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

27/02/2018

Module : Sécurité
Niveau : Master1 ASR-GL (2017-2018)

EMD N°1, Durée : 1h30mn

Exercice 1 (6 points)

1. Expliquer pourquoi on signe le haché de l'information à communiquer et non l'information elle-même ?
2. Quel est le type de chiffrement pour lequel sont définis les modes de chiffrement ?
3. Quel est le but de définir des protocoles d'application pour les chiffrements Asymétriques.
4. Sur quoi repose la sécurité du crypto-système RSA ?
5. Quel est le rôle d'une Autorités de Certification (AC) ?

Exercice 2 (8 points)

1) Soit le schéma de chiffrement **DES** illustré dans la **figure 1**.

a) Donner la taille des éléments **P**, **C**, L_i, R_i et K_j (i=0..16 et j=1..16).

a) Dans un chiffrement DES, si on a l'égalité entre les sous clés comme suit : k1=k16, k2=k15, k3=k14, k4=k13, k5=k12, k6=k11, k7=k10, k8=k9 ; quel est le problème qu'on va avoir lors des opérations de chiffrements multiples ? ce problème est dû à quoi ?

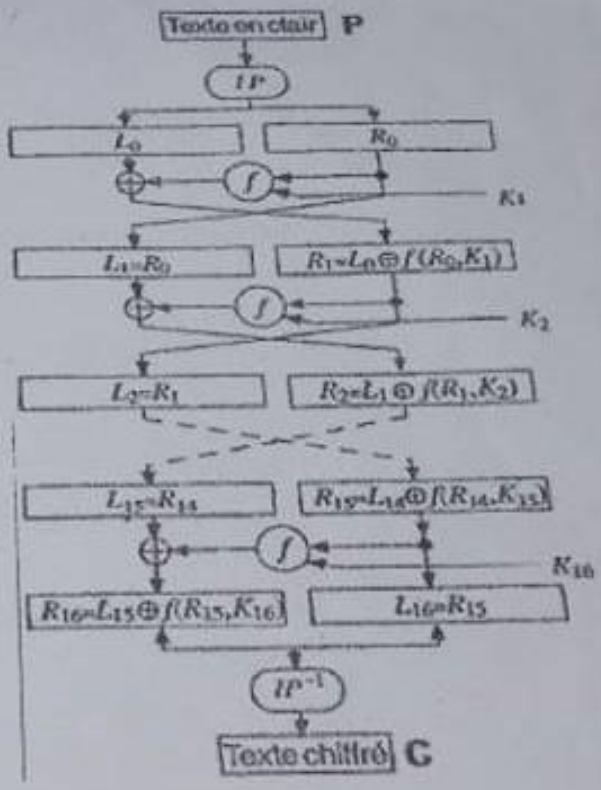


Figure 1. Chiffrement DES

2) Soit le mode de chiffrement CBC de la **figure 2**.

a) Donner ses formules de chiffrement et celles de déchiffrement.

b) Combien de blocs seront mal déchiffrés si un bloc C_i a été altéré durant la transmission ?

c) Proposer une modification sur le schéma CBC, pour ne pas avoir à définir la fonction inverse de E_k lors du processus de Déchiffrement.

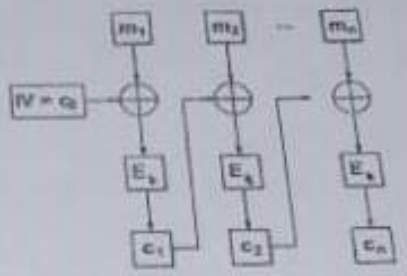


Figure 2. Mode CBC

Exercice 3 (6 points)

Soit $h_1 : \{0,1\}^* \to \{0,1\}^n$ une fonction **qui n'est pas** résistante aux collisions.

Soit $h_2 : \{0,1\}^* \to \{0,1\}^n$ une fonction **qui est** résistante aux collisions.

