2012 – 2013

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

Exercice 1

1. Résumez en termes modernes les principes de Kerckhoff.
2. Dîtes, en donnant à chaque fois un exemple de votre choix, quel type de primitive cryptographique assure : a) la confidentialité b) l'authentification c) l'intégrité.
3. Quel est principe du chiffrement `One-Time Pad` ? Donnez ses avantages et ses inconvénients.
4. Définissez la notion d'*attaquant* en cryptographie.
5. Citez deux problèmes mathématiques difficiles utilisés pour construire des cryptosystèmes.
6. Donnez la définition d'une fonction à sens unique à trappe. Expliquez comment une fonction à sens unique à trappe permet de construire des systèmes asymétriques.
7. À quelle famille de chiffrement appartient le DES ? Quelle attaque a remis principalement en cause le DES ? Quel est son remplaçant aujourd'hui ?
8. Que signifie pour un système cryptographique d'avoir κ bits de sécurité ?
9. Donnez le principe de l'attaque de l'*intrus au milieu* (*Man-in-the-Middle Attack*). Quelle solution cryptographique peut empêcher cette attaque ?
10. Quel est le rôle d'un `Message Authentication Code` (MAC) ? Pourquoi ne peut-il pas assurer la non-répudiation ?

Exercice 2 On considère le scénario suivant : Bob publie sa clef publique RSA notée (n, e). Il chiffre un message M pour obtenir $C = M^e \mod n$. Oscar intercepte C, tire un nombre aléatoire r et demande à Bob de déchiffrer le message $C' = r^e C \mod n$.

1. Dîtes pourquoi Oscar peut retrouver M.
2. À quelle catégorie d'attaque appartient ce scénario ?
3. Que faudrait-il faire pour l'éviter ?

Exercice 3

1. Deux entités A et B souhaitent partager un secret (ou une clef) K. Proposez au moins deux protocoles de votre choix qui accomplissent cet objectif.
2. On considère le protocole d'échange de clefs suivants entre A et B. Dans la suite, on note $\oplus$ le ou exclusif bit à bit.
   (a) A tire aléatoirement deux suites de bits K et a de même longueur, calcule $k = K \oplus a$ et envoie k à B
   (b) B tire aléatoirement b, calcule $\ell = k \oplus b$ et envoie ℓ à A
   (c) A calcule $c = \ell \oplus a$ et envoie c à B
3. Expliquez ce que doit faire B pour récupérer K.
4. Dîtes ce que l'espion Oscar voit passer entre A et B durant ce protocole. En déduire une attaque.

Exercice 4 Le facteur de travail d'un algorithme est le nombre d'instructions élémentaires nécessaires pour son exécution. Le facteur de travail d'un algorithme optimisé pour tester une clef de 128 bits de l'algorithme AES est d'environ 1200 instructions élémentaires. On dispose d'un couple clair/chiffré connu et on désire retrouver la clé utilisée par force brute en testant toutes les clefs les unes après les autres.

1. La puissance d'une machine est le nombre d'instructions qu'elle exécute par unité de temps. La puissance d'un PC (2012) est d'environ 100 000 Mips (Millions d'instructions par seconde). En combien de temps une machine de 100 000 Mips teste-t-elle une clef ?
2. Combien y-a-t-il de clés possibles ? Quel est le nombre moyen de clefs à tester avant de trouver la bonne ?
3. Quel est le facteur de travail moyen (en Mips $\times$ années) pour trouver la clef ?
4. A quel temps moyen de calcul cela corresponf-il si on suppose que le milliard de PC de l'Internet est mobilisé ?