Composition de Sécurité logique et Edi

La composition est décomposée en deux parties :

- Une partie théorique d'étude de certains caractéristiques des algorithmes cryptologiques
- Une partie d'étude de cas

Le support de cours est permis.

1. Algorithmes (8 points)

1.1 Vitesse d'exécution du RSA

(2 points)

a. L'implantation classique du RSA se base sur l'algorithme fastexp

fastexp: Calcul de M' = $M^{(S)}$ mod (N)

si S = $S_n S_{n-1}..S_0$
S_n, S_{n-1}. . S_0 représentent les bits de S.
Sn est le bit le plus significatif et S0 est le bit le moins significatif.

Début

```
X := M.
Si  S0 =1
                alors Y :=X
Sinon
                        Y := 0

Pour (i = 1;  i  < n; i++)
{
        X= X*X mod (N)
        Si Si=1 alors
                Y = Y*X  mod(N)
}

M' := Y.
```

Fin.

Démontrer que le temps d'exécution d'une signature est surtout proportionnelle au cube de la taille de la clé. Rappel : taille de S équivalente taille de N

b. Pour améliorer les temps d'exécution d'une signature on utilise le théorème des restes chinois basé sur l'algorithme suivant :

N = p *q
Sp = S mod (p-1)
Sq = S mod (q-1)

p2 = (M mod p) exp Sp mod p
q2 = (M mod q) exp Sq mod q

u = (p exp -1 mod q)

alors M' = p2 + (u * (q2-p2)) mod q * p

Démontrer que la performance d'une signature est améliorée par un facteur 4 par rapport à fastexp.

1.2 Attaque contre les petits exposants publiques du RSA

(2,5 points)

$M' = M^V \bmod N$.

a. Démontrer que pour les petits exposants (par exemple 3), le chiffrement de messages d'une certaine taille maximale est indépendante de N en vous basant sur V=3 .
b. Faire une analogie.
c. Pour continuer à utiliser le même exposant que proposez vous pour se protéger contre cette attaque ?

1.3 Resynchronisation du mode CBC

(1 point)

M doit être chiffré en mode CBC par un algorithme symétrique. M est décomposé en blocs Bi. (i=0 à n)
Chaque Bi est chiffré en B'i.
Lors de la transmission le bloc B'k subit une altération de transmission. Trouver le nombre de blocs affectés par l'altération.

1.4 Echange de clé par Diffie-Hellman (algorithme DH)

(2,5 points)

En utilisant les requêtes de sécurité ETEBAC5 implémenter un transfert de fichier chiffré en DES 112 bits avec échange de clé par DH ; le transfert n'inclut pas d'authentification ni signature.

Les facteurs g et n sont supposés connus.
Pour l'exponentiation utiliser la fonction CPENCIPH utilisant comme paramètres exposant et modulo.

2. Etude de Cas (12 points)

Une banque désire offrir un service d'Electronic Banking à sa clientèle professionnelle (200 clients) : virements de masse et relevés.
Elle a le choix entre les solutions suivantes :

a) Transfert par FTP de fichiers chiffrés et signés.
b) Transfert par email de fichiers attachés chiffrés et signés.

1) Quels facteurs jouent en faveur du transfert par FTP. (0,5 point)

2) La banque adapte le transfert par FTP. Les relevés sont récupérés entre 6 h et 9h le matin. La taille moyenne des relevés est de 100Koctets.
En supposant que la récupération se fait d'une façon uniforme pour tous les clients, définir le débit minimal en kb/s de la ligne côté banque. (Débits normalisés : 64kb/s, 256kb/s, 1Mb/s). (0,5 point)

3) Les virements de masse se font la fin du mois sur trois jours. Chaque fichier a une taille de 10 Mo. En ne tenant pas compte des relevés réévaluer le débit minimal de la ligne côté banque.
(0,5 point)

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

5) Définir les protections à mettre en place. (2 points)

6) Le logiciel EDI sous Windows 32 bits client coûte 1000$, la banque a trois possibilités pour la sécurisation du logiciel EDI :

- logiciel maintenu + lecteur de cartes avec clavier intégré+ carte à puce à 500$
- logiciel maintenu + lecteur de cartes + carte à puce à 200$
- logiciel non maintenu + lecteur de cartes + carte à puce à 100$

a) Quelle solution préconisez vous ?
b) La banque ne veut pas dépendre d'une seul fournisseur de lecteurs de cartes, quelle solution préconisez vous ?

(1 point)

7) La banque va fournir le service de certification pour sa clientèle ainsi que du RSA 1024 bits.

a) Est il nécessaire d'avoir un RA (autorité de définition de noms uniques) ?

b) Combien de certificats par porteur de carte préconisez vous ?
c) Définir les fichiers de la carte à puce (identité, taille, droits d'accès).

(2 points)

8) Les fichiers transmis sont signés/chiffrés avant encapsulation par une enveloppe XML.
Chaque fichier a un identifiant unique FID.
La protection des clés de chiffrement est faite par RSA.
Définir cette enveloppe de sécurité (éléments) hors DTD et hors feuille de style. (2,5 points)

9) La banque a deux possibilités pour le logiciel serveur :

- Achat d'un produit à 100000$ + 15% de maintenance annuelle à partir de la seconde année.
- Développements en interne de deux 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 ? (1 point)