Soit maintenant les définitions suivantes :

1- $H_{h1,h2}(x) = h_1(x) \| h_2(x)$, $x \in \{0,1\}^*$;

2- $H_{h1,h2}(x) = h_1(h_2(x)) \| h_2(h_1(x))$, $x \in \{0,1\}^*$.

3- $H_{h1,h2}(x) = h_1(h_2(x) \| x) \| h_2(h_1(x) \| x)$, $x \in \{0,1\}^*$.

Où $H_{h1,h2}$ est une fonction de hachage qui exploite h_1 et h_2. $\|$ indique une concaténation de bits.

Discuter (avec démonstration) les définitions ci-dessus en matière de résistance aux collisions.

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

Module : Sécurité **27/02/2018**

Niveau : Master1 ASR-GL (2017-2018)

Correction de l'EMD N°1

Exercice 1 (6 points)

1. Expliquer pourquoi on signe le haché de l'information à communiquer et non l'information elle-même ?

   *Pour des raisons de **sécurité** et d'**efficacité**.*

2. Quel est le type de chiffrement pour lequel sont définis les modes de chiffrement ?

   *Le chiffrement **symétrique** par **bloc***

3. Quel est le but de définir des protocoles d'application pour les chiffrements Asymétriques.
   Permettent de définir la façon dont le chiffrement Asymétrique est appliqué. Par exemple la taille des blocs à chiffrer…

4. Sur quoi repose la sécurité du crypto-système RSA ?

   La difficulté de factoriser un nombre entier en produit de deux nombre premier.

5. Quel est le rôle d'une Autorités de Certification (AC) ?

   ***Atteste** l'appartenance d'une **clé publique** à une **entité** par un **certificat électronique**.*

Exercice 2 (8 points)

1) Soit le schéma de chiffrement **DES** illustré dans la **figure 1**.

a) Donner la taille des éléments **P**=*64bits*, **C**=*64bits*, $\mathbf{L_i}$=*32bits*, $\mathbf{R_i}$=*32bits* et $\mathbf{K_j}$=*48 bits*(i=0..16 et j=1..16).

a) Dans un chiffrement DES, si on a l'égalité entre les sous clés comme suit : k1=k16, k2=k15, k3=k14, k4=k13, k5=k12, k6=k11, k7=k10, k8=k9 ; quel est le problème qu'on va avoir lors des opérations de chiffrements multiples ? ce problème est dû à quoi ?

Le chiffrement d'un résultat de chiffrement nous donnera le texte en clair. Car le processus de déchiffrement consiste à appliquer le même schéma de chiffrement avec l'ordre des lés inversé, et comme l'ordre k1...k16= k16..k1, le fait de chiffrer deux fois un message reproduira le même message en clair ($DES_k(DES_k(m)) = m$)

2) Soit le mode de chiffrement CBC de la **figure 2**.

a) Donner ses formules de chiffrement et celles de déchiffrement.

Figure 1. Chiffrement DES

$c_i = E_k(m_i \oplus c_{i-1})$ *Chiffrement i=1..n*

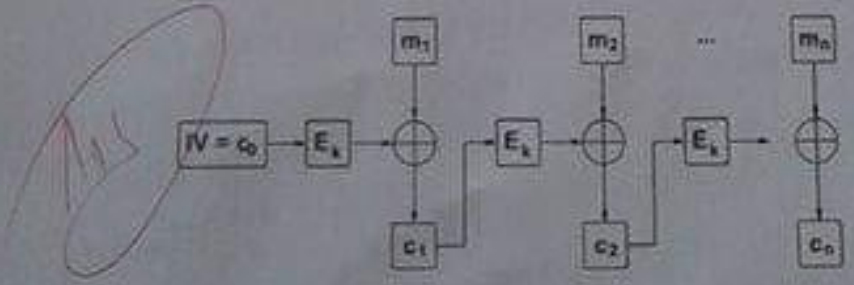
Soit $E_k^{-1}()$ *la fonction inverse de* $E_k()$. *Le Déchiffrement sera :* $m_i = c_{i-1} \oplus E_k^{-1}(c_i)$

b) Combien de blocs seront mal déchiffrés si un bloc C_i a été altéré durant la transmission ?

