

1. Représenter l'ontologie sous forme de graphe
2. Représenter les blocs B, C et D de la description en Turtle (la représentation des triplets du bloc A n'est pas demandée).

3. Soit les triplets suivants :

```
(F, rdf:type, Person)
(F, hasName, "Fares")
(W, isMemberOf, CS)
(W, hasName, "Wassim")
(doc.html, hasTitle, "Web Sem")
(doc.html, hasAuthor, W)
```

En utilisant toute l'ontologie et les triplets ci-dessus :

- a. Donner deux inférences possibles en spécifiant à chaque fois la règle utilisée (deux règles différentes)

- b. Formuler en SPARQL les requêtes suivantes et donner le résultat à chaque fois :
- Donner toutes les informations relatives à doc.html
 - Donner un seul membre de groupe dont le nom est soit Fares soit Mohamed
 - Relier par la relation « auteur » les titres des documents aux noms des auteurs.

NB : rdfs: <http://www.w3.org/2000/01/rdf-schema#>
rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>

Exercice 2:

On désire construire l'ontologie de la famille. On utilisera les classes suivantes : Personne, Homme, Femme, Parent, Pere, Mere. Une personne possède un nom (on suppose qu'il s'agit d'une relation fonctionnelle) et chaque personne possède exactement une mère et un père. Les parents de Wednesday sont Morticia et Gomez.

Travail à faire :

1. Selon la méthode SAMOD pour la construction d'ontologies, il existe deux types d'acteurs. Citer les et expliquer pourquoi nous avons besoin de ces deux acteurs différents.
2. Donner deux insuffisances de RDFS que OWL permet de résoudre
3. Donner les composants de l'ontologie
4. Représenter les classes et les relations de l'ontologie sous forme de graphe
5. Donner en OWL (langage RDF/XML) l'ontologie représentant les données ci-dessus.
6. Soit les règles SWRL suivantes :
Homme(?m) → A(?m)

Mere(?m) → B(?m)

(hasChild >= 1)(?x) ^ Femme (?x) → C(?x)

Mere(?x) ^ Pere (?x) → D

E → Femme (Wednesday)

Donner les valeurs de A, B, C, D et E

NB : OWL : <http://www.w3.org/2002/07/owl>

- Cet exercice se focalise sur la partie xml et il vous est uniquement demandé de dessiner l'interface qui correspond au fichier activity_main.xml suivant et le fichier strings.xml :

```
activity_main.xml

<LinearLayout
    android:layout_width="409dp"
    android:layout_height="729dp"
    android:orientation="vertical"
    android:layout_width="match_parent"
    android:layout_height="wrap_content"
    android:orientation="horizontal">

    <TextView
        android:id="@+id/A"
        android:layout_width="wrap_content"
        android:layout_height="wrap_content"
        android:textSize="36sp" />

    <Textview
        android:id="@+id/B"
        android:layout_width="wrap_content"
        android:layout_height="wrap_content"
        android:layout_weight="1"
        android:textSize="36sp" />

    <Textview
        android:id="@+id/C"
        android:layout_width="wrap_content"
        android:layout_height="wrap_content"
        android:layout_weight="1"
        android:textSize="36sp" />

    <Textview
        android:id="@+id/D"
        android:layout_width="wrap_content"
        android:layout_height="wrap_content"
        android:layout_weight="1"
        android:textSize="36sp" />

    <Imageview
        android:id="@+id/imageView"
        android:layout_width="50dp"
        android:layout_height="wrap_content"
        android:layout_weight="2"
        app:srcCompat="@mipmap/ic_launcher" />

<EditText
    android:id="@+id/Reponse" />
```

EXAMEN PRINCIPAL:

FRAMEWORK ET TECHNOLOGIE BIG DATA

Classe / Filière	: 3^{ème} CS
Documents	: Non autorisés
	le 6 janvier 2023 à 8h30

EXERCICE 1 : Sous PIG, (08pts)

✓1) Quelles sont les étapes d'un programme PIG ?

✓2) Proposez un programme qui permet de compte les mots d'un texte chargé de HDFS

3) Dans un tableau, expliquez comment ce programme respecte le paradigme

MapReduce en comparant les instructions PIG aux étapes Map, Shuffle et Reduce.

EXERCICE 2 : Sous Hive, (06pts)

✓1) Comment peut-on forcer Hive à travailler avec un fichier texte ?

