

UNIVERSITE BLAISE PASCAL
CLERMONT-FERRAND II

Service des concours
34 avenue Carnot
63000 Clermont-Ferrand

Concours **EXTERNE** - BAP E
Corps : **Assistant Ingénieur**
Spécialité : **Développeur, intégrateur
d'applications**

Session **2008**

Epreuve écrite d'**Admissibilité**

Durée : **3 heures** - Coefficient : **4**

Le sujet comporte 7 pages numérotées de 1 sur 7 à 7 sur 7.

Assurez-vous que cet exemplaire est complet. S'il est incomplet, demandez un autre exemplaire au surveillant de salle.

Il vous est rappelé que votre identité ne doit figurer que sur la première page de la copie d'examen. Toute mention d'identité portée sur toute autre partie de la copie que vous remettrez en fin d'épreuve mènera à l'annulation de votre épreuve.

L'usage de la calculatrice est interdit.

L'usage du téléphone portable est interdit.

Tout document et autre matériel électronique sont interdits.

Ne pas écrire au crayon de papier sur la copie.

1 Partie 1 : Algorithmique / Programmation

1.1 Algorithmes : Affectation

Il s'agit de traiter l'affectation des candidats à un concours ITRF ...

Chaque candidat a la possibilité de faire 2 vœux d'affectation dans une liste de p postes.

Le jury d'admission a choisi 5 candidats sur la liste principale.

On mettra en place une liste de postes sous la forme d'un tableau d'entiers. L'entier stocké prend la valeur 0 si le poste n'est pas attribué et prend comme valeur le n° du candidat affecté sur ce poste.

On dispose pour cela d'une liste des candidats triée par ordre de mérite.

Ecrivez deux procédures d'affectation en langage C :

- En prenant en compte les 2 vœux d'un candidat avant de passer au suivant (procédure proc1),
- En prenant en compte en premier lieu tous les vœux n°1 uniquement puis en second lieu tous les vœux n°2 (procédure proc2). Dans ce cas, on ne se préoccupe des vœux 2 seulement après avoir traité l'ensemble des vœux 1 qui sont prioritaires.

Comparez les résultats de ces 2 procédures.

Candidat	Vœu 1	Vœu 2
10	2	1
20	2	3
30	3	4
40	3	1
50	5	1

Résultat de la procédure proc1

Poste	candidat
1	
2	
3	
4	
5	

Résultat de la procédure proc2

Poste	candidat
1	
2	
3	
4	
5	

1.2 Algorithme : Triangle isocèle

Ecrire un programme en C ou en langage algorithmique, qui affiche un triangle isocèle formé d'étoiles de N lignes (N sera lu au clavier)

Exemple d'affichage attendu pour N=8.

```
*
***
*****
*****
*****
*****
*****
*****
*****
```

1.3 Programmation Orientée Objet

1.3.1 Question 1

- 1) Qu'est-ce que le principe d'encapsulation des données ?
- 2) Quels en sont les avantages ?

1.3.2 Question 2

- 1) En langage objet, qu'appelle-t-on une méthode ?
- 2) Dans le code ci-dessous donner un exemple de méthode.
- 3) Que manque-t-il ? Expliquez et complétez le code.

```
public class Poste implements java.io.Serializable {

    private String categorie ;

    private String grade ;

    private String classe ;

    public void setCategorie( String uneCategorie ) {
        this.categorie = uneCategorie ;
    }

    public getCategorie() {
        return categorie ;
    }

    public void setGrade( String unGrade ) {
        this.grade = unGrade ;
    }

    public getGrade() {
        return grade ;
    }
}
```

```
public void setClasse( String uneClasse ) {  
    this.classe = uneClasse ;  
}  
  
public getClasse() {  
    return classe ;  
}  
}
```

1.4 Divers

Questions

1. Qu'est-ce qu'un helpdesk ? Quels en sont les avantages ?
2. Qu'est-ce qu'un ENT ? Quels en sont les avantages ?

2 Partie 2 : Base de données SQL

2.1 Exercice 1

Soit la relation r de schéma R (A,B,C,D,E) ;

A	B	C	D	E
a1	b1	c1	d1	e1
a1	b2	c2	d2	e1
a2	b1	c3	d3	e1
a2	b1	c4	d3	e1
a3	b2	c5	d1	e1

Question

1. Quelles sont les dépendances fonctionnelles satisfaites par R ?

2.2 Exercice 2

Un vendeur de voitures usagées vend des voitures à un prix unique selon l'année de construction.

Soit le schéma : Voiture (n°stock, marque, modèle, année, couleur, prix).

Questions

1. Pourquoi ce schéma n'est-il pas en 3FN ?
2. Donner une décomposition en 3FN.

2.3 Exercice 3

On se situe dans un centre de gestion comprenant plusieurs agences délocalisées. Dans chaque agence travaillent plusieurs comptables, chacun gérant plusieurs exploitations.

Un comptable ne travaille que dans une seule agence et une exploitation ne peut être gérée que par un seul comptable.

