Université Joseph Fourier
DESS Génie Informatique - année 2001-2002

Examen de Systèmes Répartis
18 décembre 2001

Durée :2 heures ; documents autorisés : ceux distribués en cours

---

N.B. L'examen comporte 3 problèmes indépendants. Prière de lire attentivement l'ensemble de l'énoncé avant de commencer à répondre, et de respecter les notations du texte. La longueur de l'énoncé n'est pas un signe de difficulté, mais est nécessaire pour bien spécifier les problèmes. La **clarté**, la **précision** et la **concision** des réponses, ainsi que leur **présentation matérielle**, seront des éléments importants d'appréciation.

Problème 1. (10 points)

Ce problème est consacré à l'examen de quelques opérations utilisant les techniques de la cryptographie. On rappelle les notations : si M est un message, on note $C=\{M\}_K$ le résultat du chiffrement de M en utilisant une clé K ; on note $M=[C]_K$ le résultat du déchiffrement du message chiffré C en utilisant une clé K.

Les 3 questions sont indépendantes.

Question 1. Étant donné les avantages des algorithmes de chiffrement à clés publiques, pourquoi continue-t-on à utiliser des clés secrètes ? Comment combiner les avantages de ces deux modes de chiffrement ?

Question 2. Pour réaliser un système de paiement électronique, on utilise des "chèques électroniques" signés par le titulaire du compte, avec un système à clés publiques. Un tel chèque comporte une information M ainsi qu'une "signature" $\{D(M)\}_{KSN}$. D est une fonction de hachage non inversible, M contient le nom N du titulaire du compte, le nom B de la banque et la somme S, et enfin KSN est la clé secrète de N. On suppose que la clé publique de N, KPN, est accessible à tous. Une personne recevant un chèque en paiement l'envoie à la banque.

a) Expliquer comment la banque vérifie l'authenticité de la signature et l'intégrité du chèque (c'est-à-dire sa non-modification après signature).

b) Le schéma ci-dessus permet à une personne de faire une copie du chèque et de l'envoyer à la banque pour se faire payer deux fois. Proposez une modification simple pour éviter cela.

Question 3. On veut réaliser un système d'authentification en utilisant la cryptographie à clé secrète. Soit A et B deux partenaires qui veulent s'authentifier mutuellement, puis communiquer entre eux en utilisant le chiffrement à clé secrète. Ils font appel à un serveur d'authentification S qui connaît la clé secrète de A, KA et la clé secrète de B, KB. Le protocole se déroule comme suit :

$A \rightarrow B$: $I, A, B, \{RA, I, A, B\}_{K\,A}$ où I est un numéro d'ordre (incrémenté à chaque authentification) et RA un nombre choisi au hasard.

$B \rightarrow S$: $I, A, B, \{RA, I, A, B\}_{KA}, \{RB, I, A, B\}_{KB}$ où RB est un autre nombre tiré au hasard.

$S \rightarrow B$: $I, \{RA, K\}_{KA}, \{RB, K\}_{KB}$, où K est la clé secrète choisie par S pour la communication entre A et B.

$B \rightarrow A$: ???

a) Quel est le dernier message envoyé de *B* vers *A*, qui conclut le protocole d'authentification ?

b) Expliquer comment *A* et *B* peuvent chacun avoir l'assurance que son correspondant est bien celui qu'il prétend être. Expliquer le rôle de *I, RA* et *RB*.

Problème 2 (10 points)

Les questions de ce problème sont indépendantes.

Question 1. La réalisation d'un appel de procédure à distance fait appel à un service de gestion de noms, qui comporte trois fonctions :

Enregistrer (nom de service, adresse, numéro de version)

Supprimer (nom de service, adresse, numéro de version)

Chercher (nom de service, numéro de version) : adresse

L'information *adresse* se compose de l'adresse IP d'un serveur et d'un numéro de porte.

On souhaite modifier le service de gestion de noms de manière qu'un même service puisse être rendu par plusieurs serveurs différents.

a) Rappeler la place du service de gestion de noms dans la réalisation de l'appel de procédure à distance.

b) Quel est l'intérêt de la modification demandée ?

c) Proposer une modification de l'interface du service de noms pour permettre un tel fonctionnement et donner le principe de la réalisation du nouveau service de noms.

Question 2.

Cette question est consacrée à la conception d'un service réparti de gestion de fichiers. On souhaite que ce service présente les propriétés suivantes :

1) la gestion des noms et la gestion du stockage physique sont séparées,

2) il est possible de déplacer physiquement des fichiers (non en cours d'utilisation) sans que leur nom soit modifié.

a) Quel est l'intérêt des deux propriétés ci-dessus ?

b) Le service de noms réalise l'association entre un nom symbolique de fichier et un descripteur interne. Sans donner le détail du fonctionnement du service de noms, ni la forme des noms symboliques, on demande de définir les fonctions qui constituent l'interface du service de noms. Comment se fait la liaison entre la gestion des noms et la gestion du stockage physique ?

c) Chaque fichier possède un descripteur interne qui contient un numéro de volume et un numéro de fichier dans le volume. Un volume est un ensemble de fichiers ; c'est, par définition, l'unité de duplication et de mobilité. On ne s'occupera pas du détail de l'organisation interne des volumes. Indiquer quelles structures de données sont nécessaires pour réaliser la mobilité des volumes et donner le principe du déplacement d'un volume entre deux serveurs.

d) On souhaite maintenant pouvoir dupliquer certains volumes, sur des serveurs différents. Expliquer comment est modifiée l'organisation ci-dessus.