✓2) Ecrire un script Hive pour le comptage de lettres de l'alphabet dans un texte chargé de HDFS. (utiliser la fonction SUBSTRING() pour extraire la lettre d'un mot).

QCM : (06pts)

Choisir une ou plusieurs réponse(s) correcte(s) : (Faire un tableau de réponse sur la copie de l'examen)

1) Le type de données Timestamp est reconnu par

- a) PIG
- b) MapReduce
- c) Hive



2) Seules les paunes des « Jobtracker » et « Child » sont tolérées :

- a) Vrai
- b) Faux

3) La commande 'pig -x mapreduce' implique une exécution des taches Map et Reduce

- a) Vrai
- b) Faux

4) Hive est un environnement pour la gestion et l'interrogation de données

- a) Structurées
- b) Semi Structurées
- c) Non Structurées
- d) En dataflow

5) Hive est un

- a) Entreposé de données,
- b) Langage d'interrogation de données NoSQL,
- c) Espace de stockage MétaStore de Hadoop.

6) Les types de données sous PIG sont :

- a. Partition
- b. Bucket
- c. Tuple
- d. Map

Année Universitaire 2022/2023

Examen Final

Enseignants : Bahroun Sahbi/Ezzeddine Zagrouba

Niveau d'Etude : 3^{ème} année CS
Matière : Machine learning
Nombre de pages : 2
NB : calculatrice autorisée

Semestre : 1
Date : Janvier 2023
Durée : 1H30

Exercice 1 : (7 points)

Soit le jeu de données suivant composé de 8 individus décrits par deux variables X et Y.

Individu	X	Y
1	1.5	1
2	1	0.5
3	5	4.5
4	2	2
5	4.5	6
6	7	4.5
7	5	6.5
8	4.5	3

- \(1)\) Donnez les étapes l'algorithme de la classification k moyennes
 \(\2)\) Appliquez avec k moyennes une classification des individus du tableau ci dessus en en deux classes en choisissant initialement comme centres les individus 1 et 6.
 NB : utilisez comme distance entre individus la distance Euclidienne.
 $d(A, B) = \sqrt{(x_b - x_a)^2 + (y_b - y_a)^2}$
- \(3)\) Quels sont les inconvénients de la classification k moyennes.

Exercice 2 : (6 points)

Soit le jeu de données suivant composé de 8 individus décrits par les 2 variables (Taille, couleur). La variable à prédire étant Class.

Individu	Taille	Couleur	Class
1	P	U	Pure
2	P	U	Pure
3	G	U	Pure
4	G	M	Pure
5	G	M	NPure
6	M	M	NPure
7	P	U	NPure
8	P	M	NPure

- ✓ 1) Calculez l'indice de Gini avant séparation
- ✓ 2) Calculez l'indice de Gini des variables explicatives
- ✓ 3) Construire l'arbre de décision
- ✓ 4) Prédire la variable maladie pour l'individu caractérisé par les valeurs suivantes
(M, P)
- 5) Quelle est la profondeur idéale de l'arbre

Exercice 3 : (7 points)

- ✓ 1) Est ce que les réseaux de neurones est un algorithme d'apprentissage supervisé ou non
 - ✓ 2) Est ce que les réseaux de neurones est un algorithme qui répond au problème de régression ou de classement?
 - 3) Décrire le neurone formel et ses différentes composantes
 - 4) Soit l'ensemble d'apprentissage suivant composé de données appartenant à R^2 et la variable à prédire y représenté sous la forme $((x_1, x_2), y)$:
 $\{((2,2),0); ((1,-1),1); ((-2,3),1); ((0,1),0)\}$
- On utilise une fonction d'activation à seuil $s=0$. On suppose qu'à l'initialisation, les poids ont été choisis : $w_0=0$; $w_1 = 0$ et $w_2 = 0$. On veut construire un modèle d'apprentissage à l'aide de l'algorithme du perceptron simple sur cet ensemble de données des données d'apprentissage. Utilisez $x_0=1$ et $\varepsilon=1$

Bon travail

INSTITUT ISI الجامعة الإسلامية	Ministère de l'enseignement supérieur et de la recherche scientifique ****	Institut Supérieur d'Informatique
Classe : 3CS Date : 02 janvier 2023 Nbre pages : 2	Examen - Session principale Intitulé de la matière Développement Mobile Chargé du cours : Walid Ksiaa	Durée : 1h30 Documents non autorisés

Barème : Ex1 (12) Ex2 (3) Ex3 (5)

NB: Ne pas répondre sur cette feuille. Répondez sur l'autre feuille.

