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 Avancée des Systèmes Informatiques

Matière :	***Niveau :***	***Examen :***
Sécurité Avancée des Systèmes Informatiques	*2ème Année Master AD*	*Session Normale*
Documents non autorisés	*Durée : 01h 30mn*	*Calculatrice scientifique autorisée.*

Samedi 01/02/2020

Répondre clairement et brièvement

Exercice 1 : 8 pts (Système RSA)

Alice utilise un système RSA construit utilisant $p = 13$, $q = 19$.

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* $m = 11$ *à Alice, quel est le message chiffré* c *correspondant ?*
6) *Quel est le message clair* m *correspondant au message chiffré* $c = 23$ *?*
7) *Considérons le cas où Bob possède le même module* n *que Alice, mais avec un exposant de chiffrement* $e' \neq e$ *et* $PGCD(e, e') = 1$. *Supposons que Alice et Bob chiffrent et s'échangent un même message* m *et que Eve intercepte les deux cryptogrammes* $c_A = m^e \mod n$ *et* $c_B = m^{e'} \mod n$, *qu'elle sait être deux chiffrements du même message* m.
   (a) *Montrez qu'Eve peut alors très facilement découvrir le message* m.
   (b) *Appliquez cette technique dans le cas où* $e' = 7$, $c_A = 16$ *et* $c_B = 61$.

Remarque 1 : $\forall m \in \mathbb{Z}_{247}^*, m^{37} \equiv m \mod 247$. *(Si* $PGCD(m, 247) = 1$ *alors* $m^{36} \equiv 1 \mod 247$.
Remarque 2 : 61 *est un nombre premier.*

Exercice 2 : 6 pts (Système El-Gamal)

Dans un système El Gamal $p = 41$ *et* $g = 6$. *Alice tire au hasard sa clé privée* $x = 14$.

1) *Sur quel principe est basée la sécurité du système El-Gamal ?*
2) *Est-il possible d'obtenir deux cryptogrammes différents pour le même message clair dans ce système ?*
3) *Quelle est la clé publique d'Alice ?*
4) *Chiffrez le message clair* $M = 13$ *si le tirage aléatoire donne* $k = 17$.
5) *Déchiffrez le cryptogramme* $C = (28, 12)$.

Exercice 3 : 6 pts (Modes d'opération)

Considérons un cryptosystème symétrique simple qui opère sur des blocs de 3 bits en effectuant une transposition avec la clé suivante : $k = (3, 1, 2)$.

1) *Chiffrez le message clair* $m = 101110111$ *en utilisant les modes ECB et mode CBC (*$IV = 011$*).*
2) *Déchiffrez le cryptgramme* $c = 111011101$ *obtenu avec le mode CBC (*$IV = 011$*).*
3) *Quels sont les avantages et les inconvénients du mode CBC par rapport au mode ECB ?*

Bon courage

Corrigé-type + Barème

Réponse à l'exercice 1

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

2. *Nous avons :* $n = p \times q \times r = 13 \times 19 = 247$. 1.00

   $\phi(n) = (p-1) \times (q-1) = 12 \times 18 = 216 = 2^3 \times 3^3$. 1.00

3. *La condition est que PGCD*$(e, \varphi(n)) = 1$. *D'après la factorisation de* $\varphi(n)$, *les valeurs* $1, 2, 3, 4$ *ne conviennent pas. Ainsi la valeur minimale valide est* $e = 5$.

   La clé publique est $(n, e) = (247,\ 5)$ 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 :*

   $(-1) \times 216 + (-43) \times 5 = 1$. *La clé privée est donc :* $d = -43 \mod 216 = 173 \mod 216$.

i	r_i	q_i	α_i	β_i
1	216	–	1	0
2	5	43	0	1
3	1	5	1	-43
4	0	–	–	–

   1.00

5. $m = 11$ *et* $c = m^e \mod n = 11^5 \mod 247 = 161051 \mod 247$. *Ainsi* $c = 7$. 1.00

6. $c = 23$ *et* $m = c^d \mod n \equiv 23^{173} \mod 247 \equiv 23^{36+36+36+36+29} \mod 247 \equiv 23^{29} \mod 247$

   $m = c^d \mod n \equiv 23^{16} \times 23^8 \times 23^4 \times 23 \mod 247 \equiv 120 \times 100 \times 237 \times 23 \mod 247 \equiv 65412000 \mod 247$.

