Université de La Manouba
Ecole Nationale des Sciences de l'Informatique

Section :

Module : **Sécurité Informatique**

Classe : **II3**

Session : Principale

A.U. : 2015/2016

Signatures des Surveillants

Nom : ……………………… Prénom :……………………..

N° CIN : ……………………………………………………

N° d'inscription : …………………………………………

Salle n° :………………… Place n° :…………………..

Signature de l'étudiant

✂- -

Note

Examen de : …………………………..

Documents non autorisés

Appréciations du correcteur

Exercice 1 : Etude du jeu de pile ou face en réseau

Alice et Bernard communiquent à distance au moyen d'un réseau non sécurisé. Ayant un conflit au sujet d'une décision, ils veulent s'en remettre au hasard pour la décision finale à la façon du jeu pile ou face. Pour cela ils doivent concevoir un protocole basé sur l'échange de messages asynchrones qui leur permette de jouer à pile ou face à distance. Pour remplacer le lancement de la pièce de monnaie, Alice tire un entier au hasard : Selon que l'entier est pair ou impair, on considère que la pièce est retombée côté pile ou côté face, respectivement. Pour remplacer le choix fait par Bernard pour deviner le côté visible de la pièce, Bernard doit tirer une valeur aléatoire $0 \le p \le 1$ au hasard : Si $p < 0.5$ alors Bernard a déclaré « pile », sinon, c'est « face ».

1. On cherche une solution au jeu de pile ou face en réseau.
   a. Nommer les 4 critères de sécurité usuels.

/1

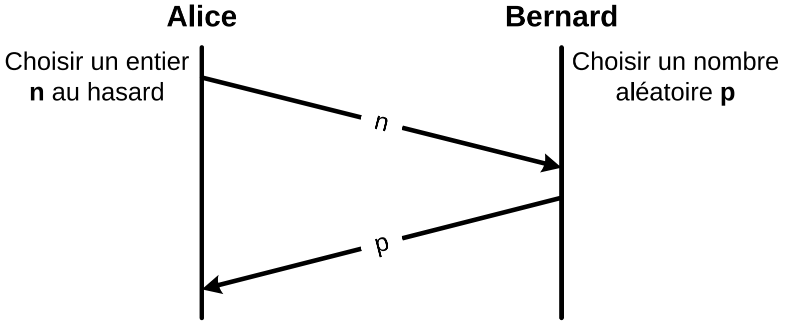
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………

   b. Est-ce possible d'assurer ces 4 critères de sécurité sans utiliser de fonctions cryptographiques ? Expliquer brièvement en considérant chaque critère à part.

/2

1.…………………………………………………………………………………………………
……………………………………………………………………………………………………
2.…………………………………………………………………………………………………
……………………………………………………………………………………………………
3.…………………………………………………………………………………………………
……………………………………………………………………………………………………
4.…………………………………………………………………………………………………
……………………………………………………………………………………………………

2. Une version de base du protocole pourrait être la suivante : Alice est la participante qui tire l'entier **n** au hasard et Bernard est le participant qui choisit pair ou impair (en choisissant le nombre aléatoire **p**). Alice et Bernard échangent ensuite en clair les valeurs générées. Suite à cet échange, les deux partenaires décident qui est gagnant.



Décision finale: Alice gagne si Bernard n'a pas deviné la parité. Sinon, c'est Bernard qui gagne.

Université de La Manouba
Ecole Nationale des Sciences de l'Informatique

Section :
Module : **Sécurité Informatique**
Classe : **II3**
Session : Principale

A.U. : 2015/2016

Signatures des Surveillants

Signature de l'étudiant

Nom : ……………………… Prénom :……………………..

N° CIN : …………………………………………………….

N° d'inscription : …………………………………………

Salle n° :…………………. Place n° :…………………..

a. Quelles sont les fraudes les plus évidentes de la part d'Alice, de Bernard ou d'un attaquant externe ?

/1,5

Alice :……………………………………………………………………………………………

……………………………………………………………………………………………………

Bernard :…………………………………………………………………………………………

……………………………………………………………………………………………………

Attaquant :………………………………………………………………………………………

……………………………………………………………………………………………………

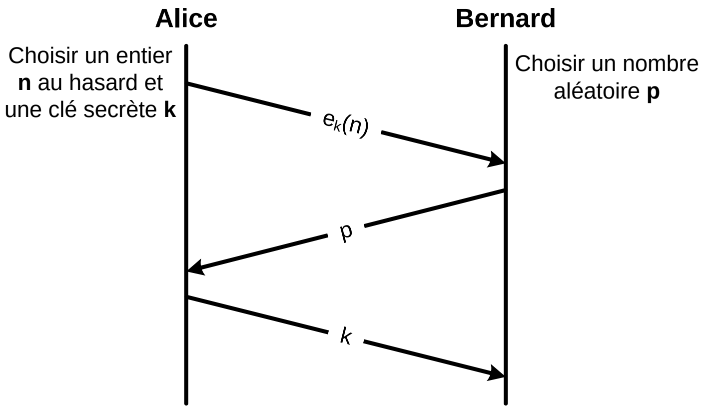
b. Quels sont les critères de sécurité qui sont assurés par ce protocole ?

/0.5

……………………………………………………………………………………………………

……………………………………………………………………………………………………

3. Pour garantir la sécurité de la décision finale, Alice et Bernard étudient la possibilité d'utiliser des fonctions cryptographiques. Au lieu d'envoyer **n** directement dans son premier message, Alice va envoyer **e_k(n)** où **e** est une fonction de chiffrement symétrique à clé secrète **k** (clé générée par Alice). Bernard transmet ensuite **p** en clair et enfin Alice transmet à Bernard **k** en clair.



Décision finale: Alice gagne si Bernard n'a pas deviné la parité. Sinon, c'est Bernard qui gagne.

a. Est-ce que les fraudes listées dans la question 2.a sont toujours possibles avec cette nouvelle version du protocole ? Expliquer.

/1

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

b. La confidentialité du nombre **n** est-elle assurée dans ce protocole ? Expliquer.

/0,5

……………………………………………………………………………………………………

……………………………………………………………………………………………………

4. Afin d'améliorer la sécurité du protocole qu'ils utilisent, Alice et Bernard décident d'utiliser l'algorithme RSA pour sécuriser les messages qu'ils échangent. Ils génèrent donc des clés (k_{pubA} , k_{prA}) et (k_{pubB} , k_{prB}), respectivement.

Université de La Manouba
Ecole Nationale des Sciences de l'Informatique

Section :
Module : **Sécurité Informatique**
Classe : **II3**
Session : Principale

A.U. : 2015/2016

Signatures des Surveillants

Signature de l'étudiant

Nom : ……………………… Prénom :……………………..

N° CIN : ………………………………………………………

N° d'inscription : ……………………………………………

Salle n° :…………………. Place n° :…………………..

✂- -

a. Alice a choisi $\mathbf{p}_A$=59, $\mathbf{q}_A$=101 et $\mathbf{e}_A$=3. En déduire la clé privée $\mathbf{d}_A$

/1

………………………………………………………………………………………………………
………………………………………………………………………………………………………
………………………………………………………………………………………………………

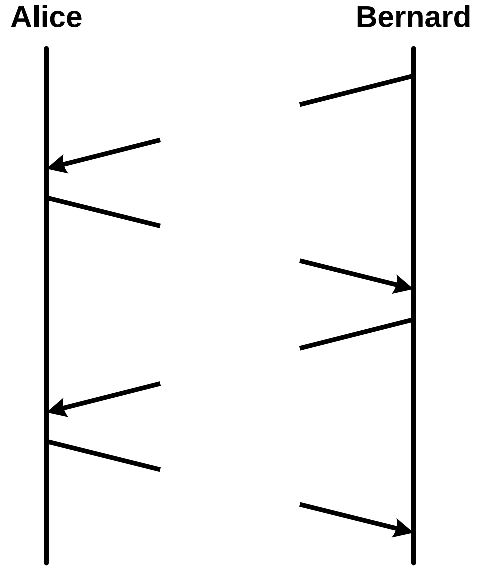
b. Bernard a choisi $\mathbf{p}_B$=3, $\mathbf{q}_B$=11 et $\mathbf{e}_B$=7. En déduire la clé privée $\mathbf{d}_B$

/1

………………………………………………………………………………………………………
………………………………………………………………………………………………………
………………………………………………………………………………………………………

c. Sur le schéma ci-dessous, proposer une solution basée sur l'utilisation de RSA (mais sans l'utilisation de certificats) pour sécuriser l'échange décrit dans la question 3. Pour chaque échange de message, préciser clairement la/les clés utilisée(s) dans l'opération. On suppose qu'avant cet échange, Alice et Bernard ne connaissent pas les clés publiques l'un de l'autre.

/2



d. Expliquer l'utilité du premier échange (de Bernard vers Alice)

/0,5

………………………………………………………………………………………………………
………………………………………………………………………………………………………
………………………………………………………………………………………………………

e. Ne pas utiliser de certificats mène-t-il à des failles de sécurité ? Expliquer.

/1

………………………………………………………………………………………………………
………………………………………………………………………………………………………
………………………………………………………………………………………………………

5. On va maintenant supposer qu'Alice et Bernard disposent chacun d'un certificat valide délivré par un organisme de certification reconnu.
   a. A quoi sert un certificat et quels sont les éléments principaux qui le composent ?

/1

………………………………………………………………………………………………………
………………………………………………………………………………………………………
………………………………………………………………………………………………………

b. Est-ce qu'il est possible d'améliorer le protocole précédent (question 4) en utilisant les certificats. Expliquer.

/1

……
……
……
……

Exercice 2 :

Dans le but d'uniformiser la gestion et le traitement des informations relatives à l'état civil dans toute la Tunisie, les systèmes d'information des différentes municipalités ont été uniformisés et connectés les uns aux autres via Internet : Chaque municipalité a son système d'information (SI-M) propre et les informations de tous les SI sont collectées dans le SI central (SI-C) du ministère de l'intérieur.

1. On considère les deux agents de menace suivant: le collectif Anonymous (AN) et un employé de municipalité malveillant (EM).
   Le tableau ci-après présente quatre scénarios à considérer lors de l'analyse du risque du système à développer. **Remplir toutes les cases du tableau.**

/3

	Agent de menace (AN ou EM)	Serveur vulnérable (SI-M ou SI-C)	C	O	M	P	I	R
Sc. 1			1	3	4		4	
Sc. 2			4	4	3		2	
Sc. 3			3	3	3		2	
Sc. 4			3	3	4		4	

Nous rappelons que : C = Capacité; O = Opportunité; M = Menace; P = Probabilité; I = Impact; R = Risque

2. Vous êtes l'ingénieur en charge de sécuriser les différents systèmes d'informations. Lors d'une réunion de travail, vous **expliquez** à vos supérieurs, qui n'ont que des connaissances générales en informatique, **les principes** de certaines attaques possibles contre le système existant (listées dans les questions a. , b. et c.) et **comment vous comptez les contrer**.
   a. Attaques DOS et DDOS

/1

……
……
……

   b. SQL injection (illustrer le principe à l'aide d'un exemple simple)

/1

……
……
……
……

   c. Port scanning

/1

……
……
……
……

Université de La Manouba
Ecole Nationale des Sciences de l'Informatique

Section :
Module : **Sécurité Informatique**
Classe : **II3**
Session : Rattrapage

A.U. : 2015/2016

Signatures des Surveillants

Nom : …………………… Prénom :……………………..
N° CIN : ………………………………………………….
N° d'inscription : …………………………………………
Salle n° :………………… Place n° :…………………..

