DESS CONCEPTION DES LOGICIELS SURS
Examen Sécurité Sûreté de fonctionnement
13 janvier 2000

Durée 3 heures
Tous documents autorisés

Conseil : Consacrer environs 2 heures à la première partie et une heure à la seconde

PREMIER PARTIE

PREMIERE PARTIE

On considère l'algorithme de synchronisation d'horloges DHSS défini par le code suivant (syntaxe de type ADA)

```
task body DHSS is
begin
Me :=myname() ;        -- fonction système rendant le nom unique de l'appelant
NEXT_SYN :=PERIODE ;
SET_TIMER(TP,NEXT_SYN) ;      -- Initialise le délai de garde TP à la valeur
                              -- NEXT-SYN absolue


loop
        select                          -- Ceci permet de se mettre en attente
                                        -- sur des évènements asynchrones
        accept TIMEOUT(TP)              -- Retombée du délai de garde TP
        --(1) à compléter
        -- Le site courant a été réveillé par son time out local. Il se dépêche de diffuser la
        nouvelle pour réveiller les autres sites. A partir de cet instant il ne traitera plus aucun
        événement pour la période.

                Mess.type :=wake_up ;
                Mess.sender :=Me
                Mess.value := NEXT_SYN ;
                M :=SIGN(Me,Mess) ;     -- Signe le message avec une signature
                                        --numérique
                BROADCAST(M) ;
                NEXT_SYN := NEXT_SYN+PERIODE ;   -- On passe à la période suivante
                SET_TIMER(TP,NEXT_SYN) ;
                CONVERGENCE_CLOCK(NEXT_SYN) ; -- Appel à la fonction
                                                -- locale de convergence
                                                -- Cet appel n'est traité
                                                -- qu'au premier appel de la
                                                -- période
```

```
        or

        accept RECEIVE(M) ;                    -- Réception d'un message
        -- (2) à compléter
        -- Le site courant est réveillé par un message reçu d'un autre site et non pas par son
        délai local. Si le message est jugé bon il le renvoie à tous
                READ_CLOCK(C) ;                -- Lecture de l'horloge locale

                -- Contrôle des signatures successives  portées par le message :
                -- M est le message signé, SUCESS est un booléen, vrai si le contrôle
                --d'intégrité et de validité des signatures est bon , s est le nombre de signataires
                -- du message, Mess est le message sans signature.

                UNSIGN(M,Mess,s, SUCCESS)

                -- Contrôle de validité du message,
                -- ρ est le taux de dérive maximal d'une horloge correcte
                -- dmax est le temps maximal entre l'émission et
                -- la réception d'un message transmis sans faute,
                -- P est la précision de l'algorithme
                if (SUCESS and (Mess.value =NEXT_SYN) and
                (Mess.value-(C –s* dmax *(1-ρ))≤P) then
                        M :=SIGN(Me, M) ;
                        BRODCAST(M) ;
                        CONVERGENCE_CLOCK(NEXT_SYN) ;
                end if
        end select
end loop
end DHSS
```

QUESTION 1. COMPREHENSION DE L'ALGORITHME

QUESTION 1.1 : (4 points) Selon la classification donnée en cours, préciser :

· L'horloge idéale

L'horloge idéale est la plus rapide : le premier site qui se réveille, réveille tous les autres

· Le choix des points de re-synchronisation

La re-synchronisation est périodique de période PERIODE

· Donner un commentaire pour les points 1 et 2 à compléter

(voir texte)

QUESTION 1.2 Rappelez les propriétés d'une signature numérique. Pourquoi s est il égal au nombre de sites qui ont renvoyés le message M ? Que représente la quantité s*dmax, Pourquoi faut-il signer les messages ? (2 points)

*Une signature est inimitable, attachée à un message, contrôlable par tous. Chaque site qui envoie le message le signe donc s est égal au nombre d'envoi de M. s *dmax est une borne supérieure du temps séparant l'émission et la courante réception de M. Il faut signer itérativement le message pour garantir que le contenu n'est jamais modifié de M et la valeur de s est juste. Si la valeur de s pouvait être modifiée (compteur), un pirate pourrait augmenter cette valeur et rendre inopérant le test de validité des messages.*

QUESTION 1.3 Dans le test de validité des messages (4 points) :

1.2.1 Que signifie Mess. Value=NEXT _SYN ? (1 point)
1.2.2 Donnez le sens général du test (Mess.value-(C -s *dmax *(1-ρ))≤P) ? (1 point)

