Composition de Sécurité logique et Edi-2001

La composition est décomposée en deux parties :

- Une partie théorique d'étude de certaines techniques de sécurité
- Une partie d'étude de cas

Le support de cours est permis.

1. Techniques de Sécurité (5,5 points)

1.1 Modes RSA

Le but de ce problème est d'étudier quelques modes du fonctionnement RSA.

a) Mode NUL : Ce mode consiste à appliquer la signature au sceau du message selon la formule :

$M' = [Sceau(M)]^S \bmod N$

- Démontrer que la force de ce mode peut être réduite à la force de la fonction de scellement. (0,5 point, deux lignes)
- Démontrer qu'une signature selon ce mode peut être attaquée pour un message ancien. (0,5 point, deux lignes)

b) Mode Récupération de Message (ISO9796/DSMR). Ce mode consiste à appliquer la signature sur le message directement selon la formule $M' = [M]^S \bmod N$

- Définir la condition pour pouvoir récupérer le message d'origine lors de la vérification. (0,5 point, deux lignes)
- Dans le cas d'un message devant être signé et ne respectant pas la condition précédente que proposer vous pour pouvoir le signer ? (1 point, deux lignes)

1.2 Utilisation des calculettes d'Authentification

Les calculettes de sécurité sont des dispositifs ayant deux fonctions de base :

- Génération de mot de passe dynamique,
- Authentification forte du porteur de calculette.

Les deux fonctions utilisent un algorithme symétrique (exemple DES).
Par exemple l'authentification est une fonction f(Horodatage, Question, Identité Porteur, Numéro de Série Calculette) ; où Question est le challenge envoyé par le serveur au porteur de calculette. Le résultat de cette fonction s'appelle authentifiant.

Les mots de passe dynamiques et authentifiants sont sur 6 à 8 digits.

Un fournisseur de calculettes fournit une troisième fonction qu'il appelle « signature » et se base sur la fonction f(Horodatage, Hash , Identité Porteur, Numéro de Série Calculette) ; où Hash est le sceau des données sur 8 digits.

- Démontrer que la fonction de signature (dont la force est réduite à celle de la fonction Hash) est facilement attaquable par l'attaque des dates d'anniversaires.(1 point ; trois lignes) en calculant le nombre des messages de la date d'anniversaire.
- Démontrer que dans le cas de litige la « signature » du propriétaire de la calculette ne peut pas constituer une preuve juridique. (1 point ; trois lignes)

1.3 Login dans une page d'accueil

Pour quelle raison le Login dans une page d'accueil doit se faire sous https et non pas sous http (1 point. 3 lignes)

2. Etude de Cas (15 points)

INGODWETRUST est une autorité mondiale de certification pour l'échange entre clients et banques ; et définit certaines règles de sécurité concernant la signature électronique et la gestion des certificats.

Une grande entreprise désire faire des virements avec ses banques à l'international, en leur spécifiant ses besoins. Les transferts seront faits par FTP sur SSL et Internet. Les virements sont au format PAYMUL. La signature est basée sur l'utilisation du message AUTACK et l'utilisation d'un certificat INGODWETRUST. L'entreprise doit mettre en marche le projet au plus tard en six mois.

1) Quels sont les avantages pour les banques participant à INGODWETRUST. (1 point. 2 lignes)

2) Pour les banques ne participant pas à INGODWETRUST, que proposez vous pour la gestion des certificats côté entreprise, et côté banques ? (1 point. 3 lignes)

3) La taille moyenne d'un virement unitaire est de 320 octets. Sachant que le message PAYMUL contient un enregistrement donneur d'ordre (512 octets), et 80000 virements unitaires en moyenne et que les virements se font la fin du mois dans un créneau horaire de trois heures. La surcharge protocolaire est de 5%.

   - Calculer la taille moyenne d'un fichier signé. (0,5 point)

- Calculer la vitesse de la ligne de transmission sachant que le transfert doit se faire en 15 minutes maximum(Choisir parmi 64kbs, 256 kbs, 1 Mbs) (0,5 point)

4) Définir les risques pour chaque entité de l'architecture (client et banque). (2 points)

5) Le client a la possibilité entre développer la solution globale lui-même et acheter un produit.

- Achat d'un produit à 300000$ + 15% de maintenance annuelle à partir de la seconde année.
- Développements en interne de quatre années-homme avec salaire annuel brut moyen de 30000$/ingénieur. Puis un ingénieur de maintenance à mi-temps à partir de la seconde année.

Quelle solution préconisez vous ? (2 point)

6) INGODWETRUST préconise l'utilisation des cartes à microcircuits. (2,5 points).

- Combien de certificats préconisez vous pour chaque entité.
- Définir le mapping de la carte (fichiers, types, droits d'accès, taille).
- Deux cartes sont préconisées : 1Koctets et 8Koctets. Quelle est la carte qui doit être choisie ?

7) Le client veut utiliser XML à la place du message AUTACK pour avoir l'accusé de réception. Ecrire une implantation de l'accusé de réception en XML en faisant figurer les références unique du PAYMUL. (Ne pas utiliser ni DTD, ni style-sheet). (1,5 point).

8) Le client émet un virement. La banque nie l'avoir obtenu. Que préconisez vous (1 point. 3 lignes).

9) La signature est appliquée sur le fichier en totalité. Implémenter la signature côté client en utilisant les requêtes de sécurité PKCS11. (1,5 point)

10) Implémenter la vérification de signature ainsi que la génération de l'accusé de réception côté banque en utilisant les requêtes de sécurité PKCS11. (1,5 point)