Signature de l'étudiant

✂- -

	Note

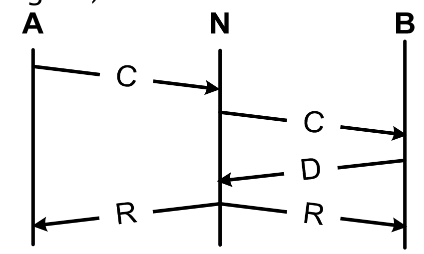
Examen de : ………………………..

Documents non autorisés

Appréciations du correcteur

Exercice1 :

On souhaite réaliser un service qui permet à deux stations A et B d'établir un contrat électronique en utilisant les services d'un tiers de confiance N qui joue le rôle de notaire (كاتب عدل). On suppose qu'avant d'utiliser ce protocole, A et B se sont mis d'accord sur les termes du contrat. Le protocole consiste alors en A qui envoie le contrat final **C** au notaire N, N qui transmet le contrat à B, B qui envoie sa décision **D** (acceptation ou rejet du contrat) à N et N qui transmet le résultat final R (réussite ou échec) de la négociation aux deux stations A et B (voir figure).



On suppose que A, B et N possèdent chacun une paire de clés (privée et publique) notées Kpr_A et Kpb_A, Kpr_B et Kpb_B et Kpr_N et Kpb_N, respectivement. On suppose également que A partage une clé secrète K_{NA} avec le notaire N et que B partage une clé secrète K_{NB} avec le notaire N.

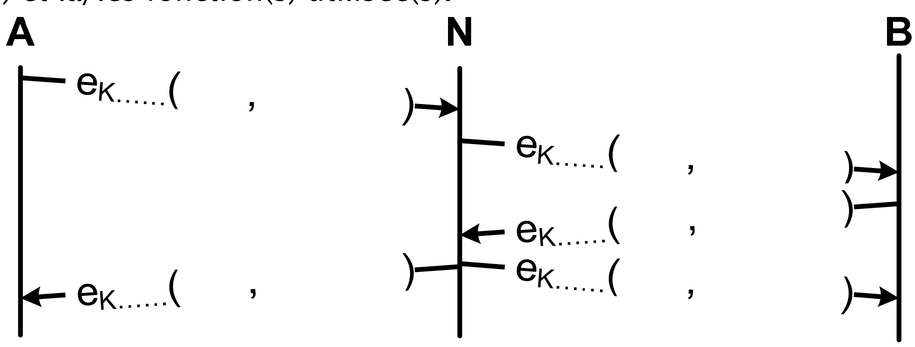
1. Tel qu'il est décrit, le protocole n'assure aucune des 4 critères de sécurité usuels : l'authentification, l'intégrité, la confidentialité et la non-répudiation. Rappeler brièvement le principe de chacun de ces critères.

/2

Authentification :…………………………………………………………………………………
…………………………………………………………………………………………………
Intégrité……………………………………………………………………………………………
…………………………………………………………………………………………………
Confidentialité………………………………………………………………………………………
…………………………………………………………………………………………………
Non-répudiation………………………………………………………………………………………
…………………………………………………………………………………………………

2. On cherche à assurer **l'intégrité** et **la confidentialité** des données échangées en utilisant une fonction de hachage h, une fonction de chiffrement symétrique e_K (K étant la clé utilisée lors de l'opération de chiffrement/déchiffrement) et les clés symétriques K_{NA} et K_{NB} que A et B partagent avec N. Sur le schéma ci-après, proposer une telle solution en précisant clairement pour chaque message la/les clé(s) utilisée(s) et la/les fonction(s) utilisée(s).

/1.5



Université de La Manouba
Ecole Nationale des Sciences de l'Informatique

Section :
Module : **Sécurité Informatique**
Classe : **II3**
Session : Rattrapage

A.U. : 2015/2016

Signatures des Surveillants

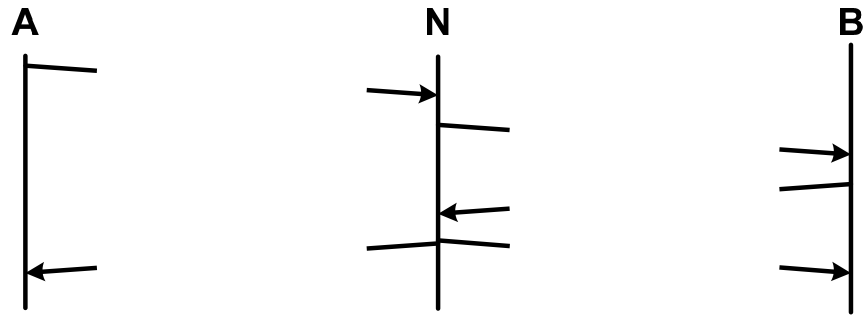
Nom : ……………………… Prénom :……………………..
N° CIN : …………………………………………………
N° d'inscription : ………………………………………
Salle n° :………………… Place n° :…………………..

Signature de l'étudiant

✂- -

3. On se propose maintenant d'utiliser une fonction de chiffrement asymétrique **Enc**$_K$ et une fonction de signature électronique **Sig**$_K$ où k représente la clé utilisée lors de l'opération. Sur le schéma ci-après, proposer une telle solution en précisant clairement pour chaque message la/les clé(s) utilisée(s) et la/les fonction(s) utilisée(s).

/2.5



4. Est-ce que l'intégrité et la confidentialité sont toujours les seuls critères de sécurité assurés par le protocole de la question 3 (celui qui utilise la cryptographie asymétrique) ? Expliquer brièvement mais clairement votre réponse.

/1

……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………

<u>Exercice 2:</u>

Dans cet exercice, on considère le chiffre de Vigenère :

1. Chiffrer le texte suivant "textesecretadecoder" en utilisant comme clé le mot *crypto*.

/1

……………………………………………………………
……………………………………………………………

2. Pour le même texte en clair que pour la question 1, on obtient le texte chiffré suivant "brqksmzcspxiqxtcxzr" .Quelle est la clé qui a été utilisée pour le chiffrement ?

/1

……………………………………………………………
……………………………………………………………

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

3. Supposons que vous disposiez d'un texte en clair et d'une partie du même texte chiffré, mais que ce texte soit plus court que la clef (par exemple, les 3 première lettres seulement du texte chiffré).
   a. Quelle information cela vous apporte-t-il ?

/0.5

……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………

Université de La Manouba
Ecole Nationale des Sciences de l'Informatique

Section :
Module : **Sécurité Informatique**
Classe : **II3**
Session : Rattrapage

A.U. : 2015/2016

Signatures des Surveillants

Signature de l'étudiant

Nom : …………………… Prénom :……………………..
N° CIN : ……………………………………………………
N° d'inscription : …………………………………………
Salle n° :………………… Place n° :…………………..

✂- -

b. Imaginez une stratégie de cryptanalyse dans le cas où la clé est un mot français. Expliquer

/1

……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………

c. Cette technique fonctionne-t-elle dans le cas où la clé est une suite aléatoire de lettres ? Expliquer.

/0.5

……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………

<u>Exercice 3 :</u>

On utilise les notations habituelles du RSA : p, q, n, $\varphi(n)$, e et d

1. Donner les formules qui définissent les variables n, $\varphi(n)$ et d en fonction d'une ou de plusieurs autres variables.

/1

……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………

2. Quelles sont les valeurs qui doivent rester secrètes parmi n, p, q, $\varphi(n)$, e et d ?

/0.5

……………………………………………………………………………………………………
……………………………………………………………………………………………………

3. Quelles sont les valeurs publiques parmi n, p, q, $\varphi(n)$, e et d ?

/0.5

……………………………………………………………………………………………………
……………………………………………………………………………………………………

4. On chiffre un message M en utilisant RSA. Donner les formules de chiffrement et de déchiffrement.

/1

Chiffrement :…………………………………………………………………………………
Déchiffrement :………………………………………………………………………………

5. On signe un message M en utilisant RSA. Donner les formules de signature et de vérification.

/1

Signature :……………………………………………………………………………………
Vérification :…………………………………………………………………………………

6. On suppose que p=19, q=23 et e=7, calculer d.

/1

……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………

7. Alice envoie deux messages M1 et M2 en clair à Bob en associant à chaque message la signature effectuée avec sa clé privée K_{PrA}

Alice ——— M1, Sig_K_{PrA}(M1) ———→ **Bob**
——— M2, Sig_K_{PrA}(M2) ———→

a. Montrer que Sig_K_{PrA}(M1*M2)= Sig_K_{PrA}(M1)* Sig_K_{PrA}(M2)

/0.5

……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………

Université de La Manouba
Ecole Nationale des Sciences de l'Informatique

Section :
Module : **Sécurité Informatique**
Classe : **II3**
Session : Rattrapage

A.U. : 2015/2016

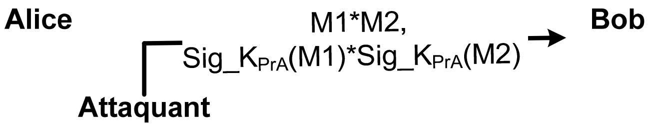
Signatures des Surveillants

Nom : …………………… Prénom :……………………..
N° CIN : ……………………………………………………
N° d'inscription : …………………………………………
Salle n° :…………………. Place n° :…………………..

Signature de l'étudiant

✂- -

b. Un attaquant écoute les échanges et souhaiterait injecter un faux message pour l'envoyer à Bob en prétendant que c'est de la part d'Alice. Pour cela, il envoie le message suivant :



Est-ce que cette attaque va réussir (c'est-à-dire que Bob va vraiment croire que c'est Alice qui a généré ce message) ? Expliquer.

/0.5
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………

Exercice 4 :

Vous êtes l'ingénieur en charge de sécuriser le système d'information d'une université. Vous identifiez 2 sortes d'attaquants : Un attaquant interne au réseau et un attaquant externe au réseau.

1. Sur une échelle de 1 à 4, estimez la capacité de chaque attaquant dans le cas où :
   a. L'université est la faculté des lettres de La Manouba

/0.5
Capacité de l'attaquant interne : ………………………………………………………………
Capacité de l'attaquant externe : ………………………………………………………………

   b. L'université est l'ENSI

/0.5
Capacité de l'attaquant interne : ………………………………………………………………
Capacité de l'attaquant externe : ………………………………………………………………

2. Lors d'une réunion de travail, vous expliquez à vos supérieurs, qui n'ont que des connaissances générales en informatique, les principes de certains concepts utilisés dans le domaine de la sécurité informatique.
   a. Key loggers

/1
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………

   b. Script Kiddies

/1
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………

Université de La Manouba
Ecole Nationale des Sciences de l'Informatique

Section :
Module : **Sécurité Informatique**
Classe : **II3**
Session : Principale

A.U. : 2016/2017

Signatures des Surveillants

Nom : …………………… Prénom :……………………..

N° CIN : ……………………………………………………

N° d'inscription : …………………………………………

Salle n° :…………………. Place n° :…………………..

Signature de l'étudiant

✂- -

Note

Examen de : …………………………..

Documents non autorisés

Appréciations du correcteur

Problème de sécurité informatique

La société XYZ est une société exportatrice de matériel informatique installée en Tunisie dont le siège central est situé dans un bâtiment de 4 étages: le 1[er] étage est consacré au service commercial, le 2[ème] étage aux ingénieurs et aux techniciens informatiques, le 3[ème] abrite les services financier et juridique et enfin le 4[ème] étage est réservé à l'administration et à la direction générale. Le rez-de-chaussée contient le dépôt du matériel informatique.

