Master – 1ère année

Cryptographie – Contrôle continu

27 novembre 2018

Consignes :

- **Durée : 1h30.**
- **Documents interdits. Aucun accès à une calculatrice, un téléphone portable, un smartphone, ou tout autre dispositif électronique, connectable ou non.**

<u>Exercice 1</u> (2 points)

1. Comment est défini l'algorithme one-time-pad ?
2. Quel niveau de sécurité permet-il d'obtenir ? Expliquer.

<u>Exercice 2</u> (3 points)

1. Quelle est la taille de la clé de l'algorithme DES ? Cette taille est-elle suffisante ? Expliquer.
2. Vous recevez un message chiffré y de 64 bits. Tout ce que vous savez est que c'est le résultat du chiffrement d'un certain message x (que vous ne connaissez pas) par l'algorithme DES. Sachant cela, combien y a-t-il (au maximum) de possibilités pour le message x ? Expliquer.
3. Même question en remplaçant le DES par le Triple-DES.

<u>Exercice 3</u> (3 points)

1. Rappeler comment fonctionne le mode de chiffrement CBC.
2. Expliquer quel est le rôle de la "valeur initiale" IV.
3. Montrer que, dans ce mode CBC, si un attaquant modifie <u>un</u> bloc du chiffré, alors au plus <u>deux</u> blocs du clair sont modifiés.

<u>Exercice 4</u> (4 points)

1. Quelles sont les tailles de l'entrée, de la sortie et de la clé dans l'algorithme AES ? Combien y a-t-il de tours ?
2. Rappeler comment est défini le produit de deux octets dans l'algorithme AES.
   [Rappel : le polynôme $X^8 + X^4 + X^3 + X + 1$ intervient dans la définition.]
3. Expliquer pourquoi tout octet non nul possède un inverse.
4. Calculer $\{B3\} \times \{97\}$.

TSVP

Exercice 5 (4 points)

1. Rappeler la définition d'une fonction à sens unique, d'une fonction à collisions faibles difficiles, et d'une fonction à collisions fortes difficiles.

2. Que dit le paradoxe des anniversaires ? Donner le plus de détails que vous pouvez.

3. Quelle condition nécessaire cela donne-t-il sur la valeur de ℓ pour qu'une fonction $f : \{0,1\}^* \longrightarrow \{0,1\}^\ell$ soit à collisions fortes difficiles ?

4. Soit $h : \{0,1\}^* \longrightarrow \{0,1\}^n$ une fonction de hachage (qui est donc en particulier à collisions faibles difficiles, et à collisions fortes difficiles). Soit $h' : \{0,1\}^* \longrightarrow \{0,1\}^{n+1}$ définie par :

$$h'(x) = \begin{cases} 0||x & \text{si } x \in \{0,1\}^n \\ 1||h(x) & \text{sinon} \end{cases}$$

   Montrer que h' n'est pas à sens unique, mais est encore à collisions faibles difficiles et à collisions fortes difficiles

Exercice 6 (4 points)

Soit d un entier. On définit le *chiffrement de Hill* de la façon suivante. L'ensemble des messages clairs possibles est $(\mathbb{Z}/26\mathbb{Z})^d$, c'est-à-dire que les messages sont des chaînes de d caractères alphabétiques encodés comme des éléments de $\mathbb{Z}/26\mathbb{Z}$. L'espace des clés est l'ensemble des matrices $d \times d$ inversibles sur $\mathbb{Z}/26\mathbb{Z}$. Étant donné une clé K et un message X, le chiffrement de X avec la clé K est $E_K(X) = K \times X$, toutes les opérations s'effectuant modulo 26.

1. Expliquer comment s'effectue le déchiffrement

2. Proposer une attaque à clair *choisi*, qui – au moyen de d messages clairs choisis – peut retrouver la clé K en complexité $\mathcal{O}(d^2)$. Justifier la complexité.

3. Étant donnés d couples (clair/chiffré) connus (et non choisis), proposer une attaque pour retrouver la clé K.

4. Montrer que dans la question précédente, on peut en général obtenir une attaque en complexité $\mathcal{O}(d^4)$.