   Ainsi $m = 225$ 1.00

7. *Alice et Bob ayant un module RSA commun* n. *Clé publique d'Alice* (n, e) *et la clé publique de Bob* (n, e') *avec* $PGCD(e, e') = 1$. *Eve intercepte* $c_A = m^e \mod n$ *et* $c_B = m^{e'} \mod n$.

   a) Du fait que Eve connait e *et* e', *elle procède à la résolution de l'équation* $\alpha e + \beta e' = 1$ *utilisant l'algorithme d'Euclide étendu. Elle calcule ensuite* $c_A^\alpha \times c_B^\beta \mod n = (m^e)^\alpha (m^{e'})^\beta \mod n = m^{\alpha e} m^{\beta e'} \mod n$. *Obtenant ainsi le message* m : $m^{\alpha e} m^{\beta e'} \mod n = m^{\alpha e + \beta e'} \mod n = m$ 1.00

   b) Application numérique : $e = 5$, $e' = 7$, $c_A = 16$ *et* $c_B = 61$ *La solution de l'équation* $7\alpha + 5\beta = 1$ *utilisant l'algorithme d'Euclide étendu donne* $\alpha = -2$ $\beta = 3$ $((-2)7 + (3)5 = 1)$.

i	r_i	q_i	α_i	β_i
1	7	–	1	0
2	5	1	0	1
3	2	2	1	-1
4	1	2	-2	3
5	0	–	–	–

   $m = 61^{-2} \times 16^3 \mod 247 = (61^{-1})^2 \times 16^3 \mod 247$. *Il nous faut calculer l'inverse de 61 dans* $\mathbb{Z}_{247}$, *ce qui revient à résoudre l'équation* $61 \times 61^{-1} \equiv 1 \mod 247$ *ou* $247\alpha + 61\beta = 1$, *utilisant l'algorithme d'Euclide étendu. Ainsi* $61^{-1} = 81$ *et* $m = 81^2 \times 16^3 \mod 247 = 6561 \times 4096 \mod 247$. *Donc* $m = 9$.

i	r_i	q_i	α_i	β_i
1	247	–	1	0
2	61	4	0	1
3	3	20	1	-4
4	1	3	-20	81
5	0	–	–	–

1.00

Réponse à l'exercice 2

1. *La sécurité du système El-Gamal est basée sur la* ***difficulté de calculer le logarithme discret.*** 1.00
2. *Ou, il est possible d'obtenir des cryptogrammes différents pour un même message clair parce que c'est un système probabiliste où l'opération de* ***chiffrement dépond d'un nombre aléatoire.*** 1.00
3. $h = g^x \mod p = 6^{14} \mod 41 = 21$. *Ainsi la clé publique d'Alice est* $\boxed{(p, g, h) = (41, 6, 21)}$ 1.00
4. $m = 13$, $c_1 = g^k \mod p = 6^{17} \mod 41 = 26$, $c_2 = m \times h^k \mod p = 13 \times 21^{17} \mod 41 = 22$. *Ainsi le cryptogramme correspondant au message clair* $m = 13$ *est* $\boxed{(c_1, c_2) = (26, 22)}$ 1.50 1.50
5. $c = (28, 12)$, $\alpha = p - 1 - x = 41 - 1 - 14 = 26$, $m = c_1^{\alpha}.c_2 \mod p = 28^{26} \times 12 \mod 41$. *Ainsi* $\boxed{m = 17}$.

Réponse à l'exercice 3

1. *Chiffrement :*
   - *Mode ECB :*
     $m = 101110111$
     $\boxed{c = 110011111}$. 1.25
   - *Mode CBC :*
     $m = 101110111$
     $IV = 011$
     $m_i \oplus c_{i-1} = 110101001$
     $\boxed{c = 011110100}$. 1.25
2. *Déchiffrement :*
   - *Mode CBC :*
     $c = 110011101$
     $IV = 011$
     $D(c_i) \oplus c_{i-1} = 111110011 \oplus 011111011$
     $\boxed{m = 100001000}$. 1.50
3. *Avantages/inconvénients du mode CBC par rapport au mode ECB :*
   - *Avantages du mode CBC par rapport au mode ECB :* 1.00
     - *Blocs identiques du texte clair ne donnent pas des blocs identiques dans le texte chiffré.*
     - *Un texte clair donne des cryptogrammes différents à chaque chiffrement (IV aléatoire).*
   - *Inconvénients du mode CBC par rapport au mode ECB :* 1.00
     - *Pas de parallélisation de l'opération de chiffrement.*
     - *Bloc IV supplémentaire nécessaire pour chiffrer et déchiffrer.*
     - *Une erreur de transmission d'un bit affecte non seulement le décodage du bloc correspondant, mais également le bloc suivant (propagation limitée)*