La société XYZ comprend au total 100 employés de diverses disciplines. Chaque jour, les employés doivent s'authentifier par empreint digitale en accédant à l'entrée du bâtiment et dès lors, ils sont autorisés à accéder à tous les étages. La société offre à ses employés et à ses visiteurs une connexion Wifi à laquelle on peut se connecter à l'aide d'un mot de passe (commun à tous les utilisateurs). Le site Web de la société est géré par un administrateur qui est le même pour le réseau et pour le système ; son bureau se trouve au 2[ème] étage là où résident les serveurs de base de données. Dans le but de simplifier la tâche de l'administrateur, les login des employés sont formés à partir de la concaténation de leurs noms et de leurs dates de naissances alors que les mots de passe représentent leurs prénoms associés à leurs dates de recrutements. Ces logins et mots de passes sont utilisés par les employés pour accéder à leurs PCs qui sont connectés au réseau Ethernet de la société. Tout document créé par un employé est par défaut accessible par tous les utilisateurs saufs si le propriétaire ou l'administrateur en change les droits.

Partie 1 : Protection générale de base :

1) Le contrôle d'accès à l'information est-il du type MAC, DAC ou RBAC ? Expliquer pourquoi ce n'est pas une bonne technique dans le cas de cette société. Proposer une meilleure solution qui prend en compte la diversité des profils des employés (secrétaires, ingénieurs, financiers, …) et la dynamique de l'entreprise (promotions, départs, …) et justifier votre choix.

/1.5

……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………

2) Récapituler les mesures mises en œuvre pour la protection du bâtiment, celles destinées à protéger le système informatique et celles qui protègent le réseau ?

/1.5

Mesures Bâtiment :………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………

Mesures Système :………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………

Mesures Réseau :…………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………

Signatures des Surveillants

Signature de l'étudiant

Nom : …… Prénom :……..

N° CIN : …….

N° d'inscription : ……

Salle n° :……. Place n° :……..

✂----------

3) Déterminer les inconvénients majeurs de ces mesures de protection (au moins deux inconvénients dans chaque cas).

/1.5

Bâtiment :……
……
……
Système :……
……
……
Réseau :……
……
……

4) A la suite de l'identification de certains des inconvénients de la question précédente, l'administrateur a décidé de définir des codes d'accès à chaque étage au niveau de l'ascenseur (les employés tapent les codes sur une console à l'intérieur de l'ascenseur). Il a également décidé d'utiliser des cartes à puce pour permettre le monitoring des accès aux étages, salles machines, bureaux, salles de réunions, … Quels sont, à votre avis, les avantages et les inconvénients de ces mesures (au moins 1 avantage et 1 inconvénient dans chaque cas) ?

/1

Code ascenseur :……
……
……
Cartes à puce :……
……
……

5) Pour renforcer la sécurité de la société, l'administrateur a procédé à une enquête dont le résultat est le suivant :
   a. 50% des employés ont avoué avoir été victimes du piratage de leurs comptes Facebook (envoi par l'attaquant de messages et de publications aux amis).
   b. Plus que 45% des employés ont constaté une consommation importante de la bande passante même si eux-mêmes ne génèrent pas de trafic réseau.
   c. 5% des employés ont déclaré perdre temporairement le contrôle de leurs machines.

Dans chacun des cas, identifier le type d'attaque et indiquer brièvement **au moins 2 façons** pour les corriger/éviter.

/3

a. ……
……
……
b. ……
……
……
c. ……
……
……

La société XYZ utilise un standard appelé SET pour sécuriser sa solution de commerce électronique. Une version simplifiée de l'architecture de SET est donnée par la figure suivante :

Signatures des Surveillants

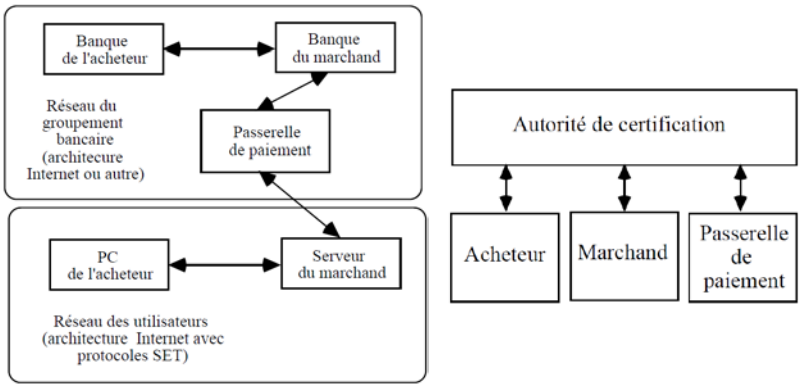
Signature de l'étudiant

Nom : …… Prénom :……..

N° CIN : ……

N° d'inscription : ……

Salle n° :……. Place n° :……..



6) Qu'est-ce qu'un certificat, quelles sont ses composantes principales et quel est l'objectif de son utilisation ?

/1.5

……
……
……
……
……

Le processus d'achat se déroule en deux échanges requêtes-réponses successifs.

Premier échange

Message1- La requête initiale *Req_init* de l'acheteur (A) vers le serveur du marchand (M) indique simplement l'intention par l'acheteur de passer commande.

Message2- La réponse initiale du serveur du marchand comporte trois éléments:

- un identifiant de commande ID_{Cd} signé avec le protocole RSA.
- le certificat du serveur du marchand.
- le certificat de la passerelle de paiement.

7) Quelle est la clé utilisée pour signer l'identifiant ID_{Cd}. On dénote par (K_{A_Pub},K_{A_Prv}) et (K_{M_Pub},K_{M_Prv}) les clés publique et privée de A et de M, respectivement.

/0.5

……
……
……

8) A la suite de ce premier échange, l'acheteur doit effectuer une/des vérification(s) qui vont lui permettre de passer au second échange. Laquelle/Lesquelles ?

/0.5

……
……
……

Second échange

L'acheteur doit d'abord générer la requête d'achat ou "Order Information" (***OI***) qui contient des informations concernant la commande ***infosCd*** (liste des produits, quantités, prix, …) ainsi que l'identifiant de la commande $\boldsymbol{ID_{Cd}}$. Cette requête va plus tard être envoyée au serveur du marchant.

L'acheteur génère ensuite la requête de paiement ou "Payment Information" (***PI***) qui contient des informations concernant la carte bancaire ***infosCB*** de l'acheteur ainsi que l'identifiant de la commande $\boldsymbol{ID_{Cd}}$. Cette requête va plus tard être envoyée à la passerelle de paiement à travers le serveur du marchant.

Les deux requêtes ***OI*** et ***PI*** sont liées, c'est pourquoi l'acheteur utilise l'algorithme SHA1 pour calculer par les fonctions de hachage $\{OI\}_{SHA1}$ et $\{PI\}_{SHA1}$. Ensuite, il calcule $\{\{OI\}_{SHA1},\{PI\}_{SHA1}\}_{SHA1}$ et signe le tout avec sa clé privée RSA $\boldsymbol{K_{A\_Prv}}$. Le message résultant s'appelle

Signature Duale (***SD***) avec $SD=\left\{\{\{OI\}_{SHA1},\{PI\}_{SHA1}\}_{SHA1}\right\}_{K_{A\_Prv}}$

L'acheteur choisit ensuite une clé aléatoire K_{RAND} pour l'algorithme DES et l'utilise pour chiffrer le message ***(PI,SD)*** auquel il ajoute la clé K_{RAND} chiffrée avec la clé publique de la passerelle de paiement K_{P_Pub} (reçu dans le certificat de la passerelle):

$$\{PI,SD\}_{K_{RAND}}, \{K_{RAND}\}_{K_{P\_Pub}}$$

Message3- Le message envoyé par l'acheteur au serveur du marchand est le suivant:

$$\{PI,SD\}_{K_{RAND}}, \{PI\}_{SHA1}, \{K_{RAND}\}_{K_{P\_Pub}}, OI, SD, Cert_A$$

avec $Cert_A$ le certificat de l'acheteur A.

Message4- Le serveur du marchant transmet à la passerelle de paiement les parties du message qui concernent le paiement et qu'il (le serveur du marchant) ne peut pas comprendre.

9) Identifier ces parties (et uniquement ces parties).

/1

……
……
……

Message5- Une fois le paiement confirmé par sa banque, le marchant génère le reçu d'achat ***RA***, lui fait subir une fonction de hachage $\{RA\}_{SHA1}$ ensuite signe le tout en utilisant RSA. Le message final que le serveur du marchant envoie à l'acheteur est le suivant :

$$RA, \{\{RA\}_{SHA1}\}_{K_{M\_Prv}}$$

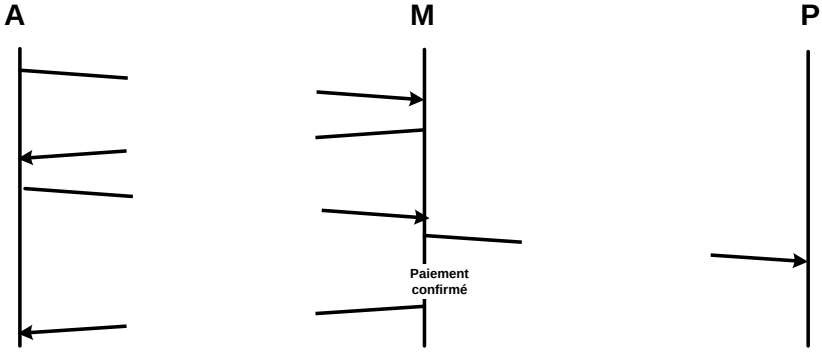
10) Pourquoi faire subir à RA une fonction de hachage avant de signer (pourquoi ne pas signer RA directement)? Quelle propriété de sécurité veut-on assurer dans de cas ?

/1

……
……
……

11) Sur le diagramme ci-dessous, représenter l'échange des messages du standard SET en précisant pour chaque message la/les opération(s) cryptographique(s) et la/les clé(s) utilisée(s) ?

/1



12) Remplir le tableau suivant en précisant, pour les messages 2, 3 et 4 les propriétés de sécurité assurées et en inscrivant dans la case correspondante la partie **précise** du message qui assure cette propriété. Le cas du message 5 est donné en exemple.

/2

	Authentification	Confidentialité	Intégrité	Non-répudiation
Message 2				
Message 3				
Message 4				
Message 5	-	-	$\{\{RA\}_{SHA1}\}K_{M\_Prv}$	$\{\{RA\}_{SHA1}\}K_{M\_Prv}$ + $Cert_M$

Université de La Manouba
Ecole Nationale des Sciences de l'Informatique

Section :
Module : **Sécurité Informatique**
Classe : **II3**
Session : Principale

A.U. : 2016/2017

Signatures des Surveillants

Nom : ……………………… Prénom :……………………..

N° CIN : ………………………………………………….

N° d'inscription : …………………………………………

Salle n° :………………… Place n° :…………………..

Signature de l'étudiant

✂- -

Exercice RSA :

On note (n, e) la clé publique d'un système RSA. On suppose que $n = 35$.