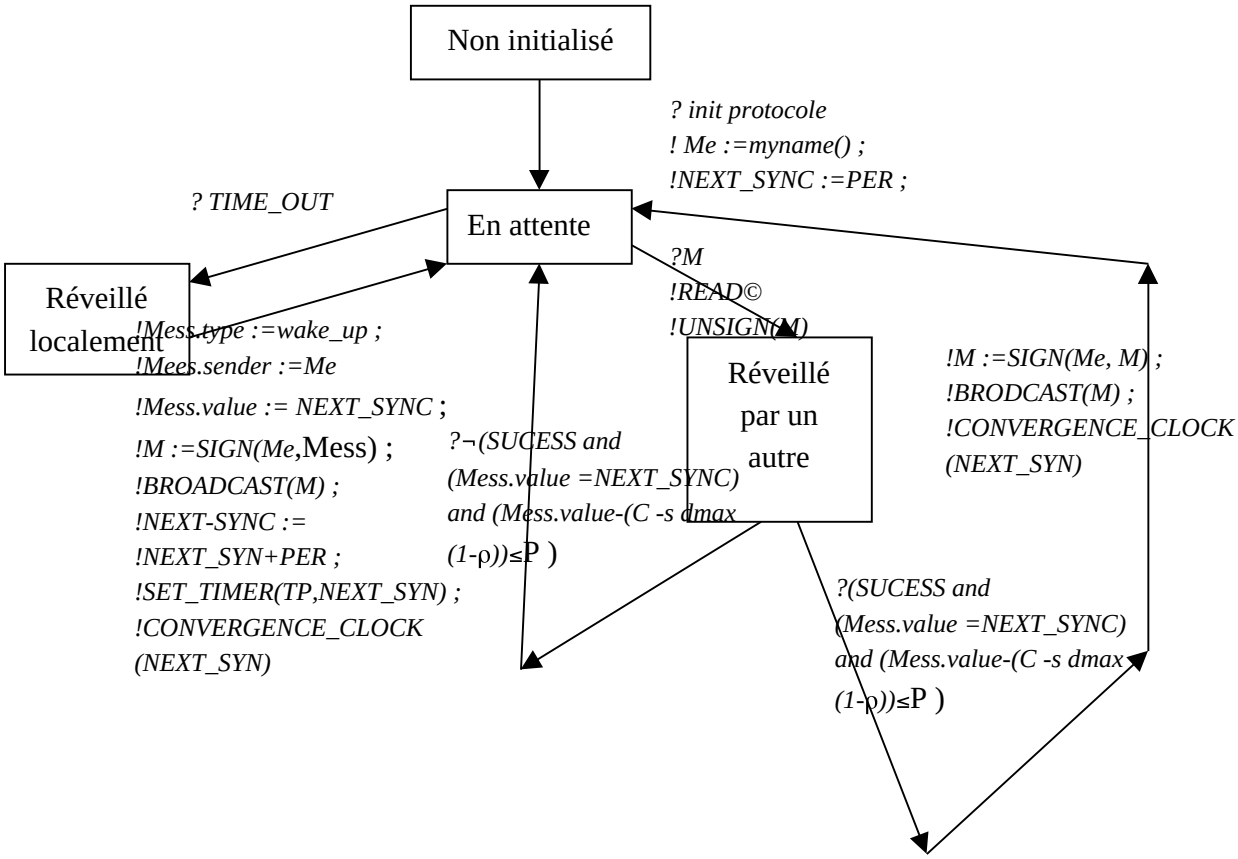
Si l'on note t l'instant de réception du message et C(x) la valeur de l'horloge locale à l'instant x, expliquez pourquoi
1.2.3 Mess.value- C(t-s *dmax) ≤P (1 point)
1.2.4 (Mess.value-(C(t) -s *dmax *(1-ρ))≤P (1 point)

SUCESS indique que toutes les signatures sont correctes, Mess.Value= NEXT_SYN indique que le message vise la même période que celle considérée dans le site courant,
(Mess.value-(C –s dmax* (1-ρ))≤P)*
indique que le message n'est pas trop vieux (parti top tôt).

Soit t la date de réception du message, datée localement par C(t).
Le message a été émis au plus tôt à C(t-s dmax).
Or comme le processus courant n'était pas réveillé
Mess.value> C(t-s dmax)*
et comme les horloges sont synchronisées
Mess.value- C(t-s dmax) ≤P.*
Or C(t-s dmax) ≤ C(t) –s dmax *(1-ρ), du fait de la limite de la dérive des horloges.*
Donc
*(Mess.value-(C -s *dmax *(1-ρ))≤P*

