Examen : Introduction à la sécruité

Date: 17.10.2014
1h00, 60 points

- Seul une feuille de note personnelle manuscrite A4 recto verso est autorisée.
- Les points des exercices correspondent au temps en minute nécessaires pour les résoudre.

Exercise 1 (Questions de cours (30 points))

1. (9 points) Expliquer ce qu'est :
   - un chiffrement à clef publique
   - un chiffrement à clefs secrètes.
   - une fonction de hachage
2. (3 points) Citer deux exemples de :
   - chiffrement à clef publique
   - chiffrement à clefs secrètes.
   - fonction de hachage
3. (6 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 un exemple d'attaque par canaux cachés, et une contremesure pour l'attaque décrite.
5. (3 points) Que signifie les acronymes AES, DES, OTP, MAC, RSA et CAIN.
6. (5 points) Expliquer pourquoi le chiffrement RSA n'est pas IND-CPA.

Exercise 2 (Chiffrement de Bellare-Rogaway et Pointcheval (10 points))

Voici deux chiffrements à clef publique, où H et G sont deux fonctions de hachage publiques, r un nombre aléatoire, $\oplus$ dénote le ou-exclusif, $a||b$ dénote la concaténation des messages a et b, et f la fonction de chiffrement RSA. Les chiffrés du message x sont donnés par les deux formules suivantes:

- $f(r)||(x \oplus G(r))||H(x||r)$,
- $f(r)||H(x||s)||[(x||s) \oplus G(r)]$.

1. (8 points) Connaissant la fonction de déchiffrement de RSA notée f^{-1}, telle que $f^{-1}(f(y)) = y$, donner les deux algorithmes de déchiffrement associés à ces chiffrements.
2. (2 points) A quoi sert les messages $H(x||r)$ et $H(x||s)$.

Exercise 3 (E-exam (20 points))
Cet exercice porte sur les examen-electronqiues (e-exam)

1. (2 points) Identifier les acteurs d'un système d'e-exam.
2. (6 points) Expliquer 6 propriétés que doit assurer un tel système.
3. Considérons le système d'e-exam naïf suivant :
   - Le jour de l'e-exam chaque étudiant s'identifie sur un serveur avec son login et mot de passe, afin de récupérer au format pdf un sujet qui est unique pour chaque élève.
   - Suite à sa connexion, l'étudiant a 2h00 pour envoyer par email au professeur sa solution.
   - Le professeur corrige les copies et publie sur une page web publique de l'université la liste des noms des candidats et leurs notes.
4. (6 points) Donner 3 attaques pour 3 propriétés différentes sur ce protocole.
5. (6 points) Proposer des moyens permettant d'empêcher individuellement les attaques données à la question précédente.