1. Expliquez pourquoi il n'est pas possible d'avoir un e pair ?

/0.5

…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………

2. Déterminer tous les e possibles.

/0.5

…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………

3. Si on choisit e=φ(n)-1 ? Calculer d. Expliquez pourquoi ce choix n'est pas judicieux ?

/1

…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………

4. Si la clé publique est (492153, 2237), quelle est la clé privée ? Détailler les calculs.

/2

…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………

Questions indépendantes :

1. Expliquer pourquoi il est déconseillé du point de vue sécurité d'utiliser la même clé secrète trop souvent. Que doit-on faire à la place?

/1

…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………

2. Illustrer le principe de l'injection SQL à l'aide d'un exemple simple.

/1

…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………

3. Expliquer brièvement le principe du « Packet Sniffing ».

/1

…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………

Université de La Manouba
Ecole Nationale des Sciences de l'Informatique

Section :
A.U. : 2016/2017
Module : **Sécurité Informatique**
Classe : **II3**
Session : Rattrapage

Signatures des Surveillants

Nom : …………………… Prénom :……………………..

N° CIN : ……………………………………………………

N° d'inscription : …………………………………………

Salle n° :………………… Place n° :…………………..

Signature de l'étudiant

✂- -

Note

Examen de : …………………………..

Documents non autorisés

Appréciations du correcteur

Exercice 1 :

1. La direction des études de l'ENSI exige que les corrections des examens soient préparées en même temps que les énoncés pour qu'en cas de maladie ou d'absence, un autre professeur soit capable de corriger les copies et de les rendre à l'administration évitant ainsi tout retard dans le calendrier académique. Cependant, votre professeur de sécurité informatique est un peu paranoïaque et ne veut dévoiler les solutions de l'examen à personne avant que l'examen ne soit fini. Il doit donc penser à une méthode qui utilise des fonctions cryptographiques simples avec laquelle il prouve au directeur des études qu'il a bien préparé la solution à l'examen sans que ce dernier ne puisse lire le document avant l'examen.
   a. Proposer une telle méthode qui se base sur des fonctions de hashage cryptographiques.

/1

……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………

   b. Proposer une telle méthode qui se base sur des fonctions de chiffrement/déchiffrement.

/1

……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………

2. Le professeur doit partir en voyage alors qu'il n'a pas fini de préparer l'examen final pour son cours. Il doit donc envoyer l'examen à sa secrétaire pour qu'elle puisse l'imprimer avant le jour de l'examen final. Cependant, le professeur se méfie de l'email comme moyen de communication car il soupçonne que certains de ses étudiants pourraient le hacker. Il décide alors d'utiliser la cryptographie à clé publique pour sécuriser l'envoi de l'examen. Le couple clé publique/ clé privée du professeur dénoté par (KP_Pub,KP_Prv) est disponible sur son PC portable. Il connait également un certain nombre de clés puliques utilisées par des collègues de l'ENSI mais, malheureusement, il remarque qu'il n'a pas la clé publique de sa secrétaire KS_Pub. Il lui envoie donc un email lui demandant de lui envoyer sa clé publique.
   a. Parmi les 4 opérations suivantes, cocher celle que le professeur doit effectuer si son but principal est d'assurer la confidentialité de l'examen qu'il va envoyer à sa secrétaire :

/1
- ☐ Chiffrement de l'examen avec sa clé publique K_{P_Pub}
- ☐ Chiffrement de l'examen avec la clé publique de sa secrétaire K_{S_Pub}
- ☐ Signature de de l'examen avec sa clé privée K_{P_Prv}
- ☐ Signature de l'examen avec la clé privée de sa secrétaire K_{S_Prv}

Signatures des Surveillants

Signature de l'étudiant

Nom : …… Prénom :……..

N° CIN : …….

N° d'inscription : ……

Salle n° :……. Place n° :……..

✂----------

b. Parmi les 4 opérations suivantes, laquelle le professeur doit-il effectuer si son but principal est d'assurer l'intégrité et la non-répudiation de l'examen qu'il va envoyer à sa secrétaire :

/1

- ☐ Chiffrement de l'examen avec sa clé publique KP_Pub
- ☐ Chiffrement de l'examen avec la clé publique de sa secrétaire KS_Pub
- ☐ Signature de de l'examen avec sa clé privée KP_Prv
- ☐ Signature de l'examen avec la clé privée de sa secrétaire KS_Prv

3. Supposons qu'une étudiante ait pu « sniffer » tout le trafic qui se dirige et/ou sort du poste de la secrétaire à partir de son portable qui est branché sur le réseau de l'École, et qu'elle soit tombée sur l'email du professeur. Selon vous, est-ce que l'étudiante serait en mesure de se servir de tout ceci pour obtenir une copie de l'examen ? Si oui comment, si non pourquoi? (Note : l'étudiante n'est pas en mesure d'empêcher le trafic de se diriger à sa destination.)

/1

……
……
……
……
……
……
……
……
……

4. Le professeur reçoit un email contenant la clé publique de sa secrétaire mais, toujours très méfiant, il appelle sa secrétaire pour vérifier l'authenticité non seulement du message reçu mais aussi de la clé publique reçue. Si on suppose que ce n'est pas possible de vérifier la clé publique chiffre par chiffre (la clé est trop longue et le risque d'erreur est trop grand, proposer une solution utilisant des outils cryptographiques qui pourrait permettre au professeur de faire cette vérification.

/1

……
……
……
……
……
……
……

5. Supposons maintenant que le professeur est dans un endroit tellement exotique qu'il ne peut pas entrer en communication avec sa secrétaire par téléphone. Il ne dispose que d'une connexion Internet de basse vitesse (donc pas de voix par IP ou autre moyen multimédia). Quel autre moyen existerait-il pour qu'il puisse obtenir une copie de la clé publique de sa secrétaire dont il soit sûr de l'authenticité ?

/1

……
……
……
……
……
……
……

Signatures des Surveillants

Signature de l'étudiant

Nom : ……………………… Prénom :……………………..

N° CIN : ……………………………………………………

N° d'inscription : …………………………………………

Salle n° :………………… Place n° :…………………..

✂- -

6. Le professeur obtient enfin la vraie clé publique de sa secrétaire. Cette clé est calculée en utilisant p=47, q=71 et e=79. Déterminer la clé privée de la secrétaire en précisant la démarche.

/2

………………………………………………………………………………………………………
………………………………………………………………………………………………………
………………………………………………………………………………………………………
………………………………………………………………………………………………………
………………………………………………………………………………………………………
………………………………………………………………………………………………………
………………………………………………………………………………………………………
………………………………………………………………………………………………………
………………………………………………………………………………………………………

Exercice 2 :

1. A quoi sert le protocole Diffie Hellman?

/1

………………………………………………………………………………………………………
………………………………………………………………………………………………………
………………………………………………………………………………………………………

2. Expliquez à l'aide d'un schéma et d'un exemple le principe de ce protocole.

/2

3. Soit p = 251 et le générateur g = 11 modulo p. Soit maintenant a = 15 et b = 21. Déterminer la clef commune à Alice et Bob, s'ils effectuent un échange de clef de Diffie-Hellman.

/1

………………………………………………………………………………………………………
………………………………………………………………………………………………………
………………………………………………………………………………………………………
………………………………………………………………………………………………………
………………………………………………………………………………………………………
………………………………………………………………………………………………………
………………………………………………………………………………………………………
………………………………………………………………………………………………………

Exercice 3 :

1. Quels sont les trois facteurs qui influencent le calcul de la probabilité d'une occurrence de menace délibérée.

/1

………………………………………………………………………………………………………
………………………………………………………………………………………………………
………………………………………………………………………………………………………
………………………………………………………………………………………………………
………………………………………………………………………………………………………

Université de La Manouba
Ecole Nationale des Sciences de l'Informatique

Section :
Module : **Sécurité Informatique**
Classe : **II3**
Session : Rattrapage

A.U. : 2016/2017

Signatures des Surveillants

Signature de l'étudiant

Nom : …… Prénom :……..

N° CIN : …….

N° d'inscription : ……

Salle n° :……. Place n° :……..

✂----------

2. La banque XY offre des services bancaires par Internet à ses clients. Auparavant, ce service permettait seulement de consulter les transactions du compte et de payer des factures de services publics. À la demande de ses clients, la banque a ajouté la possibilité d'effectuer des transferts interbancaires sur des comptes de particulier via leur interface Internet. Si on considère la menace que des malfaiteurs puissent frauder la banque en se servant du service Internet, quel facteur de l'analyse de risque est modifié par ce changement de situation? Justifier votre réponse.

/1

……
……
……
……
……

3. La banque décide plus tard d'augmenter le montant de transfert permis entre ses les abonnés de 1000 à 10 000DT. Quel(s) facteur(s) de l'analyse de risque est (sont) modifié(s) par ce changement de situation ? Justifier votre réponse.

/1

……
……
……
……
……

Questions indépendantes :

1. Quels sont les paramètres principaux qu'un pare-feu de réseau examine sur un paquet IP? (nommez-en au moins trois)

/1

……
……
……
……
……

2. Définir la stéganographie et expliquer, à l'aide d'un exemple concret, comment elle pourrait être utile à un groupe terroriste?

/1

……
……
……
……

3. Nommez deux méthodes d'authentification biométriques parmi les plus utilisés présentement, ainsi que leurs principaux inconvénients.

/2

……
……
……
……
……
……
……
……

Université de La Manouba
Ecole Nationale des Sciences de l'Informatique

Section :
Module : **Sécurité Informatique**
Classe : **II3**
Session : Principale

A.U. : 2017/2018

Signatures des Surveillants

Nom : …………………… Prénom :……………………..

N° CIN : ……………………………………………………

N° d'inscription : ………………………………………….

Salle n° :…………………. Place n° :…………………..

Signature de l'étudiant

✂- -

Note

Examen de : …………………………..

Documents non autorisés

Appréciations du correcteur

QCM

1. Parmi les critères de sécurité suivants, lequel n'est pas adapté à un système d'information ?

/0.5

- ☐ Confidentialité
- ☐ Insolvabilité
- ☐ Intégrité
- ☐ Non-répudiation

2. Quel service de sécurité la stéganographie permet-elle de réaliser ?

/0.5

- ☐ L'intégrité
- ☐ La non-répudiation
- ☐ L'authenticité
- ☐ La confidentialité

3. Quel critère de sécurité la cryptographie ne permet pas de réaliser ?

/0.5

- ☐ La confidentialité
- ☐ L'intégrité
- ☐ L'authentification
- ☐ La disponibilité

4. Dans un système de chiffrement asymétrique, quelle clé emploie l'expéditeur pour chiffrer des données confidentielles à destination d'un récepteur ?

/0.5

- ☐ La clé publique de l'expéditeur
- ☐ La clé publique du destinataire
- ☐ La clé privée de l'expéditeur
- ☐ La clé privée du destinataire

5. Laquelle des propositions suivantes ne caractérise pas les systèmes de contrôle d'accès biométrique ?

/0.5

- ☐ Exactitude, faible coût
- ☐ Atteinte à la vie privée
- ☐ Unicité de l'organe contrôlé
- ☐ Taux d'erreurs important

6. Contrairement aux codes d'authentification de message (MAC), les signatures numériques assurent :

/0.5

- ☐ l'authentification
- ☐ la non-répudiation absolue
- ☐ l'intégrité
- ☐ la confidentialité

7. Laquelle des réponses suivantes est une caractéristique d'un système de détection d'intrusions (IDS) ?

/0.5

- ☐ La récolte d'évidences de tentatives d'attaque.
- ☐ L'identification de faiblesses dans la définition de la politique de sécurité.
- ☐ Le blocage d'accès à certains sites Internet.
- ☐ Le fait d'empêcher l'accès de certains utilisateurs à certains serveurs.