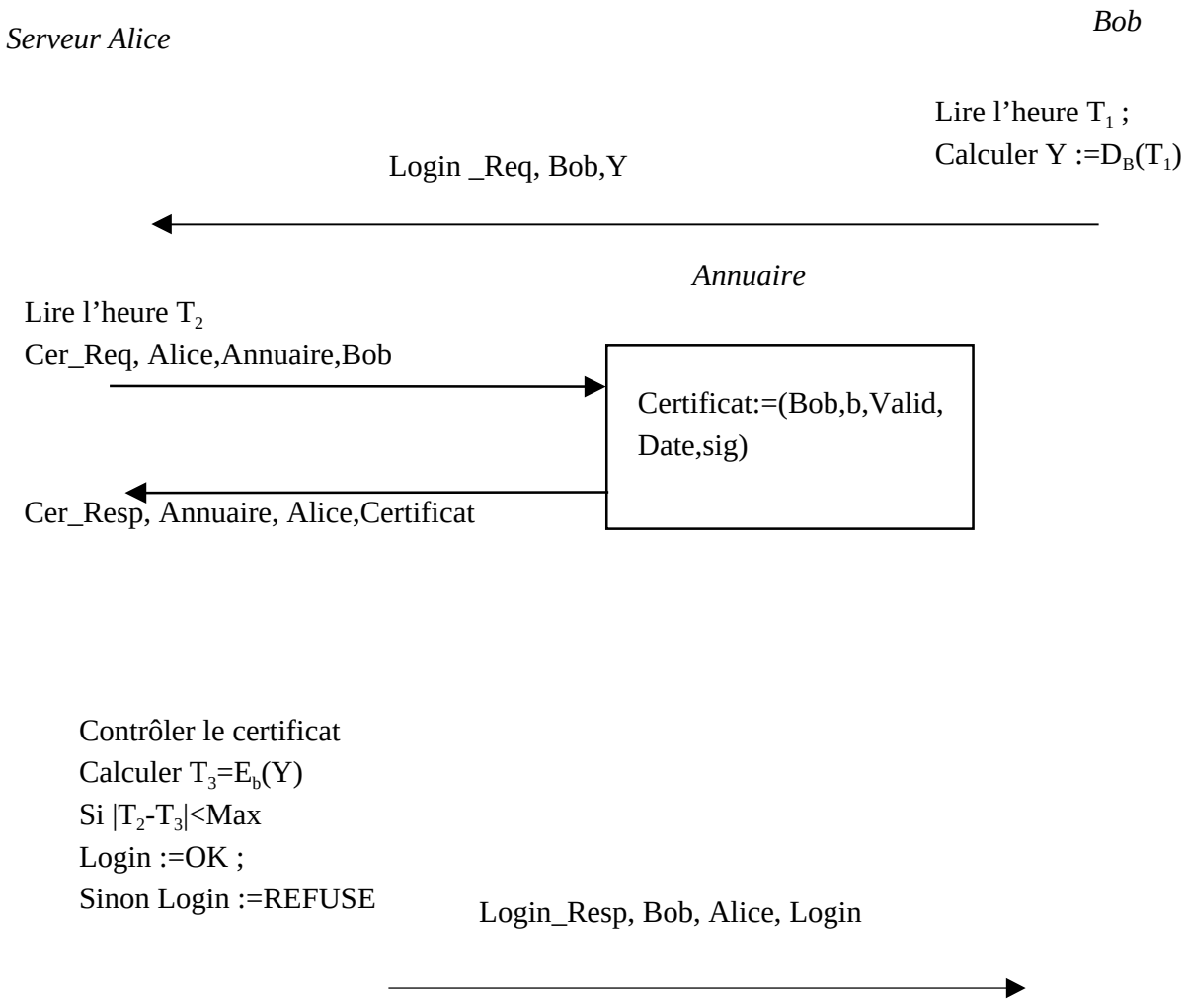
QUESTION 2 MODELISATION (4 points)

Proposez un modèle du protocole sous forme d'un automate à états communicants. On considèrera quatre états : Non initialisé, En attente, Réveillé localement, Réveillé par un autre.



QUESTION 3 SECURITE

Le protocole suivant décrit sous forme de MSC un login distant avec authentification utilisant des clefs publiques. B est la clef privée de Bob et b sa clef publique. On suppose que les horloges des deux sites sont synchronisées avec un algorithme de précision P.



Contrôler le certificat
Calculer $T_3=E_b(Y)$
Si $|T_2-T_3|<Max$
Login :=OK ;
Sinon Login :=REFUSE

Login_Resp, Bob, Alice, Login

QUESTION 3.1 (3 points)
Expliquez en quelques lignes le principe de ce protocole, en particulier l'usage des clefs. Pouquoi utilise t'on l'heure? Pourquoi est il important que les horloges soient synchronisées?

Bob chiffre l'heure avec sa clef privée. Si Alice trouve une heure correcte après déchiffrement avec la clef publique, Bob est authentifié. L'heure permet de se prémunir des rejeux

QUESTION 3.2 (3 points)
Notons Dmax le temps maximun admissible pour envoyer un message, ρ la dérive maximale relative de deux horloges et P la précision de l'algorithme de synchronisation. Quel est la plus petite valeur que l'on puisse donner à Max pour ne pas refuser à tort un login?
Rappel : le taux de dérive relatif entre deux horloges correctes définit le plus petite valeur ρ ($0 \leq \rho \leq 1$) telle que si l'un des horloges mesure une durée t par T_A, l'autre horloge par T_B alors T_B appartient à $[(1-\rho)\ T_A, [(1+\rho)\ T_A]$

Par un calcul analogue à la question 2 on trouve Max= P+(1+ρ)Dmax

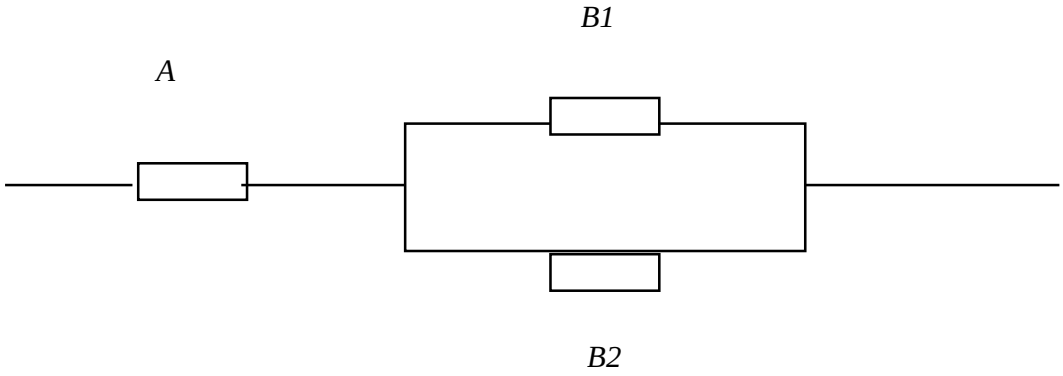
QUESTION 3.3 (2 poinst)
On suppose qu'un pirate ne peut rejouer une information dans le temps Max défini précédemment. Il décide de s'attaquer au protocole de synchronisation d'horloge pour pouvoir altérer le test de contrôle de login. Que va t'il essayer de faire? Pourquoi dans ce cas l'utilisation de l'algorithme DHSS est particulièrement indiquée?

