Université Larbi Ben M'Hidi - Oum El Bouaghi
Faculté des Sciences Exactes et des Sciences de la Nature et de la Vie
Département de Mathématiques et Informatique

2019-2020

Sécurité Informatique

Matière :	*Niveau :*	*Examen :*
Sécurité Informatique	*1ère Année Master VA*	*Session Normale*
Documents non autorisés	*Durée : 01h 30mn*	*Calculatrice scientifique autorisée.*

Mercredi 05/02/2020

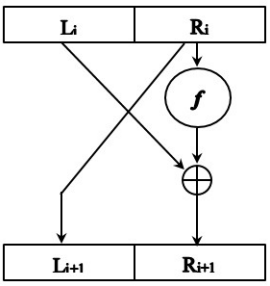
Répondre clairement et brièvement

Exercice 1 : 6 pts (Compréhension)

1) *Donnez deux (02) exemples de menaces non intentionnelles spécifiques à l'informatique ?*
2) *Donnez deux (02) exemples de menaces intentionnelles spécifiques à l'informatique ?*
3) *Quelles sont les différentes alternatives qu'on peut envisager face à un risque ?*
4) *Un groupe de 7 personnes veulent communiquer entre eux deux à deux de façon à assurer la confidentialité.*
   (a) *Quel est le nombre de clés nécessaires lorsqu'ils utilisent un système symétrique ?*
   (b) *Quel est le nombre de clés nécessaires lorsqu'ils utilisent un système asymétrique ?*

Exercice 2 : 6 pts (Schéma de Feistel)

Considérons un système de chiffrement simple qui repose sur le schéma de Feistel illustré par la figure ci-contre. Si ce système opère sur des blocs de 8 bits et et se sert de la fonction $f(b_1b_2b_3b_4) = b_2b_3b_4b_1$.



1) *Exprimez* L_1 *et* R_1 *en fonction de* L_0 *et* R_0.
2) *Exprimez* L_0 *et* R_0 *en fonction de* L_1 *et* R_1.
3) *Chiffrez le message clair* $m = 01101011$.
4) *Déchiffrez le cryptogramme* $c = 01101011$.

Considérons maintenant une amélioration de ce système qui consiste à utiliser un réseau de Feistel de deux étages au lieu d'un seul.

5) *Exprimez* L_2 *et* R_2 *en fonction de* L_0 *et* R_0.
6) *Exprimez* L_0 *et* R_0 *en fonction de* L_2 *et* R_2.

Exercice 3 : 8 pts (Système RSA)

Alice utilise un système RSA construit utilisant $p = 11$, $q = 17$.

1) *Sur quel principe est basée la sécurité du cryptosystème RSA ?*
2) *Quelles sont les valeurs de* n *et* $\phi(n)$ *?*
3) *Si Alice doit choisir la plus petite valeur valide qui sert comme exposant de chiffrement. Quelle est la valeur adéquate de* e *et celle de la clé publique à utiliser dans ce cas ?*
4) *Quelle sera sa clé privée correspondante ?*
5) *Bob veut transmrttre le message clair* $m = 13$ *à Alice, quel est le message chiffré* c *correspondant ?*
6) *Quel est le message clair* m *correspondant au message chiffré* $c = 21$ *?*

Remarque : $\forall m \in \mathbb{Z}_{187}^*, m^{81} \equiv m \mod 187$. *(Si* $PGCD(m, 187) = 1$ *alors* $m^{80} \equiv 1 \mod 187$.

Bon courage

Corrigé-type + Barème

Réponse à l'exercice 1

1. ***Exemples de menaces non intentionnelles (accidentelles) spécifiques à l'informatique :*** *pannes/dysfonctionnement du matériel, pannes/dysfonctionnement du logiciel de base, erreurs d'exploitation (oubli de sauvegardes, écrasement/suppression de fichiers, …), erreurs de manipulation des informations (erreurs de saisie/de transmission/d'utilisation, …), erreurs de conception/implémentation des applications, ….* 1.50

2. ***Exemples de menaces intentionnelles spécifiques à l'informatique :*** *modifications des logiciels (par les malwares ou non), détournements de logiciels (copies illégales), sabotage des informations, détournements des données (l'écoute sur le réseau à l'aide des sniffeurs, les indiscrétions, keyloggers, mouchards, …).* 1.50

