Examen : Introduction à la sécruité

Date: 15.10.2013
1h00, 60 points

- Seul une feuille de note personnelle manuscrite A4 recto verso est autorisée.
- Le nombre de points par exercice correspond au nombres de minutes nécessaires pour le résoudre.

Exercise 1 (Questions de cours (14 points))

1. (2 points) Expiquer la différence entre clef publique et clef symétrique
2. (2 points) Citer deux chiffrement à clef publique et deux chiffrements à clefs secrètes.
3. (3 points) Classer les trois primitives cryptographiques de la plus rapide à la plus lente en temps d'exécution. Justifiez votre classement :
   - Chiffrement assymétrique
   - Chiffrement symmétrique
   - Fonction de hachage
4. (4 points) Donner les 7 notions de sécurité utilisées pour caractériser les primitives de chiffrement modernes et donner les relations entre elles.
5. (3 points) Donner un exemple d'attaque par injection SQL.

Exercise 2 (E-exam (10 points))

Expliquer et justifier 5 propriétés que doit respecter un système d'examen en ligne. (2 points par propriétés).

Exercise 3 (Vote (14 points))

Suppossons que nous souhaitions evaluer le cours de Sécurité durant ce semestre en utilisant le protocole suivant. Sur une feuille de papier nous avons deux champs qui correspondent à "BON" et à "MAUVAIS". Dans chaque champ le professeur inscrit un nombre aléatoire. Il conserve les deux nombres inscrits dans les deux champs. Chaque étudiant prend le papier, efface le nombre présent dans le champs de son choix et inscrit le nombre effacé augmenter de 1. Une fois que tous les étudiants ont eu la feuille le professeur la récupére et en déduit le résultat.

- (4 points) Donner 4 propriétés qu'un système de vote doit satisfaire.
- (2 points) Comment le professeur retrouve-t-il le résultat ?
- (2 points) Comment vérifie-t-il que le nombre de votes correspond au nombre de participants ?
- (6 points) Décrire deux attaques contre ce protocole.

Exercise 4 (Elgamal (12 points))
Nous rappelons le chiffrement d'ElGamal.

- Clef privée : a
- Clef publique : (p, g, h), où $h = g^a \mod p$.
- Chiffrement : Pour chiffrer M Bob choisit un nombre aléatoire r et calcule $(u, v) = (g^r \mod p, Mh^r \mod p)$
- Déchiffrement : $M \equiv_p \frac{v}{u^a}$

1. (3 point) Soit $a = 2$ et $(p, g) = (5, 3)$, calculer h et déchiffré le message $c = (4, 2)$.
2. (2 points) Le nombre aléatoire $r = 2$ a servi à calculer le message c. Vérifier que le chiffré du message trouvé à la question précédente correspond bien à c.
3. (2 point) Rapeler ce qu'est le problème du logarithme discret.
4. (5 points) Montrer que si l'on sait résoudre le logarithme discrét alors on sait déchiffremt le chiffrement d'Elgamal.

Exercise 5 (Chiffrement de Churchyard (10 points))

- **Histoire:**
  - Ce message chiffré est gravé sur une tombe dans le cimetière de Trinity Churchyard (New York) depuis 1794. Of course le texte chiffré est écrit en anglais.
  - Il fut déchiffré en 1896.
- **Questions:**
  1. (6 points) En utilisant l'astuce (hint en anglais) retrouvez le message original ?
  2. (4 points) Comment fonctionne ce chiffrement ?
- Hint : TIC TAC TOE =