Exercice 1 (QCM): Cochez la ou les bonnes réponses

NB: Une question avec une étoile (*) indique qu'il y a plusieurs réponses.

- 1) Les identificateurs dans R.java font référence à des fichiers se trouvant dans le répertoire :
- a) java
 - b) res
 - c) generated
 - d) libs
- 2) AVEC ANDROID STUDIO APRES AVOR COMPILER ET GENERER DES APPLICATION ON OBTIENT COMME RESULTAT LIVRABLE UN FICHIER DE TYPE (D'EXTENSION) :
- a) apk
 - b) ipk
 - c) exe
- [*] 3) Parmi les langages suivants, lesquels sont indispensables pour créer des applications natives en android ?
- a) Php
 - b) C/C++
 - c) Java
 - d) Kotlin
 - e) Javascript
 - f) Objective C
- [*] 4) Pour développer avec Android Studio confortablement, on doit utiliser :
- a) Un ordinateur puissant côté processeur et mémoire vive.
 - b) Une connexion internet permanente pour les mises à jour.
 - c) Une tablette Android puissante.
 - d) Un émulateur pour un système Android.
- 5) Android Studio :
- a) Est Le seul environnement de développement pour créer des applications pour Android.
 - b) Permet de créer des applications pour smartphones uniquement.
- 6) Le fichier strings.xml se trouve sous le répertoire:
- a) res
 - b) values
 - c) java

7) EditText est un :

- a) Widget
- b) Layout

8) Un Layout est un :

- a) Gabarit
- b) Un Conteneur de widget(s) et de layout(s)
- c) Un conteneur de layout seulement
- d) Un ViewGroup

9) Pour programmer un évènement de « click » sur un bouton, on peut indiquer le nom de la méthode respective dans les propriétés du bouton décrit dans le fichier xml se trouvant dans le répertoire layout sous le répertoire res, pour ensuite l'implémenter en java

- a) vrai
- b) faux

10) Les répertoires xhdpi, xxhdpi, hdpi, mdpi sont incluse dans le répertoire :

- a) menu d) gradle
- b) mipmap e) drawable
- c) values

11) Android Studio utilise un système qu'on appelle Gradle pour :

- a) compiler et générer les applications
- b) gérer l'éditeur et les options de la compléction du code
- c) jouer le rôle d'un émulateur

Exercice 2: Répondez aux deux questions suivantes

1) Qu'est-ce qu'un Intent en Android ? Donnez deux exemples.

2) Donnez le rôle du fichier AndroidManifest.xml

Exercice 3: Code à compléter

Il s'agit de créer une application de Calcul mental qui fonctionne comme suit :

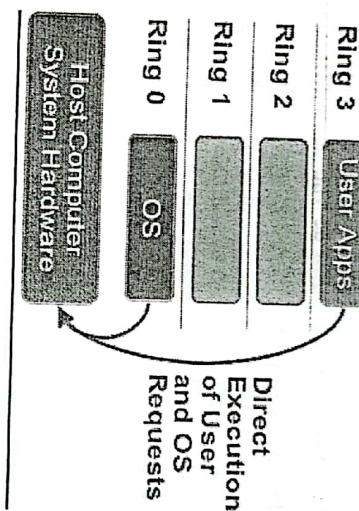
- votre programme génère aléatoirement deux valeurs entières et un opérateur arithmétique, l'affichage sera respectivement dans trois premières TextView (s)
- L'utilisateur propose un résultat dans l'EditText et appuie sur un bouton pour valider
- votre programme compare la réponse de l'utilisateur avec le résultat correcte et affiche un TextView contenant un message soit « Bravo » soit « Echec »
- votre programme donne la possibilité de rejouer une autre fois

INSTITUT SUPÉRIEUR INFORMATIQUE ISI	Ministère de l'enseignement supérieur et de la recherche scientifique ****
Classe : CS 3	Institut Supérieur d'informatique
Date : 05 janvier 2023	Examen - Session principale Intitulé de la matière Virtualisation et Cloud Computing Charge(s) du cours : Wim MRAEBET
Nbre pages : 2	Durée : 1h30 Documents et calculatrices non autorisés

Barème : Ex1 (1-2-1-1-2) EX2 (2-2-1-2) Ex3 (1-1-2-2)