Il va essayer de « ralentir » le temps synchronisé pour faire croire qu'un délai supérieur à Max s'est déroulé avant Max, ceci lui donnant le temps de rejouer. Or DHSS se synchronise sur l'horloge la plus rapide, donc à moins de pervertir tous les sites, le pirate ne peut « ralentir » le temps : il peut juste l'accélérer ce qui ne présente aucun intérêt pour lui.

SECONDE PARTIE

Un système informatique comprend un premier ordinateur A suivi de deux processeurs identiques

B1 et B2 :



Ce système peut donc assurer sa mission si A fonctionne et si B1 ou B2 (ou les deux) fonctionnent.

B1 et B2 sont en redondance sélective active : ils fonctionnent en parallèle en permanence ; si B1 tombe en panne, il est immédiatement relayé par B2 (si B2 n'est pas déjà en panne).

QUESTION 1 (3 points)

Q1.1 On suppose connues les fiabilités $R_A(t)$ et $R_B(t)$, respectivement de l'ordinateur A et d'un processeur.(B1 et B2 ont la même fiabilité.

Calculer la fiabilité R(t) du système et son MTTF (durée de vie moyenne), en l'absence de toute réparation, en fonction de $R_A(t)$ et $R_B(t)$ (1 point)

$$R(t) = R_A(t)(1-(1-(R_B(t))^2))$$

Q1.2 Application : $R_A(t) = e^{-at}$; $R_B(t) = e^{-bt}$: expliciter R(t) et le MTTF (2 points)

$$MTTF = \int_0^{+\infty} R(t)dt = \int_0^{+\infty} e^{-at}(1-(1-e^{-bt})^2\,dt$$

$$MTTF = \int_0^{+\infty} R(t)dt = \int_0^{+\infty} e^{-at}(1-(1-e^{-bt})^2 dt$$

$$= \int_0^{+\infty}(2e^{-(a+b)t} - e^{-(a+2bt)})dt = \frac{1}{a+b} - \frac{1}{a+2b}$$

QUESTION 2 (4 points)

On désire modéliser le fonctionnement de ce système par un processus de Markov à trois états (sachant que des réparations sont possibles, cf. ci-dessous) : E0, E1 et E2

E2 : panne paralysante (A en panne, ou bien B1 et B2 sont en panne).

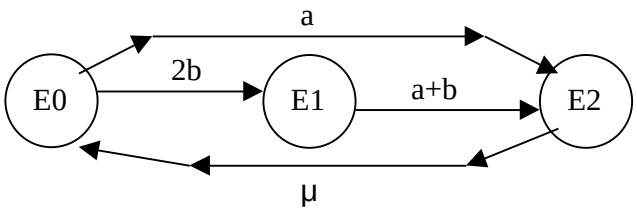
Q2.1 Préciser les états E0 et E1. (à 0,5 point)

E0 Tout marche
E1 : B1 ou (exclusivement) B2 est en panne

Dès qu'une panne paralysante est intervenue, une réparation du ou des éléments en panne démarre : la probabilité pour que la durée aléatoire d'une réparation dépasse t est $e^{-\mu t}$ (ceci, quelque soit le nombre d'éléments à réparer).

A partir de l'état E1 , on n'entreprend pas de réparation

Q2.2 Tracer le graphe simplifié du processus de Markov associé. Valuer chacun de ses quatre arcs par le taux convenable : vous commencerez par recenser pour chaque état quels sont les éléments qui fonctionnent et donc sont susceptibles de tomber en panne. Montrer, en particulier, que le taux λ_{12}, qui value l'arc (E1, E2) égale a + b. (1,5 points)



Q2.3 Ce processus est-il ergodique ? Justifier votre réponse.

Oui : le graphe est fini et fortement connexe

Si oui, appliquer le théorème des coupes à E0 puis à E1 et en déduire les probabilités, en régime permanent, sachant que a = b et μ = 10a. (2 points)

$$R(t) = R_A(t)(1-(1-(R_B(t))^2))$$

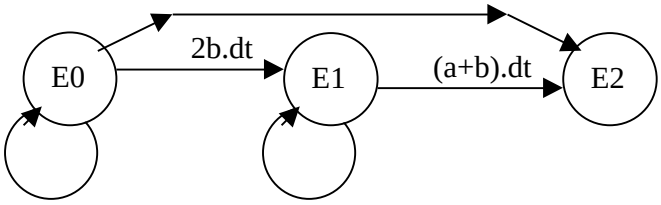
QUESTION 3 (3 points)
On considère le même système, mais en l'absence de réparations. Q3.1 Tracer et valuer le graphe (non simplifié) des transitions entre t et t + dt. (1 point)

