République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira de Bejaia
Faculté des Sciences Exactes
Département d'Informatique

Module : Sécurité

Option : Génie Logiciel

Série TD N°4

Exercice 1. (Rappel du cours)

a) A quoi servent les modes de chiffrement ?

b) Donnez les équations de récurrence pour le chiffrement et le déchiffrement des modes suivant : ECB, CBC, OFB ?

c) Qu'est ce que c'est qu'une fonction de hachage ?

d) Quelles sont les propriétés d'une fonction de hachage ?

e) Que signifie collision ?

Exercice 2. (DES avec mode de chiffrement ECB)

Soit $M = \|_{i=1}^{n} m_i$ et $C = \|_{i=1}^{n} c_i$, si on suppose que le chiffrement est fait avec le mode ECB : $\forall 1 \leq i \leq n\ c_i = DES(m_i, K)$.

Montrez que ce mode de chiffrement est vulnérable à une attaque de rejoue (utilisation de blocs déjà interceptés). Prenez inspiration de la solution à l'exercice 2 de la série de TD 2.

Exercice 3. (Fonctions de Hachage)

Soit $g : \{0,1\}^n \to \{0,1\}^m (n > m)$

$x \mapsto g(x) = y$

Algorithm 1: Fonction de hachage g

Entrée: X
/* X est de taille n */
Sortie: $Y = g(X)$
/* Y est de taille m */
if $\| X \| < m$ **then**
  $Y \leftarrow X.suite\_bit(0, m - \| X \|)$ /* Concaténer à X $(m - \| X \|)$ 0 pour avoir Y en m bits */
end
else
  $Y \leftarrow premier\_bit(X, m)$ /* prendre les m premier bits de X */
end
retourner $image\_miroir(Y)$ // image_miroir donne l'image miroir d'une suite de bits

1. Montrez que g est facile à calculer (**FC**).
2. Montrez que g est de compression (**CP**).
3. Montrez que g n'est pas résistantes aux collisions (**RC**).

Exercice 4. (Fonctions de Hachage)

On suppose que **Alice** envoie à **Bob** un message de la forme :

$Y = h(k_2) \parallel E_{k_1}(k_2 \parallel E_{k_2}(x \parallel h(x))$.

h fonction de hachage, E algorithme de chiffrement symétrique, k_1 et k_2 clés partagées entre **Alice** et **Bob**.

1. Donnez le détail de ce protocole (suite d'étapes faite par **Alice** et**Bob**) ?
2. Quelles sont les objectifs de la sécurité qui sont vérifiés dans la suite d'étapes décrites en (1) ?