Exercice 1

✓1. Interpréter le schéma suivant et donner un titre :



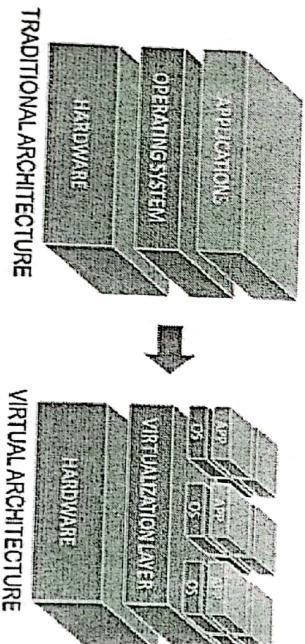
✓2. Présenter et Comparer les différents types de virtualisation.

✓3. Expliquer, à l'aide d'un schéma, chaque type.

? 4. Quels est l'intérêt des Drivers para-virtualisés développés par le VMware ?

Exercice 2

Soit le schéma suivant :



- ✓1. Comparer les deux architectures.
- ✓2. Considérons une petite entreprise qui gère quelques dizaines de serveurs physiques et veut migrer vers une infrastructure virtualisée

✓ a. Encouragez-vous l'entreprise à appliquer la virtualisation ? Justifier votre réponse.

✓ b. Quelle est l'installation typique en termes de serveurs et de stockage pour supporter la virtualisation ?

b. Citer 3 avantages financiers ou techniques de passer à un système virtualisé.

Exercice 3

✓ 1) Expliquer, à l'aide d'un schéma, l'organisation des datacenters.

✓ 2) Le cloud computing permet la maîtrise du budget et la réduction des coûts. Expliquer comment ?

✓ 3. Encouragez-vous les entreprises à utiliser le cloud computing ? Justifier votre réponse.

✓ 4. Citer et comparer les trois modèles du cloud computing, de point de vue des développeurs d'applications et de point de vue des utilisateurs. Discuter de la sécurité et de la fiabilité de chaque modèle.

INSTITUT SUPERIEUR D'INFORMATIQUE ISI	Ministère de l'enseignement supérieur et de la recherche scientifique	Institut Supérieur d'informatique	
Classe : CS 3	Examen - Session principale	Durée : 1h30	****
Date :	Développement d'applications réparties	Documents non	*****
05 janvier 2023	Chargé(s) du cours : Amen Ben Hadj Ali	autorisés	

Bârème : QR (8 pts) EX (4-2-2-4)

Questions de réflexion (8 pts)

1. 1. Un registre RMI sert à stocker les objets répartis RMI (justifiez brièvement la réponse)
 - A. Vrai
 - B. Faux
2. Un client RMI a besoin d'implémenter une interface distante afin de pouvoir invoquer les méthodes de l'objet serveur (expliquez brièvement la réponse)
 - A. Vrai
 - B. Faux
3. Le stub RMI d'un objet serveur est (expliquez brièvement la réponse)
 - A. développé manuellement
 - B. est générée automatiquement par le compilateur java à partir de la classe de l'objet réparti
 - C. est générée automatiquement par le compilateur rmi à partir de la classe de l'objet réparti
 - D. Aucune réponse n'est correcte
4. Afin d'assurer le passage des paramètres lors d'un appel d'une méthode distante, RMI utilise (expliquez brièvement la réponse)
 - A. Le passage de paramètres par référence
 - B. La sérialisation
 - C. L'emballage / déballage
 - D. Cela dépend des types de paramètres (simples ou composés)
 - E. Toutes les réponses sont correctes

Exercice (12 pts)

Il s'agit de développer une application répartie de type client/serveur en utilisant le middleware Java RMI. On considère un système de gestion de conférences offrant un service d'organisation

accessible à distance via Java RMI. Pour organiser une conférence, il faut réservé une ou plusieurs salles de conférence disponibles chez un établissement d'enseignement supérieur identifié par son nom unique et son adresse. Le système gère plusieurs établissements. Chaque établissement dispose d'un certain nombre de salles pouvant être réservées.

Le système offre deux opérations (méthodes) :

- **réserver** : à partir d'un nom de conférence (chaîne), d'un nom d'établissement (chaîne), d'une date et d'un nombre de salles (entier), cette opération renvoie un entier qui correspond au numéro de réservation si celle-ci peut être effectuée ou à -1 sinon.
- **annuler** : à partir d'un numéro de réservation (entier), cette opération annule la réservation correspondante. Cette opération ne retourne rien. Si le numéro de réservation n'est pas valide, cette opération ne fait rien.