Q 3.2 Montrer que les probabilités des états à l'instant t satisfont les équations différentielles ci-dessous (établir notamment la matrice du générateur du processus de Markov(1,5 points)) :

$$\Pi'_0(t) = -(a+2b).\Pi_0(t)$$

$$\Pi'_1(t) = \Pi_0(t).2b - (a+b).\Pi_1(t)$$

$$\Pi'_2(t) = \Pi_0(t).a + \Pi_1(t)(a+b)$$



D'après lecture du graphe on trouve

$$\Pi_0(t+dt) = \Pi_0(t)(1-(a+2b)dt)$$
$$\Pi_1(t+dt) = \Pi_0(t).2b.dt + \Pi_1(t)(1-(a+b)dt)$$
$$\Pi_2(t+dt) = \Pi_0(t).a.dt + \Pi_1(t)(a+b).dt + \Pi_2(t)$$

ce qui donne

$$(\Pi_0(t+dt) - \Pi_0(t))/\,dt = -(a+2b).\Pi_0(t)$$
$$(\Pi_1(t+dt) - \Pi_1(t))/dt = \Pi_0(t).2b - (a+b).\Pi_1(t)$$
$$(\Pi_2(t+dt) - \Pi_2(t)).dt = \Pi_0(t).a + \Pi_1(t)(a+b)$$

donc

$$\Pi'_0(t) = -(a+2b).\Pi_0(t)$$
$$\Pi'_1(t) = \Pi_0(t).2b - (a+b).\Pi_1(t)$$
$$\Pi'_2(t) = \Pi_0(t).a + \Pi_1(t)(a+b)$$

Le générateur est donc

$$\begin{pmatrix} -(a+2b) & 2b & a \\ 0 & -(a+b) & (a+b) \\ 0 & 0 & 0 \end{pmatrix}$$

Ce qui donne sous forme matricielle

$$\begin{pmatrix} \Pi'_0 & \Pi'_1 & \Pi'_2 \end{pmatrix} = \begin{pmatrix} \Pi_0 & \Pi_1 & \Pi_2 \end{pmatrix} \begin{pmatrix} -(a+2b) & 2b & a \\ 0 & -(a+b) & (a+b) \\ 0 & 0 & 0 \end{pmatrix}$$

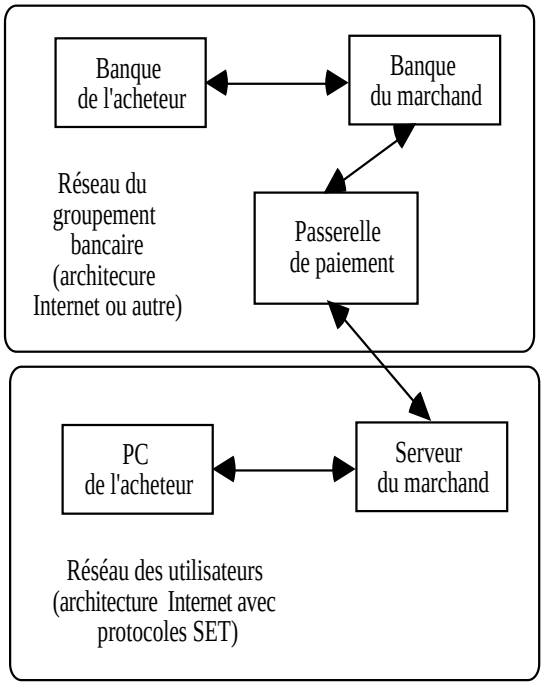
Q3.3Justifier pourquoi on a l'égalité R(t) = [ ] (0,5 point)

Le système fonctionne tant qu'il n'est pas rentré dans l'état 2, ce qui, pour une distribution initiale $\Pi_0 = 1$*, correspond à la définition de la fiabilité.*

Commerce électronique sur Internet: l'approche SET ("Secure Electronic Transactions")

Pour sécuriser le commerce électronique sur Internet le standard SET a été proposé en 1996/1997. Il est soutenu par les principaux groupements de cartes bancaires Visa et Master card ainsi que par de nombreux fournisseurs (IBM, Microsoft, ...). SET propose un ensemble de protocoles de sécurité pour le paiement par carte bancaire sur Internet. Il utilise pour cela des techniques de cryptographie (à clés publiques RSA, à clés secrètes DES, de fonction de hachage SHA-1). C'est une solution purement logicielle.

Une vision simplifiée de l'architecture de SET est donnée par la figure suivante ou apparaissent les différents calculateurs de l'acheteur, du marchand, des banques ainsi qu'une passerelle faisant interface entre le monde internet (utilisant le protocole SET) et le réseau bancaire.



Le fonctionnement de base est analogue à celui des cartes de crédits habituelles. L'acheteur connecte son poste de travail sur le serveur du marchand. Il consulte le catalogue des produits proposés, passe commande et autorise le paiement. Le marchand accepte la commande et la réalise. Le marchand pour se

faire payer adresse à sa banque l'autorisation de paiement de l'acheteur via la passerelle de paiement.