8. Un système cryptographique est dit incassable et robuste s'il peut résister à une attaque de cryptanalyse du type :

/0.5

- ☐ texte chiffré seul
- ☐ texte en clair choisi
- ☐ texte en clair connu
- ☐ texte chiffré choisi

Signatures des Surveillants

Signature de l'étudiant

Nom : …… Prénom :……..

N° CIN : ……

N° d'inscription : ……

Salle n° :……. Place n° :……..

9. Laquelle des affirmations suivantes est fausse ? Le modèle DAC :
   - délègue l'accord des permissions d'accès à la discrétion des propriétaires des ressources du système.
   - a le mérite de la simplicité.
   - permet de limiter l'accès d'utilisateurs honnêtes et d'éviter l'altération d'information.
   - est adapté au contexte où l'information est très sensible.

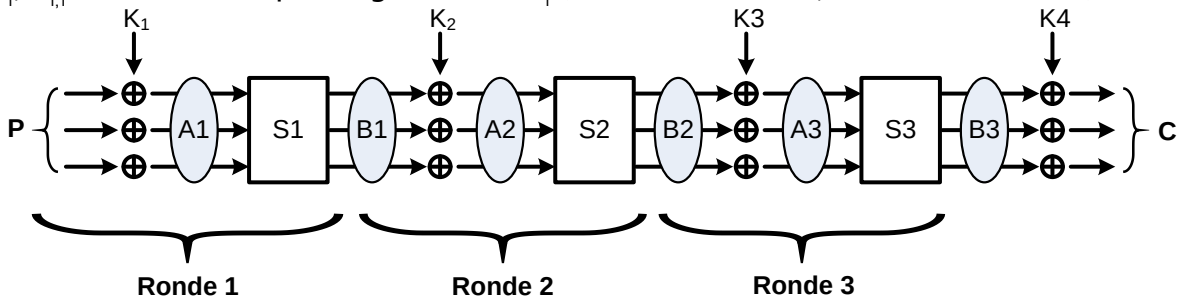
/0.5

10. Parmi les propositions suivantes quelle est celle qui correspond le mieux au besoin de gérer la sécurité ?
    - Traiter la sécurité comme une exigence du business.
    - Appréhender et traiter la sécurité comme un processus continu.
    - Appréhender et traiter la sécurité comme un processus discontinu.
    - Appréhender et traiter la sécurité comme un processus connu.

/0.5

Exercice 1

On considère l'algorithme de chiffrement illustré dans la figure ci-après et qui prend en entrée un bloc de texte en clair P constitué de 3 bits et fournit en sortie un bloc de texte chiffré C de 3 bits également. L'algorithme considéré se sert de quatre clés intermédiaires de 3 bits chacune K_1, K_2, K_3, K_4 tirées d'une clé principale K et utilisées pour l'exécution des trois rondes intermédiaires et pour le XOR final. Dans chaque ronde intermédiaire *Ronde*$_i$, le texte en entrée subit un XOR avec la clé intermédiaire correspondante K_i suivi d'une fonction de substitution représentée par une boîte de substitution (Boîte-S) S_i. On note $K_{i,j}$ le j^e bit de la clé intermédiaire K_i, $K_{i,1}$ étant le bit le plus à gauche de K_i (sur notre schéma, c'est le bit du bas).



1. Décrire la procédure de chiffrement, c'est-à-dire donner les expressions de A_1, B_1, A_2, B_2, A_3, B_3, et C en fonction des autres variables, des clés intermédiaires K_i et des fonctions de substitution S_i,

/1.75

A1=……	B1=……
A2=……	B2=……
A3=……	B3=……
C=……	

Signatures des Surveillants

Signature de l'étudiant

Nom : …… Prénom :……..

N° CIN : ……

N° d'inscription : ……

Salle n° :……. Place n° :……..

✂----------

On se propose de casser cet algorithme en appliquant une des principales techniques d'attaque à texte clair connu qui est la cryptanalyse linéaire.

2. Décrire brièvement le principe de cette attaque.

/1.25

……
……
……
……
……
……

3. En énumérant les propriétés non linéaires des deux premières boîtes de substitution S_1 et S_2, on a pu mettre en exergue les deux approximations linéaires suivantes :

(Eq1) $S_1 : X_1 \oplus X_2 \oplus X_3 = Y_2$ avec une probabilité $p_1 = 3/4$
(Eq2) $S_2 : X_2 = Y_1 \oplus Y_3$ avec une probabilité $p_2 = 2/7$

$X = (X_1, X_2, X_3)$ et $Y = (Y_1, Y_2, Y_3)$ dans la première équation représentent respectivement l'entrée et la sortie de la boîte de substitution S_1 alors qu'ils représentent dans l'équation 2 respectivement l'entrée et la sortie de la boîte de substitution S_2.

a. En utilisant l'approximation linéaire de S_1, exprimer $B_{1,2}$ en fonction de $P_{1,i}$, $i \in \{1,2,3\}$ et de $K_{1,i}$, $i \in \{1,2,3\}$.

/1

……
……
……
……

b. En déduire l'expression de $A_{2,2}$ en fonction de $P_{1,i}$, $i \in \{1,2,3\}$, de $K_{1,i}$, $i \in \{1,2,3\}$ et de $K_{2,i}$, $i \in \{1,2,3\}$.

/1

……
……
……
……

c. En utilisant l'approximation linéaire de S_2 et l'expression de $A_{2,2}$ obtenue dans la question précédente, déterminer l'expression décrivant $P_{1,1}$, $P_{1,2}$, $P_{1,3}$, $K_{1,1}$, $K_{1,2}$, $K_{1,3}$ et $K_{2,2}$ en fonction de $K_{3,1}$, $K_{3,3}$, $A_{3,1}$ et $A_{3,3}$.

/1

……
……
……
……

Signatures des Surveillants

Signature de l'étudiant

Nom : ……………………… Prénom :……………………..

N° CIN : ……………………………………………………

N° d'inscription : ……………………………………………

Salle n° :………………… Place n° :…………………..

---

d. Appliquer le lemme de Piling-Up de Matsui (ci-après) afin de calculer la probabilité pour que l'expression déterminée dans la question 3.c soit valable.

> *Lemme de Piling-UP de Matsui*
>
> Soit N variables aléatoires, indépendantes et binaires, $X_1, X_2, X_3, \ldots, X_N$, la probabilité que l'équation $X_1 \oplus X_2 \oplus X_3 \oplus \ldots \oplus X_N = 0$ soit correcte est :
>
> $$P(X_1 \oplus X_2 \oplus X_3 \oplus \ldots \oplus X_N = 0) = \frac{1}{2} + 2^{N-1} \prod_{i=1}^{N} (p_i - \frac{1}{2})$$

/1

……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………

e. A ce stade, on a pu déterminer une expression approchant linéairement les 2 premiers tours de l'algorithme de chiffrement considéré qui n'est fonction que des bits du texte en clair P (entrée de l'algorithme) et des bits d'entrée de la dernière boîte de substitution S_3 (càd les bits de A_3) et ce en combinant les approximations linéaires obtenues des deux boîtes de substitution S_1 et S_2.
Sachant qu'on dispose de N morceaux d'un message en clair et de leurs cryptogrammes correspondants (i.e. N couples (clair,cryptogramme) connus) chiffrés tous avec l'algorithme de la figure et la même clé K, décrire en détails la procédure à suivre pour retrouver progressivement les 4 clés intermédiaires.

/2

……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………

Exercice 2

1. Proposer une définition du risque.

/1

……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………

Signatures des Surveillants

Signature de l'étudiant

Nom : …… Prénom :……..

N° CIN : ……

N° d'inscription : ……

Salle n° :……. Place n° :……..

✂----------

2. Quels sont parmi ces facteurs ceux qui interviennent dans l'analyse de risque ?

/1

- ☐ Impact
- ☐ Opportunité
- ☐ Occurrence
- ☐ Disponibilité
- ☐ Menace
- ☐ Capacité
- ☐ Motivation
- ☐ Vulnérabilité

3. La BIAT offre des services bancaires par Internet à ses clients. Auparavant, ce service permettait seulement de consulter les transactions du compte et de payer des factures de services publics.
   A la demande de ses clients, la BIAT a ajouté la possibilité d'effectuer des transferts interbancaires sur des comptes de particulier via leur interface Internet. Si on considère la menace que des malfaiteurs puissent frauder la banque en se servant du service Internet, quel facteur de l'analyse de risque est modifié par ce changement de situation ? Justifier votre réponse.

/0.5

……
……
……
……

4. La BIAT décide plus tard d'augmenter le montant de transfert permis entre ses abonnés de 1000 à 10 000 DT. Quel facteur de l'analyse de risque est modifié par ce changement de situation ? Justifier votre réponse.

/0.5

……
……
……

5. En cas d'émission d'une nouvelle carte bancaire à un client de la banque, ce client doit aller chercher sa carte et le code PIN correspondant (code d'accès de 4 chiffres) à l'agence à laquelle il est domicilié. La BIAT souhaite moderniser cette procédure ; La nouvelle méthode consiste à envoyer les cartes aux clients par courrier postal et les codes associés par email. Pour cela, la banque demande à chacun de ses clients de générer une paire de clés publiques/privées RSA et de communiquer la clé publique en personne au service informatique de la banque.

   a. Mr Foulène a généré une paire de clés et a voulu remettre la clé publique (e,n)= (13 , 4985) à la banque mais le responsable du service informatique ne l'a pas acceptée et a demandé à Mr Foulène de générer une «meilleure» paire de clés. Expliquer pourquoi.

Université de La Manouba
Ecole Nationale des Sciences de l'Informatique

Section :
Module : **Sécurité Informatique**
Classe : **II3**
Session : Principale

A.U. : 2017/2018

Signatures des Surveillants

Signature de l'étudiant

Nom : ……………………… Prénom :……………………..

N° CIN : …………………………………………………….

N° d'inscription : ……………………………………………

Salle n° :…………………. Place n° :…………………..

✂- -

/1.5

………
………
………

b. Mr Foulène a généré une nouvelle paire de clés en utilisant des nombres premiers p et q qui sont compris entre 160 et 170 et il a obtenu la clè publique suivante (e,n)=(7,27221). Trouver la clé privée (d,n). **Expliquer la démarche utilisée en détails.**

/1

………
………
………
………
………
………
………
………

c. Le code PIN à 4 chiffres associé à la carte bancaire de Mr Foulène lui est parvenu (chiffré) par email. Quelle est la valeur reçue dans l'email sachant que la valeur du code avant chiffrement est 0012 et qu'elle est considérée comme le nombre 12 et pas la chaine de caractère « 0012 » ?

/0.5

………
………
………
………
………
………
………
………

Université de La Manouba
Ecole Nationale des Sciences de l'Informatique

Section :
Module : **Sécurité Informatique**
Classe : **II3**
Session : Rattrapage

A.U. : 2017/2018

Signatures des Surveillants

Nom : ………………………. Prénom :……………………..

N° CIN : ………………………………………………………

N° d'inscription : ……………………………………………

Salle n° :…………………. Place n° :…………………..

Signature de l'étudiant

✂- -

Note

Examen de : …………………………..

