Composition de Sécurité logique - 2006

La composition est décomposée en trois parties :

- Une partie d'étude de cas réel
- Question Bonus concernant le cas réel
- L'utilisation d'une API de sécurité

Il est recommandé aux élèves de bien choisir l'ordre des parties selon leurs compétences et rapidités.

Le support de cours est permis. La majeure partie des questions font appel au sens pratique d'ingénieur et le suivi du cours en classe, il est recommandé à l'élève de ne pas perdre son temps pour rechercher les solutions dans le support de cours.

1. Etude de Cas Réel. Le Parti Politique Electronique (15 points)

L'Association des Utilisateurs de l'Internet du Royaume du Wouroudistan désire créer un parti politique et prôner la dématérialisation totale de l'activité politique à travers l'utilisation de l'Internet. Plusieurs fournisseurs locaux (au Royaume) d'Internet existent mais sont concurrents pour la plupart de l'Association. Un des fournisseurs appartient à la famille royale.

La première étape consiste à promouvoir l'association et récolter les adhésions via un serveur Web hébergé en dehors du Wouroudistan .
L'adhésion consiste à introduire les diverses informations d'identité de l'adhérent, son adresse, son email, la localité d'élection, des informations familiales et le numéro de téléphone.
Les informations saisies d'adhésion sont envoyées dans une base de données.

a) Quels sont les risques pour un adhérant se connectant en dehors du Wouroudistan et proposant son adhésion? (2 lignes)
b) Quels sont les risques pour un adhérant se connectant de l'intérieur du Wouroudistan et proposant son adhésion? (4 lignes)
c) Quelles sont les protections contre les risques du point b.
d) Le site a été attaqué par une attaque de type SYN-FLOOD. Quelles protections proposez vous ?
e) En dehors de l'indisponibilité du service du point d quels sont les divers risques sur le serveur incluant la base de données et les protections que vous proposez ? (10-15 lignes)
f) Le site peut être administré et mis à jour soit à partir du Wouroudistan soit à partir du lieu de l'hébergement. Dans le cas d'administration et la mise à jour à partir du Wouroudistan quels sont les risques et les protections que vous proposez ?
g) En fonction des divers points précédents quels sont les règles de filtrage du Firewall ?

L'Association veut démontrer la facilité d'utilisation des certificats pour le vote électoral. Elle distribue à tous ceux qui le demandent des certificats délivrés par une autorité reconnue mondialement dans le but de signer une pétition demandant le vote électronique.

h) Pour quelle raison la distribution des certificats doit se faire pour tous ceux qui demandent de signer la pétition ? (1 ligne)
i) Est ce qu'on doit être limité au nombre de signataires et pourquoi? En fonction de la réponse quel type d'enveloppe de signature préconisez vous ? (5 lignes)
j) Quel type de signature doit s'appliquer sur la pétition ? (1 ligne)

La pétition a été acceptée par le Roi et qui décide de créer une autorité de certification pour délivrer des certificats sur des cartes à puce.
L'usage des divers certificats est le suivant : démarches administratives, vote et protection de clés de chiffrement.
Chaque carte à puce doit contenir trois certificats, trois clés privées (sous forme S,N,P) correspondant à chaque certificat. Les clés des citoyens ont une taille de 1024 bits chacune et l'autorité racine a une taille de 4096 bits.

k) En terme d'autorités quelle politique de certification proposez vous et pourquoi? (3-5 lignes)
l) Pour quelle(s) raison(s) il est préférable d'avoir les certificats sur une carte au lieu du disque ? (2-3 lignes)
m) Définir la mapping de la carte en tenant compte des droits à l'utilisation et personnalisation et choisir parmi une des cartes suivantes (16koctets, 32koctets, 64koctets)

Le vote électronique doit se faire par le Web. Mais pour cela il faut qu'il respecte exactement les lois locales incluant l'existence d'une commission indépendante électorale qui supervise les élections et le conseil constitutionnel pour recevoir les plaintes.

n) Citez cinq règles que doivent respecter un vote non électronique en général ? (5 lignes)
o) Décrire un processus de vote électronique par le Web en implémentant tous les mécanismes et techniques de sécurité pour respecter les règles citées précédemment.