On trouve donc trois protocoles essentiels dans SET:

- Le protocole d'achat.
- Le protocole d'autorisation de paiement.
- Le protocole de paiement

Voici (parmi de nombreuses autres) quelques règles de sécurité de base que les protocoles SET doivent respecter :

a) L'acheteur et la passerelle de paiement doivent pouvoir vérifier que le marchand est bien celui qu'il prétend être. Le marchand doit pouvoir vérifier que l'acheteur et la passerelle de paiement sont bien ceux qu'ils prétendent être.

b) Une personne non autorisée ne doit pas pouvoir modifier les messages échangés entre le marchand et la passerelle de paiement.

c) Le marchand ne doit pas pouvoir accéder au numéro de la carte de l'acheteur.

d) Le banquier n'a pas à connaître la nature de la commande passée par l'acheteur au marchand

1) Les trois propriétés de sécurité sont associées aux règles précédentes sont des problèmes généraux traités en cours. Donnez chaque propriété les noms des problèmes associés (1,5 points). Rappelez de manière succinte la définition de ces problèmes (en une phrase) (2 points).

Correction

a) Authentification : C'est le processus qui consiste à vérifier que l'auteur d'une action (ici l'émetteur d'un message) est bien celui qu'il prétend être.

b) Intégrité: C'est la propriété qui assure qu'une donnée (ici un message) n'est modifiée que dans des conditions prédéfinies (par des entités autorisées).

c) Confidentialité. C'est la propriété qui assure qu'une donnée (ici un numéro de carte) n'est consulté que par des entités autorisées.

2) SET est un protocole de sécurité applicatif, qui inclut une politique de sécurité. A partir des éléments précédents on vous demande de spécifier cette politique
2.1) Quels sont les quatre rôles qui doivent être considérés (2 points)

Correction

Le banquier, l'acheteur, le marchand, les autres

On définit les objets suivants

1. La carte bleue
2. Le pin code de la carte bleue
3. Le numéro de la carte bleue
4. L'identifiant de la commande
5. Le contenu qualitatif de la commande
6. Le prix de la commande

Selon l'objet une ou plusieurs des méthodes suivantes sont applicables:
A. Créer,
B. lire/connaître,
C. Accepter/signer
D. Détenir

2.2) Pour chaque objet donner les méthodes applicables (3 points)

Correction

1: A,D
2:A,B
3:A,B
4:A,B
5: A,B,C
6: A,B,C

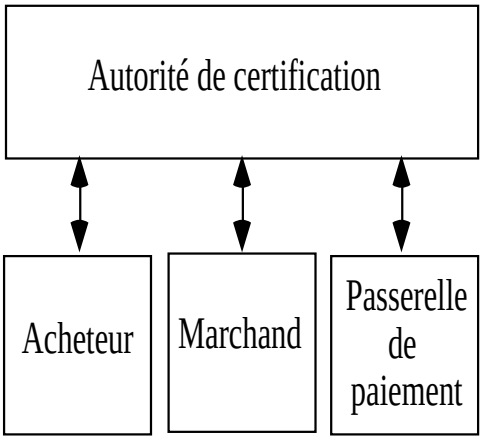
2.3) Etablir la matrice des droits: Il s'agit d'une matrice ayant en colonne (au nombre de14) les méthode et en ligne (au nombre de 4) les rôles. Si un rôle X à le droit d'utiliser la méthode y l'élément X,y est marqué à 1 et n'est pas marqué sinon (5 points)

Correction

1A : Créer carte
1D détenir carte
2A créer pin code
2B connaître pin code
3A créer numéro de carte
3B connaître numéro de carte
4A créer identifiant commande
4B Connaître identifiant commande
5A créer contenu de la commande
5B connaître le contenu qualitatif de la commande
5C signer le contenu de la commande
6A créer le prix de la commande
6B connaître le prix de la commande
6C signer le prix de la commande

	1A	*1D*	*2A*	*2B*	*3A*	*3B*	*4A*	*4B*	*5A*	*5B*	*5C*	*6A*	*6B*	*6C*
Banquier	*1*		*1*		*1*	*1*		*1*					*1*	
Acheteur		*1*		*1*		*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*
Marchand								*1*		*1*			*1*	
Autres														

2 Pour mettre en oeuvre les protocoles de sécurité utilisant la cryptographie SET définit une phase d'accréditation préalable des acteurs par une autorité de certification (en fait une hiérarchie d'autorités).



Vue globalement l'autorité de certification délivre des certificats aux différents acteurs des protocoles SET. Qu'est ce qu'un certificat? Quelles en sont les propriétés principales? (2 points)

Correction

Un certificat regroupe un ensemble d'informations caractéristiques d'un usager (et de l'autorité de délivrance du certificat). Il comporte donc toujours un identificateur précis de l'usager (nom, adresse,) mais aussi différentes informations utiles dans le cadre d'une politique de sécurité. Les certificats au format X509 les plus utilisés contiennent la clé publique de l'usager, la date limite de validité, le numéro du certificat etc.

Le certificat est délivré par une autorité de certification à un usager pour être utilisé en univers réseau. On doit pouvoir vérifier qu'un certificat n'a pas été forgé par un intrus mais uniquement par un organisme de confiance. L'autorité de certification doit donc être connue et authentifiable. Elle doit appliquer une signature numérique infalsifiable au certificat qui soit vérifiable par tous.