3. *Face à un risque il est possible de :*
   - *Prendre le risque (ne rien faire).*
   - *Eviter le risque (éliminer toutes les vulnérabilités du système).*
   - *Eliminer le risuqe (agir sur les sources de menaces et les éliminer toutes).* 1.00
   - *Diminuer le risque (éliminer partiellement les vulnérabilités du système).*
   - *Partager le risque (payer un tiers pour rembourser les dégats en cas d'incidents comme l'assurance).*

4. *Un groupe de 7 personnes qui veulent communiquer entre eux deux à deux en assurant la confidentialité :*
   a) *Utilisant un système symétrique : chaque 2 personnes doivent partager une clé secrète ce qui donne pour n personnes $\frac{n(n-1)}{2}$ clés. Alors pour $n = 7$ nous aurons besoins de $\frac{7\times 6}{2} = 21$ clés secrètes.* 1.00
   b) *Utilisant un système asymétrique : chaque personne doit posséder une paire de clés (l'une privée et l'autre publique) ce qui donne pour n personnes $2n$ clés. Alors pour $n = 7$ nous aurons besoins de $2 \times 7 = 14$ clés secrètes.* 1.00

Réponse à l'exercice 2

1. *L_1 et R_1 en fonction de L_0 et R_0 :*

$$\begin{cases} L_1 = R_0 \\ R_1 = L_0 \oplus f(R_0) \end{cases}$$ 1.00

2. *L_0 et R_0 en fonction de L_1 et R_1 :*

$$\begin{cases} L_0 = R_1 \oplus f(L_1) \\ R_0 = L_1 \end{cases}$$ 1.00

3. $m = 01101011$, $L_0 = 0110$ *et* $R_0 = 1011$. *Ainsi :* $L_1 = 1011$ *et* $R_1 = 0110 \oplus f(1011) = 0110 \oplus 0111 = 0001$. *Donc* $\boxed{c = L_1||R_1 = 10110001}$. 1.00

4. $c = 01101011$, $L_1 = 0110$ *et* $R_1 = 1011$. *Ainsi :* $L_0 = 1011 \oplus f(0110) = 1011 \oplus 1100 = 0111$ *et* $R_0 = 0110$. *Donc* $\boxed{m = L_1||R_1 = 01110110}$. 1.00

Réseau de Feistel à 2 étages :

5. *L_2 et R_2 en fonction de L_0 et R_0 :*

$$\begin{cases} L_2 = R_1 = L_0 \oplus f(R_0) \\ R_2 = L_1 \oplus f(R_1) = R_0 \oplus f(L_0 \oplus f(R_0))) \end{cases}$$ 1.00

6. *L_0 et R_0 en fonction de L_2 et R_2 :*

$$\begin{cases} L_0 = R_1 \oplus f(L_1) = L_2 \oplus f(R_2 \oplus f(L_2)) \\ R_0 = L_1 = R_2 \oplus f(L_2) \end{cases}$$ 1.00

Réponse à l'exercice 3

1. *La sécurité du cryptosystème RSA est basée sur la difficulté de factorisation des grands nombres entiers (problème mathématique réputé difficile).* — 1.00

2. *Nous avons :* $n = p \times q \times r = 11 \times 17 = 187$. — 1.00

   $\varphi(n) = (p-1) \times (q-1) = 10 \times 16 = 160 = 2 \times 5 \times 2^4 = 2^5 \times 5$.

3. *La condition est que PGCD*$(e, \varphi(n)) = 1$. *D'après la factorisation de* $\varphi(n)$, *les valeurs* 1 *et* 2 *ne conviennent pas. Ainsi la valeur minimale valide est* $e = 3$.

   La clé publique est $(n, e) = (187,\ 3)$ — 1.00

4. *L'exposant de déchiffrement* d *doit vérifier* $e \times d \equiv 1 \mod \phi(n)$ *et en utilisant l'algorithme d'Euclide étendu, nous obtenons :* — 2.00

   $(1) \times 187 + (-53) \times 3 = 1$. *La clé privée est donc :* $d = -53 \mod 160 = 107$.

i	r_i	q_i	α_i	β_i
1	160	–	1	0
2	3	53	0	1
3	1	3	1	-53
4	0	–	–	–

5. $m = 13$ *et* $c = m^e \mod n = 13^3 \mod 187 = 2197 \mod 187$. *Ainsi* $c = 140$. — 1.50

6. $c = 21$ *et* $m = c^d \mod n \equiv 21^{107} \mod 187 \equiv 21^{81+26} \mod 187 \equiv 3^{27} \times 7^{27} \mod 187$ — 1.50

   $m = 75 \times 116 \mod 187 \equiv 8700 \mod 187$.

   Ainsi $m = 98$.