Documents non autorisés

Appréciations du correcteur

Questions indépendantes :

1. Remplir le tableau en faisant correspondre chaque notion à la définition qui lui correspond.

A	Cryptosystème
B	Propriétés des cryptosystèmes difficiles à cryptanalyser
C	Cryptologie
D	Cryptanalyse
E	Chiffrement mono-alphabétique
F	Chiffrement poly-alphabétique
G	Méthodes de cryptanalyse de base
H	Cryptographie
I	Chiffre de César
J	Algorithme OTP

1	Un chiffre où chaque lettre est remplacée par une autre lettre ou symbole
2	Un chiffre où chaque lettre est remplacée par une autre lettre qui n'est pas toujours la même
3	L'art de casser les cryptosystèmes
4	Diffusion et confusion
5	Un quintuplet S={P,C,K,E,D}
6	Un chiffrement de Vigenère avec taille(OTP)=taille(message)
7	L'art de concevoir des cryptosystèmes
8	Un chiffrement de décalage avec k=3
9	La science qui étudie la cryptographie et la cryptanalyse
10	Force brute et analyse fréquentielle

/5

Notion	A	B	C	D	E	F	G	H	I	J
Définition										

2. Le débordement de tampon (en anglais, buffer overflow) est une attaque système couramment utilisée par les pirates informatiques.
   a- Rappeler le principe de cette attaque.

/1

……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………

   b- Expliquer comment peut-on l'utiliser pour provoquer un déni de service (DoS) dans le système.

/1

……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………

   c- Citer deux mesures de sécurité permettant de se protéger contre ce type d'attaques.

/1

……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………

Université de La Manouba
Ecole Nationale des Sciences de l'Informatique

Section :
Module : **Sécurité Informatique**
Classe : **II3**
Session : Rattrapage

A.U. : 2017/2018

Signatures des Surveillants

Signature de l'étudiant

Nom : …………………… Prénom :……………………..

N° CIN : ……………………………………………………

N° d'inscription : …………………………………………

Salle n° :………………… Place n° :………………..

✂- -

3. Le processus de gestion des risques est un processus continu et itératif.
   a. Expliquer pourquoi.

/1
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………

   b. Rappeler ses principales étapes.

/1
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………

4. Alice souhaite envoyer à Bob via le réseau Internet un document confidentiel écrit sur une dizaine de pages. Afin de garantir la confidentialité des données transmises, Alice chiffre le contenu dudit document avec un système de chiffrement symétrique.
   a. Justifier le choix d'un système de chiffrement symétrique pour le cryptage des données à transmettre.

/1
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………

   b. Rappeler l'inconvénient majeur de ce système.

/1
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………

   c. Dans le but d'assurer un échange sécurisé de la clé secrète utilisée pour le chiffrement, Alice et Bob se sont mis d'accord sur l'utilisation du protocole de Diffie-Hellman.
      i. En l'absence d'authentification, expliquer pourquoi ce choix n'est pas judicieux.

/1
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………

      ii. Proposer une meilleure alternative.

/1
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………

Université de La Manouba
Ecole Nationale des Sciences de l'Informatique

Section :
Module : **Sécurité Informatique**
Classe : **II3**
Session : Rattrapage

A.U. : 2017/2018

Signatures des Surveillants

Nom : …………………… Prénom :……………………..

N° CIN : ……………………………………………………

N° d'inscription : ……………………………………………

Salle n° :………………… Place n° :…………………..

Signature de l'étudiant

✂- -

Exercice 1 :

On considère un système de chiffrement opérant sur l'alphabet {A, B, C, …, Z, _} dont chaque symbole est désigné par un nombre compris entre 0 et 26 :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	_
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Etant donnés une clé $K = K_0K_1K_2\ldots K_k$ et un message clair $M = M_0M_1M_2\ldots M_k$, le chiffré $C = C_0C_1C_2\ldots C_k$ est donné par :

$$\textit{Pour tout } i \in [0,k], \quad C_i = M_i + K_i \mod 27$$

C'est ce qu'on appelle le chiffrement de Vigenère.

1. Proposer une méthode de cryptanalyse d'un chiffrement de Vigenère sachant la taille de la clé K utilisée pour le chiffrement.

/1

……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………

2. Deux attaquants Oscar et Eve ont intercepté le texte ci-après et travaillent sur sa cryptanalyse.

HWQIO QVPIF TDIHT Y_WAF NGY_F COMVI CGEVZ CVIAF JDFZK YLYHG YGEHR SHMMX CVHBF AJYKN ZIXHP ZHEQY YJRHT YWMUK YKPBY YGEHA G_DY_ YWDTF MHFZK YZYHX CISVI CHIVZ

Oscar a réussi à déterminer la longueur de la clé K et veut l'envoyer de façon sécurisée à Eve. Pour cela, il utilise la clé publique RSA suivante (e,n)=(17,33).

a. A qui appartient cette clé publique ? Justifier votre réponse.

/0.5

……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………

b. La valeur reçue par Eve est 14. Quelle est la longueur de la clé ? Détailler la démarche.

/1.5

……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………

3. Eve a réussi à déchiffrer les deuxième et troisième symboles (i.e. K_1 et K_2) de la clé de chiffrement K. Elle les envoie à Oscar en utilisant la clé publique RSA (e,n)=(7,65). Les valeurs reçues par Oscar sont respectivement 48 et 4. Quelles sont les valeurs de K_1 et de K_2 ? Il n'est pas nécessaire de détailler la démarche.

Université de La Manouba
Ecole Nationale des Sciences de l'Informatique

Section :

Module : **Sécurité Informatique**

Classe : **II3**

Session : Rattrapage

A.U. : 2017/2018

Signatures des Surveillants

Signature de l'étudiant

Nom : …………………… Prénom :……………………..

N° CIN : ………………………………………………….

N° d'inscription : ……………………………………………

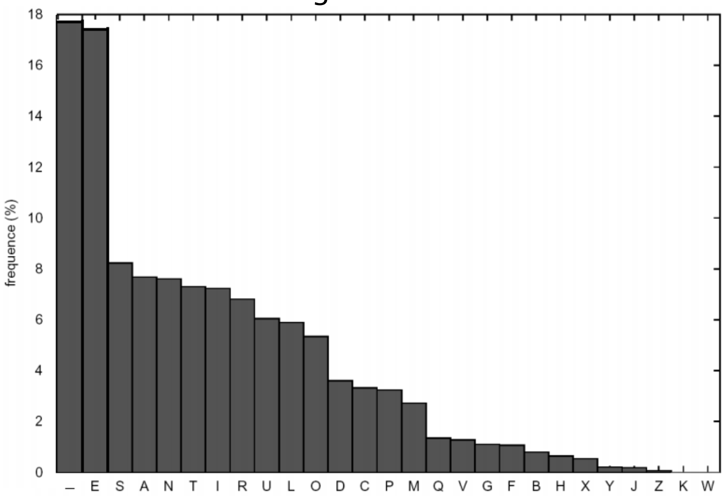
Salle n° :………………… Place n° :…………………..

/2

………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………

4. Maintenant que vous disposez de la longueur de la clé de chiffrement K et de deux des symboles de cette clé, regrouper les caractères du texte chiffré intercepté par Oscar par groupe de cette longueur et appliquer une analyse de fréquence pour le déchiffrer (utiliser la dernière page de l'examen pour illustrer la démarche). Préciser la clé utilisée pour le chiffrement et celle utilisée pour le déchiffrement (sous forme de chaîne de caractères).

   Nous rappelons que la répartition (%) des symboles utilisés dans un texte en français est résumée dans le diagramme suivant :



/3

………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………

Université de La Manouba
Ecole Nationale des Sciences de l'Informatique

Section :
Module : **Sécurité Informatique**
Classe : **II3**
Session : Rattrapage

A.U. : 2017/2018

Signatures des Surveillants

Nom : ……………………… Prénom :……………………..

N° CIN : ……………………………………………………….

N° d'inscription : ……………………………………………

Salle n° :…………………. Place n° :…………………..

Signature de l'étudiant

✂- -

H W Q I O Q V P I F T D I H T Y _ W A F N G Y _ F C O M V I C G E V Z C V I A F

J D F Z K Y L Y H G Y G E H R S H M M X C V H B F A J Y K N Z I X H P Z H E Q Y

Y J R H T Y W M U K Y K P B Y Y G E H A G _ D Y _ Y W D T F M H F Z K Y Z Y H X

C I S V I C H I V Z

H W Q I O Q V P I F T D I H T Y _ W A F N G Y _ F C O M V I C G E V Z C V I A F

J D F Z K Y L Y H G Y G E H R S H M M X C V H B F A J Y K N Z I X H P Z H E Q Y

Y J R H T Y W M U K Y K P B Y Y G E H A G _ D Y _ Y W D T F M H F Z K Y Z Y H X

C I S V I C H I V Z

H W Q I O Q V P I F T D I H T Y _ W A F N G Y _ F C O M V I C G E V Z C V I A F

J D F Z K Y L Y H G Y G E H R S H M M X C V H B F A J Y K N Z I X H P Z H E Q Y

Y J R H T Y W M U K Y K P B Y Y G E H A G _ D Y _ Y W D T F M H F Z K Y Z Y H X

C I S V I C H I V Z

Université de La Manouba
Ecole Nationale des Sciences de l'Informatique

Section :
Module : **Sécurité Informatique**
Classe : **II3**
Session : Principale

A.U. : 2018/2019

Signatures des Surveillants

Nom : ……………………… Prénom :……………………..

N° CIN : ………………………………………………………

N° d'inscription : ……………………………………………

Salle n° :………………… Place n° :…………………..

Signature de l'étudiant

Note

Examen de : …………………………..

Documents non autorisés

Appréciations du correcteur

QUIZ :

1. Un utilisateur souhaite chiffrer un très long message confidentiel avant de l'envoyer à l'un de ses partenaires. Quel algorithme est le plus approprié ?

/0.5 ☐ SHA1 ☐ Diffie – Hellman ☐ RSA ☐ DES

2. Quelles attaques ne pourraient pas affecter l'intégrité des données?

/0.5
☐ Craquage du mot de passe ☐ Port Scan
☐ IP Spoofing. ☐ Deni de service.

3. Quels procédés permettent-ils d'assurer la non-répudiation des données ?

/0.5
☐ La signature électronique ☐ Le hachage des mots de passes
☐ Le chiffrement à clé symétrique ☐ Le certificat électronique

4. Lesquelles des menaces suivantes permettent l'usurpation du mot de passe ?

/0.5
☐ Attaque par dictionnaire ☐ Cheval de Troie
☐ Spyware ☐ DDOS

5. Parmi les affirmations suivantes, laquelle correspond à une stratégie de défense plus robuste ?

/0.5
☐ Il vaut mieux interdire tout ce qui n'est pas explicitement permis.
☐ Il vaut mieux permettre tout ce qui n'est pas explicitement interdit.
☐ Il ne faut jamais utiliser une même paire de clés publique/privée pour sécuriser deux messages distincts
☐ Plus le système est simple, plus il est difficile à sécuriser.

Exercice 1 :

Le site d'une banque en ligne dispose d'une base de données clients présente sur un serveur de son parc informatique et contenant les informations personnelles et bancaires de ces derniers.

1. Identifier les actifs à protéger.

/0.5
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………

2. Parmi les critères suivants, lesquels la banque doit-elle satisfaire pour assurer la sécurité de son site:

/0.5
☐ Anonymat ☐ Insolvabilité
☐ Confidentialité ☐ Disponibilité

3. Quels sont, parmi les acteurs suivants, ceux qui constituent des agents de menace très probables?

/0.5
☐ Fournisseur d'accès Internet ☐ Client malveillant
☐ Web master du site de la banquee ☐ Pirate informatique

Université de La Manouba
Ecole Nationale des Sciences de l'Informatique

Section : A.U. : 2018/2019
Module : **Sécurité Informatique**
Classe : **II3**
Session : Principale

Nom : …… Prénom :……..