3 SET utilise la cryptographie à clé publique RSA avec des clés d'une longueur de 1024 bits.

3.1 Quels sont les avantages et les inconvénients d'une telle longueur de clés? (1 point)

3.2 En fait le RSA est utilisé pour distribuer des clés privées DES (c'est l'algorithme de cryptographie à clé privée DES qui set à chiffrer les messages). Pourquoi adopter une telle stratégie? (1 point)

3.3 Dans un cas d'école en cryptographie RSA on utilise comme clé publique le couple (3 , 55) et comme clé privée le couple (27, 55). Quel est le codage du message M = 7 lorsque l'on chiffre avec la clé publique? (2 points).

Correction

3.1 L'avantage d'une clé longue est la difficulté pour un attaquant de casser le code. Les clés de 512 bits étaient jugées incassables il y a quelques années mais des réussites spectaculaires ont été obtenues par la progression dans les puissances de calcul. On a pu casser le RSA 512 bits en plusieurs mois de calcul. Pour assurer une durée suffisante à la norme il est donc préférable de choisir une longueur un peu surdimensionnée.

L'inconvénient est le coût plus important en temps de calcul dans la fabrication des clés et dans les phases d'encryptage/décryptage.

3.2 C'est justement pour ne pas perdre de temps avec un RSA à clé très longue portant sur le contenu des messages qu'on utilise le RSA pour échanger une clé DES puis on passe en mode DES qui est environ mille fois plus rapide.

3.3 La règle de codage du RSA indique que pour une clé publique (e, n) le message M codé est défini par M^e *mod (n). Ici on a M=7, e=3 et n = 55 . On doit donc faire le calcul de* 7^3 *mod (55) = 343 mod(55). Comme 343 = 6*55 +13 le message codé est 13.*

4 SET adopte une méthode de signature numérique basée sur la norme SHA-1 ("Secure Hash Algorithm" - Version 1) et sur l'algorithme RSA.

4.1 SHA-1 définit une fonction de hachage à sens unique sans clé. Rappelez la définition d'une fonction de hachage à sens unique sans clé? (1 point)

4.2 La signature numérique d'un message en SET est définie par:

$RSA_{clé\_privée\_émetteur}$ (SHA-1 (Message))

C'est l'application au message de la fonction de hachage à sens unique sans clé puis l'application au résultat précédent du cryptage RSA avec la clé privée de l'émetteur. Par rapport aux propriétés attendues d'une signature, pourquoi définit-on ainsi la signature numérique? (2 points)

Corrigé

4.1 On rappelle qu'une fonction de hachage est une fonction mathématique qui à partir d'un message (d'une donnée) génère une autre chaîne (généralement plus courte) "aussi caractéristique que possible de la chaîne initiale". Plus précisément pour une utilisation en sécurité il faut que f posséde des propriétés intéressantes: il est difficile de créer un message M significatif tel que f(M) = K (notion de collision faible). Il est difficile de trouver M et M' significatifs tels que f(M) = f(M') (notion de collision forte). Autre terminologie: fonction de contraction, digest, empreinte digitale, "hash code"...

Une fonction à sens unique est une fonction f(M) facile à calculer mais telle qu'il est extrêmement difficile de déduire M de f(M) (de calculer la fonction inverse).

Une fonction de hachage à sens unique sans clé est donc une fonction de hachage à sens unique qui peut être calculée sans connaissance d'un secret (par n'importe qui). Exemples types MD5, SHA-1

4.2 Une signature manuscrite idéale est réputée posséder les propriétés suivantes:

*- La signature **ne peut-être imitée.***

Elle prouve que le signataire a délibérément signé le document.

*- La signature **authentifie** le signataire.*

Seul le signataire peut avoir signé.

*- La signature appartient à un seul document (elle **n'est pas réutilisable**).*

*- Le document signé ne peut être partiellement ou totalement **modifié**.*

*- La signature ne peut-être **reniée**.*

Reprenons les points précédents en utilisant sur un message une fonction de hachage à sens unique chiffrée en RSA avec la clé privée de l'émetteur.

*- La signature **ne peut-être imitée. -> Utilisation du chiffre RSA à clé privée si la clé reste effectivement secrete.***

*- La signature **authentifie** le signataire. -> Seul le propriétaire de la clé privée peut chiffrer ainis: cest donc bien lui.*

Seul le signataire peut avoir signé.

*- La signature appartient à un seul document (elle **n'est pas réutilisable**) -> L'existence d'une fonction de hachage à sens unique qui fournit une empreinte caractéristique du document.*

*- La signature ne peut-être **reniée**. -> C'est un autre problème- Plus juridique celui de la non répudiation.*

5 On étudie maintenant le processus d'achat. Il se déroule en deux échanges requêtes réponses successifs.

Premier échange (l'échange initial)

La requête initiale de l'acheteur vers le marchand indique simplement en clair l'intention par l'acheteur de passer commande.

La réponse initiale du marchand comporte trois éléments:

- un identifiant de commande plus sa signature numérique
- le certificat du marchand avec sa clé publique
- le certificat de la passerelle de paiement avec sa clé publique.

A la suite de ce premier échange, quelles vérifications peuvent être effectuées par l'acheteur (2 points).

