Master SSI 2016 - 2017

BCS **Examen**

Toutes les réponses doivent être justifiées. N'hésitez pas à passer des questions, quitte à y revenir ensuite.

Exercice 1 - Questions de Cours

1. Expliquer ce qu'est un chiffrement symétrique et donner un exemple. Quelle taille de clé est recommandée ?
2. Expliquer ce qu'est un chiffrement à clé publique et donner un exemple. Quelle taille de clé est recommandée ?
3. Donner les propriétés que doit satisfaire une fonction de hachage cryptographique. Quelle taille minimum est recommandée pour l'empreinte ?
4. Quel est le principe du chiffrement hybride ?
5. Quand peut-on dire qu'un chiffrement est sûr ?
6. Pour générer des clés RSA il est nécessaire de générer de grands nombres premiers. Donner une façon de le faire et expliquer les limitations.
7. Qu'apporte le chiffrement authentifié par rapport au chiffrement classique ? Donner une méthode pour en construire un.
8. Existe-t-il un chiffrement à la sécurité parfaite ?
9. Qu'est-ce que l'attaque *CBC-Padding Oracle* ? Quel leçon en tirer ?

Exercice 2 - Serveur de Stockage Sécurisé

Vous disposez d'un serveur en ligne exposé sur l'Internet. C'est un serveur ayant une bonne puissance de calcul qui réalise des calculs assez lourds et génère un volume important de donnée. Le stockage sur ce serveur est assez cher. Pour cette raison, vous devez régulièrement faire des copies de vos résultats sur un support de stockage en ligne beaucoup moins onéreux. La bande passante dont vous disposez ne vous permet pas de rapatrier directement ces données chez vous. Au total, vous disposez donc de trois machines : votre serveur de calcul, qui est assez sûr mais dispose de peu de stockage, un espace de stockage en ligne important mais peu sûr, et votre machine à la maison.

1. Quels mécanismes cryptographiques utiliseriez-vous pour protéger les données générées ?
2. Comment distribueriez-vous les clés ?

Exercice 3 - RSA

Soit (e, N), (d, p, q) une paire de clés RSA.

1. Donner les relations entre e, N, d, p et q.
2. Déterminer le secret d correspondant à $N = 55$ et $e = 3$. Chiffrer 7 avec la clé publique.

3. **On suppose que si $d^4 \leq N$ alors on peut retrouver d à partir de e et N.** Le but de l'exercice est d'insérer une trappe dans la génération de p et q, utilisant cette propriété. On considère l'algorithme suivant :

Algorithm 1: RSA Key

Soit M un nombre constant, paire et de n bits, fixé dans le programme;
Générer un nombre premier p de $n/2$ bits;
Générer un nombre premier q de $n/2$ bits;
$N \longleftarrow \ldots$;
repeat
  repeat
    Générer un nombre d' tel que $d'^4 < N$;
  until $pgcd(d', \varphi(N)) = 1$;
  Trouver e' tel que (e', N), (d', p, q) soit une paire de clés RSA;
  $e \longleftarrow e' + M$;
until $pgcd(e, \varphi(N)) = 1$;
Trouver d tel que (e, N), (d, p, q) soit une paire de clés RSA;
return (e, N), (d, p, q)

   a) Est-ce que la paire de clés produite par l'algorithme vérifie $d^4 < N$?
   b) Indiquez comment l'auteur de ce programme peut retrouver la clé privée en connaissant la clé publique.

Exercice 4 - Construction de MAC

Soit $M = M_1||M_2||\ldots||M_t$ un message de t blocs de taille n. On cherche à construire un algorithme de MAC pour de tels messages.

1. Rappeler la construction de Merkle-Damgard d'une fonction de hachage h à partir d'une fonction de compression f.
2. Soit h une telle fonction de hachage. On définit $\text{MAC}_k(M) = h(k||M)$.
   a) Que doit satisfaire un MAC sûr ?
   b) Montrer que ce MAC n'est pas sécurisé, *i.e.* étant donné un couple valide (M, H), on peut facilement construire un autre couple (M', H') sans connaitre la clé k. (Pour simplifier, on supposera que la clé et les blocs de messages ont la même longueur).
3. Qu'en est-il si $\text{MAC}_k(M) = h(M||k)$?
4. Soit E_k un chiffrement symétrique par blocs de taille n et h une fonction de hachage dont la sortie est également de taille n. On définit $\text{MAC}_k(M)$ par :
   — Pour tout message M de taille $N > n$, $\text{MAC}_k(M) = E_k(h(M))$
   — Pour tout message de taille exactement n, $\text{MAC}_k(M) = E_k(M)$
   Montrer que ce MAC n'est pas sécurisé.

Exercice 5 - FEAL

FEAL-4 est un algorithme de chiffrement par bloc qui utilise des clés de 64 bits pour chiffrer des blocs de 64 bits. Après une procédure de diversification de clé, la clé K produit deux sous-clés de 64 bits K_0 et K_5 et quatre sous-clés de 16 bits K_1, K_2, K_3 et K_4. La fonction de tour F utilise deux S-boîtes S_0 et S_1 définies par

$$S_i(x, y) = (x + y + i \mod 256) \lll 2,\ i \in \{0, 1\}$$

En utilisant une clé de tour de 16 bits K_i décomposée en deux octets $K_i = (K_i^0, K_i^1)$, la fonction F_{K_i} prenant en entrée 32 bits décomposés en quatre octets $X_i = (x_i^0, x_i^1, x_i^2, x_i^3)$ calcule

$$u_i = S_1(x_i^0 \oplus x_i^1 \oplus K_i^0, x_i^2 \oplus x_i^3 \oplus K_i^1), \;\; v_i = S_0(x_i^2 \oplus x_i^3 \oplus K_i^1, u_i)$$

puis retourne $F_{K_i} = (S_0(x_i^0, u_i), u_i, v_i, S_1(x_i^3, v_i))$.

1. Montrer que pour tout couple d'octets (x, y), on a $S_0(x \oplus \mathsf{80}, y) = S_0(x, y) \oplus \mathsf{02}$.
2. Soient X_0 un mot de 64 bits et $Y_0 = X_0 \oplus (\mathsf{80\ 80\ 00\ 00\ 00\ 00\ 00\ 00})$. On note X_2 et Y_2 leurs images après 2 tours de chiffrement avec une clé arbitraire. Montrer que

$$X_2 \oplus Y_2 = (\mathsf{02\ 00\ 00\ 00\ 80\ 80\ 00\ 00}).$$

3. En déduire une relation liant les chiffrés de deux messages dont la différence est égale à

$$(\mathsf{80\ 80\ 00\ 00\ 00\ 00\ 00\ 00})$$

   qui ne dépend que de la valeur de $K_5^R \oplus (0, K_4^0, K_4^1, 0)$.
4. *(bonus)* Proposer une attaque contre le chiffrement FEAL utilisant seulement deux clairs choisis permettant de retrouver la valeur de $K_5^R \oplus (0, K_4^0, K_4^1, 0)$.
5. *(bonus)* En supposant connue la valeur de $K_5^R \oplus (0, K_4^0, K_4^1, 0)$ et en utilisant une propriété différentielle sur 1 tour, proposer une attaque à deux clairs choisis permettant de retrouver la valeur de $K_5^L \oplus (0, K_3^0, K_3^1, 0)$.
6. *(bonus)* Proposer une attaque à huit clairs choisis permettant de retrouver la clé secrète.