2. Question Bonus : Choisir **une** questions sur trois (5 points)

- Discuter de la nécessité d'une autorité différente de celle créée par le Roi.
- Discuter du rôle en tant qu'entités de sécurité de la commission et du conseil constitutionnel.
- Comment le Roi peut falsifier les votes sans laisser de traces ?

3. API de sécurité (5 points)

Utiliser les requêtes ETEBAC5 (incluant l'accès au dispositif de sécurité) pour implémenter le chiffrement et le déchiffrement 3DES en mode CBC d'un fichier échangé entre un émetteur et un récepteur et utilisant les techniques suivantes :

- génération aléatoire d'une clé 3DES (112 bits) et un vecteur d'initialisation IV de 8 octets.
- échange protégé par certificats de la clé et de l'IV concaténés. La taille de la clé RSA est de 1024 bits.
- Lecture du fichier par blocs de 2048 octets.

Requêtes ETEBAC5 disponibles :

```
XEVoid MOP_DEV(OLDPTRUCHAR coderet,    int  *lg,uchar *device, uchar **IDi, uchar *version);
XEVoid MCL_DEV(OLDPTRUCHAR coderet,char *IDi, uint * File_num);
XEVoid MD_INTRO(OLDPTRUCHAR coderet, char *IDi, uchar *noserie, OLDPTRUCHAR pres_clavier, uchar *version);
XEVoid MV_PRES (OLDPTRUCHAR coderet, char *IDi , uchar *noserie);
XEVoid MV_CODE (OLDPTRUCHAR coderet,uchar *IDi,  uint lg_code, uchar *code, OLDPTRUCHAR etat);
XEVoid MMOD_CODE (OLDPTRUCHAR coderet,uchar *IDi, uint lg_code, uchar *Certificatncien_code,uchar
*nouveau_code);
XEVoid ML_ACCR(OLDPTRUCHAR coderet, uint rang, char *IDi, uint *lg_a, uchar *Certificat);
XEVoid MD_ACCR(OLDPTRUCHAR coderet,char *IDi,  uint lga, uchar *Certificat);
XEVoid D_ALEA(OLDPTRUCHAR coderet, uint lg, uchar *Q);
XEVoid MD_SIGN(OLDPTRUCHAR coderet, uint rang, char *IDi, uint lg1, uchar *D, uint *lg2, uchar *S);
XEVoid V_SIGN(OLDPTRUCHAR coderet, uint lgcp, uchar *Certificat, uint lg1, uchar *D, uint lg2, uchar *S, uint *lg3,
uchar *R);
XEVoid MD_AUTH(OLDPTRUCHAR coderet, uint rang, char *IDi, uint lg1, uchar *Q, uint *lg2, uchar *S);
XEVoid DV_AUTH(OLDPTRUCHAR coderet, uint lgcp, uchar *Certificat, uint lg1, uchar *Q, uint lg2, uchar *S);
XEVoid D_CPDECIPH(OLDPTRUCHAR coderet, uint lg, uchar *Certificat, uint lgin, uchar *pin, uint *lgout, uchar *pout);
XEVoid MD_DECIPH(OLDPTRUCHAR coderet, uint rang,char *IDi, uint lgin, uchar *kin,uint *lgout,uchar *kout);
XEVoid D_K2_1(OLDPTRUCHAR coderet, uint t, uint lgk, uint lgiv, uchar *kiv);
XEVoid D_CHIF(OLDPTRUCHAR coderet, uint t, uint m, uint lgk, uint lgiv, uchar *kiv,  uint lgdata, uchar *pdata, uint
*lgout, uchar *pout);
XEVoid D_DECHIF(OLDPTRUCHAR coderet, uint t, uint m, uint lgk, uint lgiv, uchar *kiv, uint lgdata, uchar *pin, uint
*lgout, uchar *pout);
```