On souhaite connaître la liste des exploitations gérées par chacun des comptables et chacune des agences.

Les informations retenues sont :

- Le nom de l'exploitation,
- La commune où se situe l'exploitation,
- Le nom du comptable,
- Le directeur et la ville de l'agence,
- Le nom de l'agence,
- L'âge du comptable,
- Le n° de téléphone du comptable.

Questions

1. Quelles entités identifiez-vous ?
2. Listez sous forme de tableau les données retenues dans le modèle en identifiant pour chacune son type et sa longueur.
3. Etablissez le schéma entité-relation correspondant à cet énoncé.

4. Etablissez le modèle logique associé, en précisant les clés primaires et étrangères.

2.4 Exercice 4

Le schéma relationnel suivant représente la gestion simplifiée de bandes dessinées (BD) :

BD (NumBD, NomAlbum, NBPages, EditeurNumDessinateur, NumScénariste)

Auteur (NumAuteur, Prénom, Nom, Nationalité)

Magasin (NumMag, NomMag, Adresse, Téléphone, NomResponsable)

BDDansMagasin (NumBD, NumMagasin, NbBDDispo, PrixVente)

Questions

En langage SQL :

1. Donnez les noms des auteurs de bande dessinée (en tant que scénariste ou dessinateur) qui sont responsables d'un magasin.
2. Donnez les noms des magasins dont le responsable est aussi un des auteurs d'une des BD disponibles dans ce même magasin.
3. Donnez la liste des titres d'albums de BD disponibles, regroupés par magasin.

3 Partie 3 : Anglais technique

SecurID

The RSA SecurID authentication mechanism consists of a "token", a piece of hardware (e.g. a token or USB) or software (e.g. a "soft token" for a PDA or cell phone)—assigned to a computer user that generates an authentication code at fixed intervals (usually 30 or 60 seconds) using a built-in clock and the card's factory-encoded random key (known as the "seed" and often provided as a *.asc file). The seed is different for each token, and is loaded into the corresponding RSA SecurID server (RSA Authentication Manager, formerly ACE/Server) as the tokens are purchased. The seed is typically 128 bits long. Some RSA SecurID deployments may use varied second rotations, such as 30-second increments.

The token hardware is designed to be tamper-resistant to deter reverse engineering of the token. Despite this, public code has been developed by the security community allowing a user to emulate RSA SecurID in software, but only if they have access to a current RSA SecurID code, and the original RSA SecurID seed file introduced to the server. In the RSA SecurID authentication scheme, the seed record is the secret key used to generate One Time Passwords. "Soft tokens" are merely commercial software implementations of the same algorithms implemented in the tamper-resistant hardware, only the soft tokens require the seed record to be distributed to clients so that the seed record may be used as input in the One Time Password generation.

A user authenticating to a network resource—say, a dial-in server or a firewall—needs to enter both a personal identification number and the number being displayed at that moment on their RSA SecurID token. Some systems using RSA SecurID disregard PIN implementation altogether, and rely on password/RSA SecurID code combinations. The server, which also has a real-time clock and a database of valid cards with the associated seed records, computes what number the token is supposed to be showing at that moment in time, checks it against what the user entered, and makes the decision to allow or deny access.

On systems implementing PINs, a "duress PIN" may be used—an alternate code which creates a security event log showing that a user was forced to enter their PIN, while still providing transparent authentication.

While the RSA SecurID system adds a strong layer of security to a network, difficulty can occur if the authentication server's clock becomes out of sync with the clock built in to the authentication tokens. However, typically the RSA Authentication Manager automatically corrects for this without affecting the user. It is also possible to manually resync a token in the RSA Authentication Manager. Providing authentication tokens to everyone who might need to access a resource can be expensive, particularly since tokens are programmed to "expire" at a fixed time, usually three years, requiring purchase of a new token.

RSA SecurID currently commands over 70% of the two-factor authentication market (source: IDC) and 25 million devices have been produced to date. A number of competitors, such as VASCO, make similar security tokens.

RSA Security has pushed forth an initiative called "Ubiquitous Authentication", partnering with device manufacturers such as Sandisk, Motorola, Freescale Semiconductor, Redcanon, Broadcom and BlackBerry to embed the SecurID software into everyday devices such as memory sticks and cell phones, to reduce cost and the number of objects that the user must carry.

Other network authentication systems, such as OPIE and S/Key (sometimes more generally known as OTP, as S/Key is a trademark of Telcordia Technologies, formerly Bellcore) attempt to provide the "something you have" level of authentication without requiring a hardware token.

Questions

1. Qu'est-ce qu'un OTP?
2. Quel est son principe de fonctionnement?
3. Quels sont ses atouts et ses failles ?
4. Citez et décrivez succinctement d'autres systèmes d'authentification
5. Qu'est ce que le SSO (Single Sign On) ? Quels en sont les avantages ?
6. Quelle est la différence entre autorisation et authentification ?