Élaborez un diagramme de classes qui représente l'architecture de l'application répartie en précisant le domaine et le rôle de chaque classe.

✓1. Donner un exemple de causes possibles d'une exception de type « `RemoteException` » dans le contexte d'une application RMI.

✓2. Donner le code de l'interface distante.

3. 4. Proposez le code en Java de l'application répartie représentant le service d'organisation de conférences à distance.

NB Le code proposé dans la question 4 doit être en harmonie avec le diagramme de classes déjà proposé dans la première question.

ISI الجامعة الإسلامية	Ministère de l'enseignement supérieur et de la recherche scientifique ****	
Classe : L3CS	Institut Supérieur d'Informatique	Durée : 1h30
Date : 4 janvier 2023	Examen - Session principale Intitulé de la matière SECURITE INFORMATIQUE	Documents non autorisés
Nbre de pages : 8	Chargé(s) du cours : Mhenni Sourour	Calculatrice autorisée

Barème : chaque question 0,4 pts

- Une ou plusieurs réponses sont correctes.
- donner la réponse dans le tableau ci après.
- dans la même question, une réponse fausse annule une réponse correcte

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20
Q21	Q22	Q23	Q24	Q25	Q26	Q27	Q28	Q29	Q30
Q31	Q32	Q33	Q34	Q35	Q36	Q37	Q38	Q39	Q40
Q41	Q42	Q43	Q44	Q45	Q46	Q47	Q48	Q49	Q50

Q1 : L'exhaustivité est la caractéristique d'un scanner de vulnérabilités

- a- pour réduire les vulnérabilités fantômes
- b- pour réduire le nombre des fausses vulnérabilités
- c- pour corriger les vulnérabilités détectées
- d- aucune réponse n'est correcte

Q2 : un pare-feu fonctionne au niveau de la couche

- a. Application
- b. transport
- c. Réseau
- d. Accès réseau

Q3 : « Il peut détecter de nouvelles attaques » Il s'agit de

- a- Signature based IDS
- b- Behavior based IDS

Q4 : Combien de temps faudra t'il pour corriger l'attaque ? La réponse à cette question aura un impact sur

- a- cout de la sécurité seulement
- b- cout du risque seulement
- c- cout implicite seulement
- d- cout explicite seulement
- e- aucune réponse n'est correcte

Q5 : un administrateur pose la question suivante « L'attaque aura-t-elle un impact sur d'autres cibles en relation avec l'entreprise ? »

Il est au niveau de l'étape

- a. Identification du risque
- b. Calcul du cout total de la sécurité
- c. Détermination du niveau du risque
- d. Evaluation du risque
- e. Estimation du risque
- f. Calcul du cout du risque

Q6 : un administrateur fait l'inventaire des contres-mesures dans le SI. Il est au niveau de l'étape

- a. Identification du risque
- b. Calcul du cout total de la sécurité
- c. Détermination du niveau du risque
- d. Evaluation du risque
- e. Estimation du risque
- f. Calcul du cout du risque

Q7 : A votre avis, quel algorithme doit s'exécuter avant l'autre dans un scenario cryptographique.

- a. Diffie Hellman avant DES
- b. DES avant Diffie Hellman

Q8 : pour évaluer le risque, on prend en considération

- a- deux paramètres
- b-trois paramètres
- c-quatre paramètres
- d-cinq paramètres
- e-aucune réponse n'est correcte

Q9 : « Il peut déterminer les attaques de modification de fichiers binaires et fichier de configuration. Il peut identifier des tentatives d'accès non autorisées » Il s'agit de

- a- Firewall applicatif
- b- AIDS
- c-Firewall circuit
- d-HIDS
- e-pot de miel
- f-scanner de vulnérabilités

Q10 : pour déterminer le niveau de risque, on prend en considération un seul et unique paramètre :

a-vrai

b-faux

Q11 : l'opérateur de sécurité pose cette question « Quels sont les formes de perte qui peuvent avoir lieu ? » durant la phase de

- a- la détermination du niveau du risque
- b- l'évaluation du risque
- c- l'identification du risque
- d- le calcul du cout du risque