N° CIN : ……

N° d'inscription : ……

Salle n° :……. Place n° :……..

Signatures des Surveillants

Signature de l'étudiant

✂----------

4. Quels sont les facteurs qui différentient entre ces agents de menace ?

/0.5 ☐ Capacité ☐ Motivation ☐ Opportunité ☐ Impact

5. Citer au moins 2 menaces permettant de compromettre la sécurité d'un site de banque en ligne. **Expliquer**.

/1

Menace1 :……
……
……
Menace2 :……
……

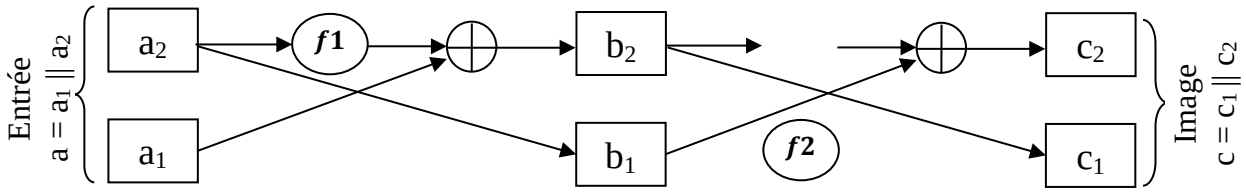
6. Proposer au moins une contre-mesure à implémenter pour contrer chacune des menaces citées dans la question précédente.

/1

Contre-mesure 1 :……
……
……
Contre-mesure 2 : ……
……
……

Exercice 2 :

On considère un diagramme de Feistel à deux rondes sur des chaînes de 8 bits avec deux fonctions $f1$ et $f2$ avec $f1(x) = x \oplus 1011$ et $f2(x) = \bar{x} \oplus 0101$ pour toute chaine de caractère de 4 bits x.



1. Donner les formules de chiffrement de ce diagramme en exprimant c_1 et c_2 en fonction de a_1, a_2, $f1$ et $f2$.

/1

C_1=……
……
……
C_2=……
……
……

2. Calculer l'image de l'entrée 11010011 par ce diagramme.

/1

……
……
……
……
……
……
……
……

Signatures des Surveillants

Signature de l'étudiant

Nom : …… Prénom :……..

N° CIN : …….

N° d'inscription : ……

Salle n° :……. Place n° :……..

✂----------

3. En utilisant les formules de la question 1, déterminer une chaine de 8 bits invariante, c'est-à-dire que son image par le diagramme est elle-même.

/1

……
……
……
……
……

4. Quelle est la condition que doit satisfaire $f1$ pour que le diagramme de Feistel n'ait pas de chaine invariante.

/1

……
……
……
……
……

Exercice 3 :

Un professeur P veut diffuser les notes de l'examen de sécurité à ses étudiants sur un même fichier excel en lecture seule où chaque ligne contient un ensemble d'information sur un étudiant (nom, prénom, n°CIN et note) et ce en respectant les règles suivantes :

Règle 1 : Les notes sont chiffrées de sorte que chaque étudiant ne peut déchiffrer que sa note.
Règle 2 : Le fichier est signé pour permettre à chaque étudiant de vérifier qu'il est déposé par son professeur.

Nous supposons que le professeur P possède une paire de clés publique/privée (PUB_P / PRIV_P). Nous supposons aussi que chaque étudiant Ei possède une paire de clés publique/privée (PUB_Ei / PRIV_Ei) et partage une clé symétrique K_Ei_P avec le professeur P.

1. Proposer une solution satisfaisant la règle 1 qui utilise un schéma de chiffrement symétrique.

/0.5

……
……
……

2. Proposer une solution satisfaisant la règle 1 qui utilise un schéma de chiffrement asymétrique.

/0.5

……
……
……

3. De quoi doivent disposer les étudiants pour pouvoir satisfaire la règle 2 ?

/0.5

……
……
……

Université de La Manouba
Ecole Nationale des Sciences de l'Informatique

Section :
A.U. : 2018/2019
Module : **Sécurité Informatique**
Classe : **II3**
Session : Principale

Signatures des Surveillants

Nom : …………………… Prénom :……………………..

N° CIN : ………………………………………………….

N° d'inscription : ……………………………………………

Salle n° :………………… Place n° :…………………..

Signature de l'étudiant

---

4. Lors de la création de leurs paires de clés publiques RSA, deux étudiants E1 et E2 ont choisi les mêmes nombres premiers p et q et ont donc pour clés publiques RSA respectivement (N, e1) et (N, e2) avec e1 et e2 premiers et distincts. Le professeur envoie le même message **m** chiffré par les clés publiques RSA de E1 et E2 (messages chiffrés **c1** et **c2**, respectivement).

   Expliquer comment Eve, qui intercepte les deux messages chiffrés et qui connait les clés publiques de E1 et E2, peut décrypter le message clair **m**.

   On rappelle que si deux nombres x et y sont premiers entre eux, il existe deux entiers u et v tels que $u.x + v.y = 1$.

/1

……………………………………………………………………………………………

5. <u>Application numérique :</u> On suppose qu'on est toujours dans les conditions de la question 4 et que p=137 et q=139, e1=11 et e2=7.
   a. Calculer les clés privées de E1 et E2. Expliquer la démarche

/1

d_{E1}……………………………………………………………………………………

d_{E2}……………………………………………………………………………………

   b. Les étudiants E1 et E2 ont eu la même note m=10. Donner c1 et c2.

/1

c1……………………………………………………………………………………

c2……………………………………………………………………………………

   c. Expliquer par application numérique comment Eve arrive à décrypter la note m à partir des notes chiffrées c1 et c2.

/2

……………………………………………………………………………………………

<u>Exercice 4 :</u>

Une entreprise dispose d'un réseau interne constitué de deux parties nommées respectivement LAN2 et LAN3 (voir schéma). L'architecture du réseau de l'entreprise comprend également une zone neutre dite zone démilitarisée (DMZ) représentée par le réseau LAN1et contenant les serveurs propres à l'entreprise étant susceptibles d'être accédées depuis l'extérieur

Signatures des Surveillants

Signature de l'étudiant

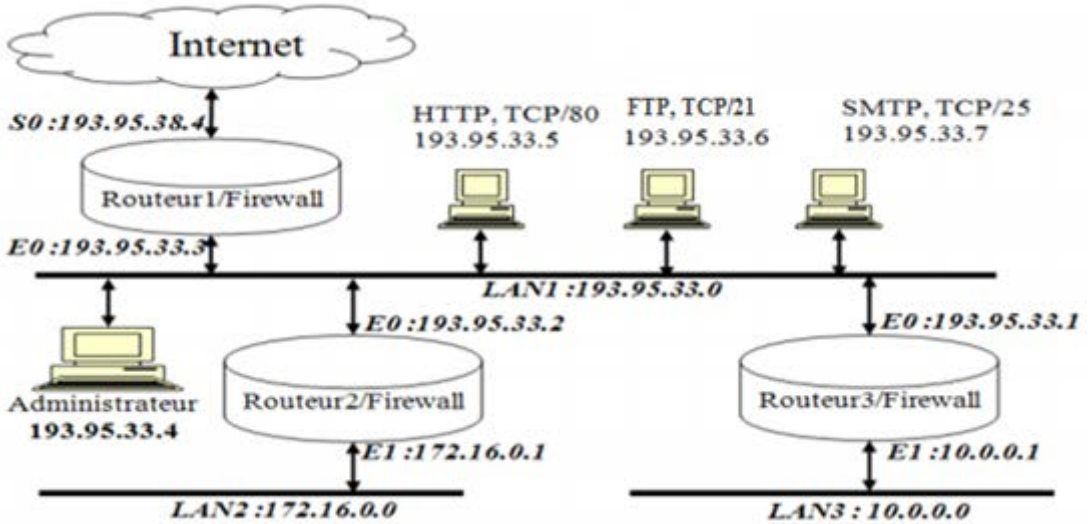
Nom : …… Prénom :……..

N° CIN : …….

N° d'inscription : ……

Salle n° :……. Place n° :……..

(Internet) et l'intérieur (LAN2 et LAN3). Les routeurs R1, R2 et R3 qui permettent aux différents LANs de communiquer entre eux et avec l'Internet implémentent des FIREWALLs sans état (stateless firewalls) qui contrairement aux Firewalls avec état (statefull firewalls) traitent chaque paquet de manière isolée et ne gardent pas en mémoire les états précédents de connexions qui les traversent.



1- Dans quels routeurs doit-on implémenter des règles de filtrage dans chacun des cas suivants (répondre par oui ou non et **remplir toutes les cases du tableau**):

/1

	R1	R2	R3
Permettre aux utilisateurs internes d'accéder aux serveurs HTTP, FTP et SMTP du LAN1.			
Permettre aux utilisateurs externes d'accéder aux serveurs HTTP, FTP et SMTP du LAN1.			
Permettre à la machine admin d'accéder aux ≠ LANs.			
Permettre aux utilisateurs du LAN1 d'accéder à Internet			

2- Les règles de filtrage implémentées au niveau du routeur R1 sont explicitées dans la Table 1 (on utilise S pour source et D pour destination) :

- Règle 1 : Toute demande de connexion vers le serveur FTP est autorisée.
- Règle 2 : Les réponses aux requêtes venant au serveur FTP sont autorisées.
- Règle 3 : Toute demande de connexion vers le serveur SMTP est autorisée.
- Règle 4 : Les réponses aux requêtes venant au serveur SMTP sont autorisées.
- Règle 5 : Toute autre connexion est explicitement interdite dans les deux sens.

N° règle	@IP S	@IP D	port S	Port D	Protocole	Action
1	toutes	193.95.33.6	tous	21	TCP	autoriser
2	193.95.33.6	toutes	21	tous	TCP	autoriser
3	toutes	193.95.33.7	tous	25	TCP	autoriser
4	193.95.33.7	toutes	25	tous	TCP	autoriser
5	toutes	toutes	tous	tous	tous	refuser

Table 1

Université de La Manouba
Ecole Nationale des Sciences de l'Informatique

Section :

A.U. : 2018/2019

Module : **Sécurité Informatique**

Classe : **II3**

Session : Principale

Signatures des Surveillants

Nom : ……………………… Prénom :……………………..

N° CIN : ……………………………………………………….

N° d'inscription : ……………………………………………

Salle n° :………………… Place n° :…………………..

Signature de l'étudiant

✂- -

a- Compléter le tableau suivant permettant aux utilisateurs externes d'accéder au serveur HTTP du LAN1.

/1

@IP S	@IP D	port S	Port D	Protocole	Action

b- Où doit-on placer les règles de filtrage ajoutées à la question précédente dans la Table 1 pour avoir un filtrage efficace ? **Justifier votre réponse.**

/0.5

……
……
……

3- Par mesure de sécurité, les machines situées dans la zone DMZ (machines du LAN1) ne doivent pas pouvoir initier une connexion vers le réseau externe (Internet).

a- Quelles sont les conséquences sur la sécurité des machines du LAN1 si cette règle n'est pas respectée ?

/0.5

……
……
……

b- Expliquer comment la politique de sécurité appliquée par le routeur filtrant R1, telle qu'elle a été définie dans la Table 1, ne vérifie pas cette règle.

