2013 – 2014

Filière	Master 2 GIL
Épreuve	Applications Web et sécurité
Durée	2 heures
Documents autorisés	Aucun

Exercice 1 (10 points)

1. Quel est principe du chiffrement `One-Time Pad` ? Donnez ses avantages et ses inconvénients.
2. À quel type de chiffrement appartient le DES ? Quelle attaque a remis principalement en cause le DES ? Quel est son remplaçant aujourd'hui ?
3. Citez deux problèmes mathématiques difficiles utilisés pour construire des systèmes de chiffrement. Donnez un exemple de système pour chaque problème.
4. Que signifie pour un système cryptographique d'avoir κ bits de sécurité ?
5. Que signifie pour système de chiffrement d'être *hybride* ? Pourquoi existe-t-il ? Donnez un exemple de votre choix.
6. Quel est le but du protocole de Diffie-Hellman ? Rappelez son principe.
7. Donnez la définition d'une fonction à sens unique ? Sait-on en construire (si oui, donnez alors un exemple de fonction) ?
8. Quelles sont les principales méthodes actuelles pour authentifier un individu ?
9. Que signifie et pourquoi utilise-t-on la *certification* de clef publique ?
10. On imagine qu'une banque souhaite proposer une application web qui permette à ses clients de gérer leur compte courant au moyen d'un navigateur. Dîtes quelles sont les contraintes sécuritaires que l'application doit satisfaire ?

Exercice 2 (2 points) Rappeler les paramètres du système de chiffrement RSA(n,e). On suppose que le même message m est chiffré deux fois (pour deux personnes différentes) avec les clefs (n, e_1) et (n, e_2). Les chiffrés sont respectivement c_1 et c_2. On suppose de plus que le $\text{PGCD}(e_1, e_2) = 1$.

1. Montrer que l'on peut retrouver m à partir c_1 et c_2.
2. Quelles solutions préconisez-vous pour éviter ce genre d'attaque ?
3. Appliquer cette attaque lorsque les clefs RSA sont (493,3) et (493,5), et les chiffrés sont respectivement 293 et 421.

Exercice 3 (3 points) On suppose que l'on essaye d'améliorer la sécurité d'un système de chiffrement *symétrique* $(f_K)_{K\in\mathcal{K}}$ (on peut penser au DES) avec $f_K : \{0,1\}^n \to \{0,1\}^n$ dont les clés trop courtes n'interdisent pas une recherche exhaustive en chiffrant deux fois :

$$M \longmapsto C = f_{K_2}(f_{K_1}(M)).$$

1. Quelle est la taille de la nouvelle clé ?
2. On considère l'attaque suivante : Oscar connaît M et $C = f_{K_2}(f_{K_1}(M))$ et crée deux listes

$$\mathcal{L}_M = (f_K(M))_{K\in\mathcal{K}} \qquad \text{et} \qquad \mathcal{L}_C = (f_K^{-1}(C))_{K\in\mathcal{K}}$$

   Dites quel est le type de cette attaque, et ce que doit rechercher Oscar dans ces listes.
3. Pouvez-vous donner la complexité de cette attaque *i.e.* le nombre de comparaisons nécessaires (*Indic.* Les listes étant triées $\rightsquigarrow n \times \#\mathcal{K}$) ?

Exercice 4 (5 points) Dans un protocole d'identification, une entité P que l'on appelle *prouveur* doit prouver son identité à une entité V que l'on appelle *vérifieur*. P choisit un secret s et publie $I = \alpha^s \mod p$ où α est un générateur de $'\mathbb{Z}_p^*$ et p un nombre premier. Ces données sont publiques et on suppose que I identifie P. L'objectif du protocole suivant est de prouver que P connaît le secret s sans le révéler à V :

i. (**Engagement**) : P choisit $r \mod (p-1)$ aléatoire, calcule $R = \alpha^r \mod p$ et communique R à V

ii. (**Défi**) : V choisit un bit aléatoire $\varepsilon = 0, 1$ et le communique à P

iii. (**Réponse**) : P donne x à V où :
— $x = r \mod (p-1)$ si $\varepsilon = 0$
— $x = (r+s) \mod (p-1)$ si $\varepsilon = 1$

iv. (**Vérification**) : V calcule $X = \alpha^x \mod p$ et vérifie que $R = X$ quand $\varepsilon = 0$ et $X = R \times I$ quand $\varepsilon = 1$.

Un attaquant P^* cherche à se faire passer pour P auprès de V sans connaître s.

1. Sur quel problème repose la sécurité de ce protocole ?
2. Montrer que si P^* choisit $r \mod (p-1)$ comme engagement, il ne peut alors répondre correctement que si $\varepsilon = 0$.
3. Montrer que si dans la phase d'engagement P^* tire $r \mod (p-1)$ aléatoire et envoie $RI^{-1} \mod (p-1)$, il peut répondre correctement uniquement quand $\varepsilon = 1$.
4. En déduire que si V répète k fois le protocole, P^* se fait passer pour P avec une probabilité de $\frac{1}{2^k}$.
5. Pourquoi ce protocole est à divulgation nulle de connaissance ?