Q12 : un IDS est un équipement qui analyse en temps réel et prend une décision active lorsqu'un incident de sécurité est détecté

a-vrai

b-faux

O Roux Pointing

Q13 : pour la pertinence d'une réponse d'un mécanisme de sécurité, il faut utiliser une solution passive (qui ne donne pas de réponse en temps réel)

- b. Faux

Q14 : l'identification des vulnérabilités dans un SI, durant le processus de gestion du risque, se fait sur

- ~~a- une étape
b- deux étapes
c- trois étapes
d- quatre étapes~~

a-vrai
b-faux

- b-faux

Q10 : Une signature d'attaque contre un serveur web est définie comme suit :

```
RECHERCHE EXEC echo toor::0:::/bin/sh >> /etc/
```

Fragment 1 - QUOTE SITE

```
fragment 2 - EXEC echo toor::0:0::/bin/sh >> /etc/passwd
```

Est-ce que l'IDS peut détecter cette attaque

b-faux dans tous les cas

d- suivant le mode de positionnement de l'IDS

卷之三

'extérieur alors il faut "utiliser"

a-NIDS

3 - Firewall Circuit

- AIDS

Faux : le « tunnelling » veut dire que les données à transmettre vont être prises en charge par un protocole différent d'IP.

- Q19 : pour mettre à jour la base d'un « signature based IDS », on peut avoir recours à un

 - a- Firewall
 - b- IDS
 - c- Pot de miel
 - d- Scanner de vulnérabilités

Ensuite, nous nous intéressons à l'approche comportementale au niveau des IDS. Nous présentons ici une technique typique qui est la technique probabiliste. Cette technique spécifie la probabilité de chaque événement susceptible de se produire suite à un autre. Par exemple, nous supposons qu'après une séquence A-B-C, le profil accorde à l'événement D une probabilité de 8%. Si l'événement D se produit dans le système à 10%, l'IDS signale une violation du profil.

écart entre la probabilité attendue de l'événement D (c'est-à-dire 8%) et la fréquence observée (c'est-à-dire 10%), l'IDS peut effectuer :

- a. Un vrai positif
- b. Un faux positif
- c. Un vrai négatif
- d. Un faux négatif

Q21 : en basant sur la même technique de la question Q20, et nous supposons que l'IDS peut modifier le profil afin de mieux correspondre au fonctionnement réel. C'est-à-dire que l'IDS peut porter la probabilité normale de l'événement D de 8% à 10%. Alors dans ce cas, l'IDS peut effectuer :

- a. Un vrai positif
- b. Un faux positif
- c. Un vrai négatif
- d. Un faux négatif

Q22 : l'administrateur analyse que les vulnérabilités détectées dans le SI présentent un risque pour le système informatique et les informations de l'entreprise et qu'il y a une réelle possibilité que cela puisse arriver. On peut déduire que le risque est :

- a- majeur
- b- moyen
- c- élevé
- d- faible
- e- acceptable

Q23 : L'identification du risque se base sur

- a- deux étapes
- b- trois étapes
- c- quatre étapes
- d- cinq étapes
- e- aucune réponse n'est correcte

Q24 : soit une clé privée (1079, 1073), une clé publique (1074, 1073) et un message $m=726$. Pour assurer la confidentialité de ce message, il faut calculer

- a. $726^{1074} \bmod(1073)$
- b. $726^{1079} \bmod(1073)$

Q25 : l'algorithme « masque jetable » se base sur la technique

- a. CBC
- b. transposition
- c. substitution

Q26 : l'algorithme « Caesar's cypher » se base sur la technique

- a. ECB
- b. CBC
- c. transposition

Q27 : plus le cout total de la sécurité est réduit, plus le cout initial de la sécurité est important

- a- vrai
- b- faux

Q28 : le paramètre qui existe simultanément dans le calcul du cout du risque et le calcul du cout total de la sécurité est :

- a. Le cout implicite

- b. Le cout de la sécurité initial
c. Le cout des controles-mesures
 d. Le cout explicite

- Q29 : le terme « synchronous cypher » veut dire que
a. la clé dépend du texte clair
b. la clé est aussi longue que le texte clair
 c. la clé ne dépend pas du texte clair
d. aucune réponse n'est correcte