Corrigé

L'acheteur commence par vérifier les certifcats du marchand et de la passerelle de paiement en s'adresse à l'autorité de certification.

Au moyen de la signature numérique et du certificat du marchand l'acheteur peut vérifier:

- que le message n'a pas été modifié en cours de route (le numéro de commande est le bon.

- que le marchand est bien celui qu'il prétend être puisqu'il a pu signer avec sa clé privée l'empreinte.

6 Le second échange du processus d'achat comporte l'envoi de la requête d'achat et une réponse d'accusé de réception de commande.

Envoi de la requête d'achat

L'acheteur construit la structure de donnée commande qui a vocation a être communiquée au marchand (produits, quantités, prix avec l'identification de la commande fournie par le marchand pendant l'échange initial...). Elle est baptisée par la suite OI ("Order Information").

L'acheteur construit la structure de données de paiement qui a vocation a être communiquée à la passerelle de paiement (informations concernant la carte bancaire de l'acheteur et identification de la commande à payer fournie par le marchand pendant l'échange initial). Elle est baptisée dans la suite PI ("Payment Information").

En fait les deux structures de données sont liées. Le paiement ne concerne que la commande identifiée. Il doit être effectué que si la commande est acceptée par le marchand. La commande n'est effective que si la banque approuve le paiement. De plus le contenu de la commande doit-être caché à la banque et le contenu des instructions de paiement doivent être cachées au marchand.

Pour lier les deux structures de données, l'acheteur calcule par l'algorithme SHA-1 la fonction de hachage de chacune des structures de données SHA-1(OI) et SHA-1(PI). Il applique à nouveau la fonction de hachage SHA_1 à l'ensemble (SHA-1(OI), SHA-1(PI)) des fonctions de hachage concaténées. Il chiffre cette dernière empreinte en RSA avec sa clé privée. C'est en fait une signature numérique double qui est réalisée. Elle est baptisée dans la norme SET signature duale.

Signature duale =

$RSA_{clé\_privée\_acheteur}$ (SHA_1 ((SHA-1(OI), SHA-1(PI))

Le message suivant est préparé pour la passerelle de paiement:

PI, Signature duale

L'acheteur choisit une clé aléatoire clé_aléa pour le DES. Le message a destination de la passerelle de paiement est chiffré en DES au moyen de cette clé.

$DES_{clé\_aléa}$ (PI, Signature duale)

La clé DES est chiffrée au moyen de la clé publique de la passerelle arrivée avec le certificat de la passerelle.

$RSA_{clé\_publique\_passerelle}$ (clé_aléa)

Finalement le message de requête d'achat envoyé au marchand contient toutes les informations suivantes:

$DES_{clé\_aléa}$ (PI, Signature duale) ,

SHA-1(PI) ,

$RSA_{clé\_publique\_passerelle}$ (clé_aléa) ,

OI,
Signature duale,
Certificat de l'acheteur.

Envoi de la réponse du marchand à la requête d'achat

Le marchand construit un message de réponse qui a comme unique signification d'être un accusé de réception de la commande. Le marchand signe numériquement ce message(fonction SHA_1 et chiffre RSA avec sa clé privée). Il ajoute à l'ensemble son propre certificat.

6.1 Comment le marchand vérifie t'il l'intégrité de la commande OI? (1 point)
6.2 Comment est réalisée la confidentialité des informations concernant la carte de crédit vis à vis du marchand? (1 point)
6.3 Comment le marchand vérifie t'il que l'acheteur est bien celui qu'il prétend être? (1 point)

Corrigé

6.1 La vérification de l'intégrité de la commande est un peu plus compliquée que dans le mode de signature simple. En fait on dispose de OI en clair donc on peut calculer SHA-1(OI). On a pris soin d'envoyer dans le message SHA-1(PI). Donc on peut concaténer les deux empreintes et en prendre l'empreinte. On refrabrique une valeur de la signature duale que l'on peut comparer avec la valeur acheminée dans le message.

6.2 De manière assez naturelle compte tenu de la composition du message on voit que le marchand dispose d'une version chiffrée en DES des informations de paiement qu'il ne peut déchiffrer car la clé DES a été choisie aléatoirement, elle est présente dans le message mais chiffrée avec la clé publique de la passerelle de paiement donc indéchiffrable par le marchand.

Quand le marchand demandera le paiement à la passerelle de paiement il pourra passer le version chiffrée et la clé de chiffrement déchiffrable par la passerelle.

6.3 Lorsque l'acheteur a envoyé sa commande il a présenté son certificat (qui est vérifiable et contient la clé publique de l'acheteur) et la signature duale (chiffrée en RSA avec la clé privée de l'acheteur que lui seul peut utiliser). Le marchand peut donc vérifier la signature de l'acheteur.

Remarque: Les commandes des acheteurs circulent en clair sur le réseau ce qui veut dire que si un intrus arrive à espionner les voies de communication il peut connaitre la nature des relations commerciales entre l'acheteur et le marchand. Ceci n'a pas été jugé suffisamment grave pour des relations de commerce électronique grand public (la plus grande partie probablement du commerce électronique). Pour des relations industrielles ou plus sensibles il pourrait être jugé nécesssaire de crypter OI en confidentialité. Rien n'empèche de le prévoir spécifiquement dans certaines relations commerciales.