Figure 2. Mode CBC

(≠ n (2 blocs)
i=n (1 bloc)

c) Proposer une modification sur le schéma CBC, pour ne pas avoir à définir la fonction inverse de E_K lors du processus de Déchiffrement.



Le mode **CFB** : *Chiffrement :* $c_i = m_i \oplus E_k(c_{i-1})$; *Déchiffrement :* $m_i = c_i \oplus E_k(c_{i-1})$

Exercice 3 (4 points)

Soit $h_1 : \{0,1\}^* \to \{0,1\}^*$ une fonction **qui n'est pas** résistante aux collisions.
Soit $h_2 : \{0,1\}^* \to \{0,1\}^*$ une fonction **qui est** résistante aux collisions.
Soit maintenant les définitions suivantes :

Trouver une collision revient à trouver facilement $x_1, x_2 \in \{0,1\}^*, x_1 \neq x_2$ *et* $H_{h1,h2}(x_1) = H_{h1,h2}(x_2)$

1- $H_{h1,h2}(x) = h_1(x) \| h_2(x)$, $x \in \{0,1\}^*$;

$H_{h1,h2}(x_1) = H_{h1,h2}(x_2) \Rightarrow h_1(x_1) \| h_2(x_1) = h_1(x_2) \| h_2(x_2)$
Il est facile de trouver $h_1(x_1) = h_1(x_2)$ *car elle ne résiste pas aux collisions, par contre on ne peut pas avoir* $h_2(x_1) = h_2(x_2)$ *car elle résiste aux collisions. Ce qui veut dire que* $H_{h1,h2}$ ***est résistante aux collisions.***

2- $H_{h1,h2}(x) = h_1(h_2(x)) \| h_2(h_1(x))$, $x \in \{0,1\}^*$;

$H_{h1,h2}(x_1) = H_{h1,h2}(x_2) \Rightarrow h_1(h_2(x_1)) \| h_2(h_1(x_1)) = h_1(h_2(x_2)) \| h_2(h_1(x_2))$
-Pour la partie $h_2(h_1(x_1)) = h_2(h_1(x_2))$ *Il est facile de trouver* $h_1(x_1) = h_1(x_2)$ *et par conséquent* $h_2(h_1(x_1)) = h_2(h_1(x_2))$.
-Pour la partie $h_1(h_2(x_1)) = h_1(h_2(x_2))$, *comme on a* $h_2(x_1) \neq h_2(x_2)$ *et* h_1 *ne résiste pas aux collisions on aura facilement* $h_1(h_2(x_1)) = h_1(h_2(x_2))$
Ce qui veut dire que $H_{h1,h2}$ ***ne résiste pas aux collisions.***

3- $H_{h1,h2}(x) = h_1(h_2(x) \| x) \| h_2(h_1(x) \| x)$, $x \in \{0,1\}^*$;

$H_{h1,h2}(x_1) = H_{h1,h2}(x_2) \Rightarrow h_1(h_2(x_1) \| x_1) \| h_2(h_1(x_1) \| x_1) = h_1(h_2(x_2) \| x_2) \| h_2(h_1(x_2) \| x_2)$
Supposons que $H_{h1,h2}$ *ne résistent pas aux collision, cela veut dire que pour la partie* $h_2(h_1(x_1) \| x_1) = h_2(h_1(x_2) \| x_2)$ *on a* $h_1(x_1) \| x_1 = h_1(x_2) \| x_2$ *comme* h_2 *résiste aux collisions et cela implique que* $h_1(x_1) = h_1(x_2)$ *...(1) et* $x_1 = x_2$ *...(2)*
(1) vérifié car h_1 *ne résiste pas aux collisions, mais (2) donne une contradiction avec la définition des collisions*$(x_1, x_2 \in \{0,1\}^*, x_1 \neq x_2)$
Ce qui veut dire que $H_{h1,h2}$ ***résiste aux collisions.***