- Q30 : un NIDS installé dans un SI dans lequel le trafic qui circule est chiffré. Le rendement de cet IDS dans le SI va être
a. 100% vrai positif
b. 100% faux positif
 c. 100% vrai négatif
 d. 100% faux négatif
- Q31 : le critère fiabilité avec lequel circule les données dans un réseau a des répercussions sur
 a- la fiabilité du NIDS
b- l'exhaustivité du NIDS
c- la pertinence du NIDS
d- la cohérence du NIDS
e- aucune réponse n'est correcte

- Q32 : le critère fiabilité pour évaluer un mécanisme de sécurité veut dire

- a. 100% vrai positif
b. 0% faux positif
 c. 100% vrai négatif
 d. 0% faux négatif

- Q33 : lors du choix du protocole VPN à adopter, il faut prendre en considération :

- a. 2 critères de sélection
 b. 3 critères de sélection
 c. 4 critères de sélection
d. 5 critères de sélection

- Q34 : le facteur risque est primordiale pour déterminer les mécanismes de sécurité nécessaires pour le cycle de la sécurité
 a- vrai
b- faux

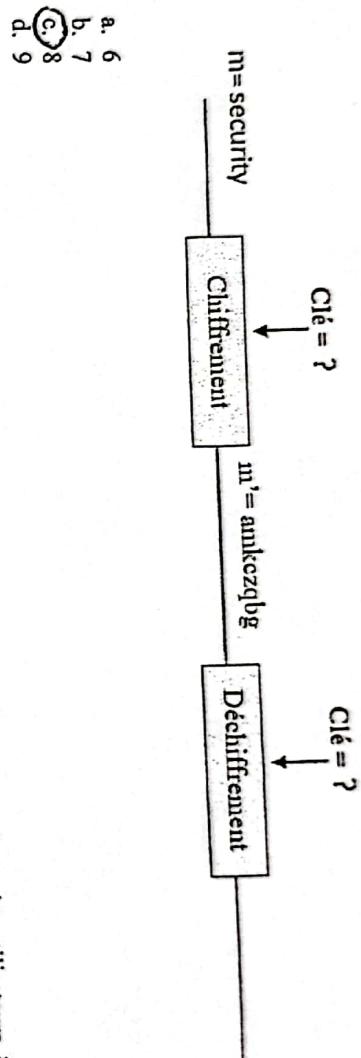
- Q35 : le terme « confusion » en cryptographie veut dire

- a. Un petit changement dans le texte clair doit avoir un effet sur une large partie du texte crypté.
b. Le texte clair ne doit pas être facilement obtenu à partir d'un texte crypté
 c. L'effet d'un petit changement sur le texte clair ne doit pas être prévisible
d. Les clés ne doivent pas être facilement obtenues à partir d'un texte crypté
e. Aucune réponse n'est correcte

- Q36 : Si un émetteur A加密 une empreinte par sa clé privée et l'envoie à B, alors On gagne

- a. La confidentialité et l'intégrité
b. L'authentification et l'intégrité
 c. L'authentification et non répudiation
 d. L'authentification, l'intégrité et non répudiation

Q37 : En utilisant l'algorithme César, la clé utilisée dans le scenario suivant est



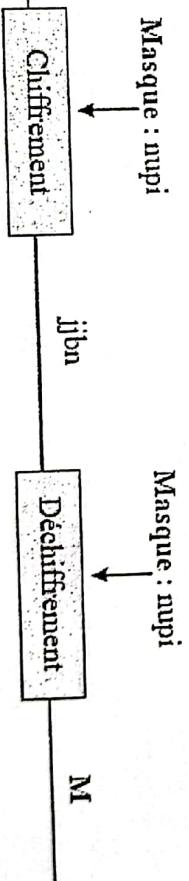
Q38 : si l'opérateur de sécurité veut contrôler l'accès à certaines URL demandées par les utilisateurs, il faut utiliser :

- a- IDS
- b- VPN
- c- Pare-feu (circled)
- d- Scanner de vulnérabilités

Q39 : Le type de chiffrement qui va avec le protocole cryptographique Diffie Helman est

- a. Chiffrement symétrique (circled)
- b. Chiffrement asymétrique
- c. Chiffrement hybride
- d. Tout type de chiffrement

Q40 : En utilisant l'algorithme Masque Jetable. Le message original M est



Q41- En appliquant l'algorithme RSA pour $p = 29$ et $q = 37$; la quelle des valeurs de « e » est correcte

- a. 15
- b. 9
- c. 24
- d. 49
- e. Aucune réponse n'est correcte (circled)

Q42- En appliquant l'algorithme RSA pour $p = 29$ et $q = 37$; si on souhaite chiffrer le message $m = 72697673$, quelle combinaison représente les nombres correctes de blocks du message clair à chiffrer :

- a. soit 6 blocks ou 7 blocks ou 8 blocks

- b. soit 3 blocks ou 4 blocks ou 5 blocks
- c. soit 3 blocks ou 4 blocks ou 8 blocks
- d. soit 4 blocks ou 5 blocks ou 8 blocks
- e. aucune réponse n'est correcte

Q43- Une entité dispose d'une clé privée (1079, 1073) et une clé publique (1074, 1073) et un message $m=726$. Pour assurer l'authenticité de cet utilisateur, il faut calculer ?

- a. $726^{1074} \text{ mod } (1073)$
- b. $726^{1079} \text{ mod } (1073)$
- c. $726^{1073} \text{ mod } (1079)$
- d. $726^{1073} \text{ mod } (1074)$

Q44- Dans la pratique, dans quel but on combine le processus de la signature numérique avec le processus du hachage ?

- a. Gagner du temps
- b. Gagner des ressources
- c. Gagner la confidentialité, l'authentification et l'intégrité
- d. Compliquer le scenario vis à vis des attaquants

Q45- un crypto-système est décrit par

- a. 3 uplets
- b. 4 uplets
- c. 5 uplets
- d. aucune réponse n'est correcte

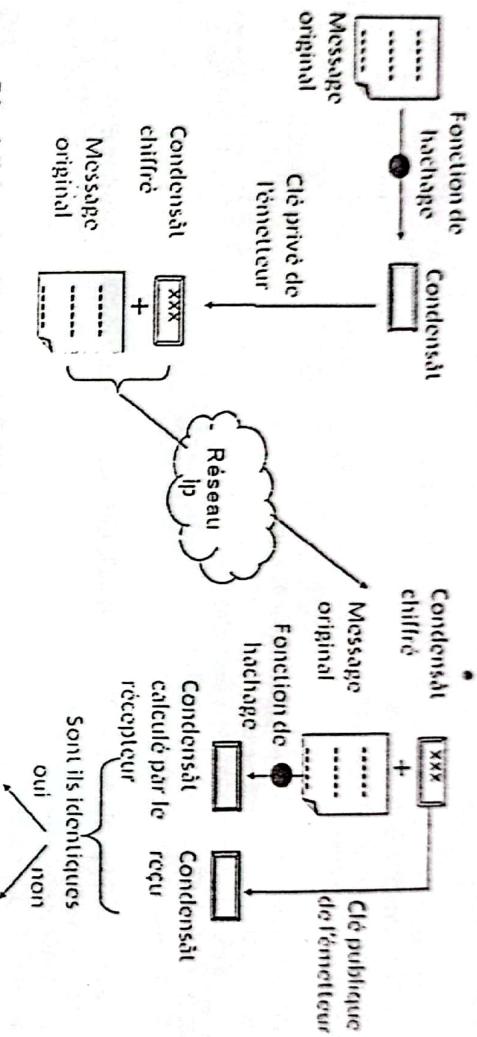
Q46- L'altération d'un message transitant entre deux machines A et B peut être l'une des situations qu'un attaquant peut utiliser. Avec quelle d'algorithme, on peut détecter cette attaque.

- a. AES
- b. DES
- c. RSA
- d. SHA
- e. DH

Q47- pour appliquer la signature numérique sur un message M, le critère principal qu'il faut considérer est que :

- a. le message M soit secret
- b. le message M a une petite taille
- c. le message M ne soit pas secret
- d. le message M a une taille importante

Q48- les services de sécurité obtenus grâce à ce procédé sont



- a. confidentialité, authentification et non répudiation
 b. intégrité, confidentialité et authentification
 c. intégrité, authentification et non répudiation
 d. intégrité et authentification

Q49- la fonction de cryptage au niveau de l'algorithme DES est basée sur

- a. 2 opérations
 b. 3 opérations
 c. 4 opérations
 d. 5 opérations

- Q50- la caractéristique « cohérente » pour une fonction de hachage H veut dire
 a. impossible de trouver $M_1 \neq M_2$ alors que $H(M_1) = H(M_2)$
 b. impossible de trouver M à partir de $H(M)$
 c. impossible de trouver un message M tel que $H_{00}(M) \neq H_{01}(M)$
 d. aucune réponse n'est correcte