/0.5

……
……
……
……
……
……

c- Proposer une solution pour remédier à ce problème.

/0.5

……
……
……
……
……
……
……

Université de La Manouba
Ecole Nationale des Sciences de l'Informatique

Section :
Module : **Sécurité Informatique**
Classe : **II3**
Session : Rattrapage

A.U. : 2018/2019

Signatures des Surveillants

Nom : …………………… Prénom :……………………..

N° CIN : ………………………………………………………

N° d'inscription : ……………………………………………

Salle n° :…………………. Place n° :…………………..

Signature de l'étudiant

✂- -

Note

Examen de : …………………………..

Documents non autorisés

Appréciations du correcteur

QUIZ :

1. Afin d'assurer l'intégrité d'un message M envoyé par A vers B, A envoie le message M accompagné de :

/0.5
- ☐ $DES_{K\_AB}(M)$
- ☐ $RSA_{K\_Privée\_B}(M)$
- ☐ CRC(M)
- ☐ H-MAC(M)

2. Lequel de ces algorithmes/protocole devrait être utilisé pour sécuriser au maximum l'échange de clés symétriques partagées entre deux entités A et B?

/0.5
- ☐ RSA
- ☐ TCP/IP
- ☐ SHA-1
- ☐ DES

3. Deux nœuds A et B ont chacun une paire de clés publique/privée (K_{A_Pub} ,K_{A_Prv}) et (K_{B_Pub} ,K_{B_Prv}) respectivement. A désire envoyer un message M à B

   a. Parmi les 4 opérations suivantes, cocher celle que A doit effectuer si son but principal est d'assurer la confidentialité de son message M:

/0.5
- ☐ Chiffrement de M avec sa clé publique K_{A_Pub}
- ☐ Chiffrement de M avec la clé publique de B K_{B_Pub}
- ☐ Chiffrement de M avec sa clé privée K_{A_Prv}
- ☐ Chiffrement de M avec la clé privée de B K_{B_Prv}

   b. Parmi les 4 opérations suivantes, cocher celle que A doit effectuer si son but principal est d'assurer la non-répudiation de son message M :

/0.5
- ☐ Chiffrement de M avec sa clé publique K_{A_Pub}
- ☐ Chiffrement de M avec la clé publique de B K_{B_Pub}
- ☐ Chiffrement de M avec sa clé privée K_{A_Prv}
- ☐ Chiffrement de M avec la clé privée de B K_{B_Prv}

4. Le chiffrement par substitution consiste à

/0.5
- ☐ Changer l'ordre des lettres dans le texte
- ☐ Organiser le texte en colonnes et changer l'ordre des colonnes
- ☐ Remplacer une lettre par une autre lettre ou un symbole
- ☐ Effectuer un XOR du texte avec une phrase clé

5. Quelle différence y a-t-il entre les chiffrements symétrique et asymétrique ?

/0.5
- ☐ Il n'y a aucune différence
- ☐ Le chiffrement symétrique est réversible alors que le chiffrement asymétrique ne l'est pas
- ☐ Le chiffrement symétrique nécessite des clefs publique/privée alors que le chiffrement asymétrique a besoin d'une clef secrète
- ☐ Le chiffrement symétrique nécessite une clef secrète alors que le chiffrement asymétrique utilise une paire de clefs publique/privée

Signatures des Surveillants

Nom : …………………… Prénom :……………………..

N° CIN : ………………………………………………….

N° d'inscription : ……………………………………….

Salle n° :…………………. Place n° :…………………..

Signature de l'étudiant

✂- -

6. Le but du DNS spoofing est de:

/0.5
- ☐ falsifier l'adresse IP d'un utilisateur
- ☐ falsifier un serveur DNS
- ☐ s'approprier l'adresse IP d'un utilisateur
- ☐ rediriger un utilisateur vers un site falsifié

7. Dans une attaque de type DDOS :

/0.5
- ☐ Une machine maître contrôle d'autres machines qui pourront réaliser une attaque distribuée sur la cible.
- ☐ Une machine maître inonde des machines cibles à l'aide d'applications distribuées
- ☐ Une machine maître redirige un utilisateur vers un site falsifié
- ☐ Une machine maître attaque des connexions sécurisées des machines cibles
- ☐ L'objectif est de paralyser la machine cible

8. Le rôle d'un Firewall est :

/0.5
- ☐ De créer des connexions sécurisées entre les machines internes et externes
- ☐ D'empêcher l'accès à certaines ressources du réseau interne
- ☐ De détecter les virus accompagnant les messages
- ☐ De filtrer les accès entre l'Internet et le réseau local

9. Le rôle d'une autorité de certification est de :

/0.5
- ☐ Etablir une clé secrète de chiffrement entre deux individus.
- ☐ Attribution d'une clé publique de chiffrement à une entité (individu ou entreprise..).
- ☐ Sécuriser l'envoi de messages.
- ☐ Distribuer de manière sécurisée des clés publiques/privés partagées à plusieurs entités (entreprises..).

Exercice 1 :

Kerberos permet une authentification centralisée et mutuelle entre un serveur du réseau (noté V) et un utilisateur se connectant à partir d'une machine notée C. Il est basé sur du chiffrement symétrique. Il utilise un serveur d'authentification (AS) et un serveur de ticket (TGS). Ces serveurs partagent une même clé symétrique noté K_{tgs}. l'AS connaît les mots de passe de tous les utilisateurs alors que le TGS partage une clé secrète K_v avec chaque serveur V.

La figure suivante décrit l'échange de messages dans la version 4 de Kerberos. Les notations suivantes sont utilisées.

ID_c	identité de l'utilisateur sur la machine C
ID_v	identité du serveur V
ID_{tgs}	identité du serveur TGS
AD_c	adresse réseau de C
K_c	clé symétrique partagée entre l'AS et C (dérivée du mot de passe de l'utilisateur)
$K_{c,tgs}$	clé de session symétrique partagée entre C et TGS
$K_{c,v}$	clé de session symétrique partagée entre C et V
TS	TimeStamp (date)
Lifetime	durée de vie
E(K, M)	chiffrer le message M avec l'algorithme symétrique E et la clé K.
||	concaténation

Signatures des Surveillants

Signature de l'étudiant

Nom : …… Prénom :……..

N° CIN : ……

N° d'inscription : ……

Salle n° :……. Place n° :……..

Notons que contrairement aux tickets, l' « authenticator » ne peut être utilisé qu'une seule fois.

Table Summary of Kerberos Version 4 Message Exchanges

(1) $\mathbf{C \rightarrow AS}$ $ID_c \| ID_{tgs} \| TS_1$

(2) $\mathbf{AS \rightarrow C}$ $E(K_c, [K_{c,tgs} \| ID_{tgs} \| TS_2 \| Lifetime_2 \| Ticket_{tgs}])$

$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$

(a) Authentication Service Exchange to obtain ticket-granting ticket

(3) $\mathbf{C \rightarrow TGS}$ $ID_v \| Ticket_{tgs} \| Authenticator_c$

(4) $\mathbf{TGS \rightarrow C}$ $E(K_{c,tgs}, [K_{c,v} \| ID_v \| TS_4 \| Ticket_v])$

$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$

$Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$

$Authenticator_c = E(K_{c,tgs}, [ID_C \| AD_C \| TS_3])$

(b) Ticket-Granting Service Exchange to obtain service-granting ticket

(5) $\mathbf{C \rightarrow V}$ $Ticket_v \| Authenticator_c$

(6) $\mathbf{V \rightarrow C}$ $E(K_{c,v}, [TS_5 + 1])$ (for mutual authentication)

$Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$

$Authenticator_c = E(K_{c,v}, [ID_C \| AD_C \| TS_5])$

(c) Client/Server Authentication Exchange to obtain service

1) Expliquer comment la clé $K_{c,tgs}$ est transmise d'une manière sécurisée à C et à TGS ? En déduire le rôle principal de l'envoi des Tickets

/1

……
……
……
……
……

2) Comment le TGS s'assure-t-il que le ticket du messsage 3 est créé par l' AS ?

/0.5

……
……
……
……

3) Un attaquant ayant capté les trois premiers messages échangés pourrait-il réutiliser le ticket « $Ticket_{tgs}$ » et s'authentifier à la place de C ? Expliquer.

/1

……
……
……
……
……
……

Université de La Manouba
Ecole Nationale des Sciences de l'Informatique

Section :
A.U. : 2018/2019
Module : **Sécurité Informatique**
Classe : **II3**
Session : Rattrapage

Signatures des Surveillants
Signature de l'étudiant

Nom : …………………… Prénom :……………………..

N° CIN : ……………………………………………………

N° d'inscription : ………………………………………

Salle n° :………………… Place n° :…………………..

✂- -

4) Comment le TGS s'assure-t-il que l'utilisateur qui lui présente $Ticket_{tgs}$ est bien celui qui l'a obtenu?

…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………

/0.5

5) Un attaquant ayant sniffé un ticket et un authenticator pourrait-il les utiliser prochainement ? Expliquer.

…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………

/0.5

6) Comment C peut-il confirmer, à partir du message 2, que le ticket obtenu est à envoyer au TGS?

…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………

/0.5

7) Quel problème peut surgir si le serveur ne s'authentifie pas auprès du client ?

…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………

/0.5

8) Peut-on utiliser kerberos comme système d'authentification SSO ? Expliquer

…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………

/0.5

Exercice 2 :

Soit X et Y deux entités désirant échanger des messages chiffrés en utilisant un algorithme symétrique. X et Y doivent se mettre d'accord sur une même clé symétrique KS sur un canal non-sécurisé.

1- Soit un protocole permettant à X et Y de se mettre d'accord sur une même clé symétrique K_S de longueur n bits. X choisit un challenge C et une clé partielle K_X puis envoie à Y ($K_X \oplus C$). Y choisit KY et répond par $K_X \oplus C \oplus K_Y$. Enfin, X répond par $C \oplus K_Y$. C, K_X et K_Y sont tous de longueur n bits. La clé sera $K_S = K_X \oplus K_Y$

Nom : …………………… Prénom :……………………..

N° CIN : ……………………………………………………

N° d'inscription : ……………………………………………

Salle n° :………………… Place n° :…………………..

Signatures des Surveillants

Signature de l'étudiant

✂- -

a- Expliquer comment X et Y retrouvent la clé K_S.

/1

……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………

b- Ce protocole est-il sécurisé? Expliquer ?

/1

……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………

2- Nous supposons maintenant que X et Y possèdent déjà une clé symétrique pré-partagée K. Cependant, pour renforcer la sécurité de cette clé, une clé de session K_s sera établie entre X et Y selon le protocole suivant: X envoie à Y le couple (R1, H(K⊕ R1)) alors que Y lui envoie le couple (R2, H(K⊕ R2)), H est une fonction de hachage, R1 et R2 sont deux nombres aléatoires générés par X et Y respectivement. X et Y utilisent les messages échangés pour dériver une clé de session K_s.

a- Que doit vérifier X pour s'assurer qu'il est en train de communiquer avec Y et vice versa ?

/1

……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………

b- Proposer une méthode permettant à X et Y de construire, en utilisant les variables des messages échangés, une clé symétrique K_S qui rende ce protocole résistant à l'attaque MITM (Man In The Middle).

/1

……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………

Exercice 3 :

On utilise les notations habituelles du RSA : p, q, n, φ(n), e et d

1. Donner les formules qui définissent les variables n, φ(n) et d en fonction d'une ou de plusieurs autres variables.

/1

n=……………………………………………………………………………………………
φ(n)=………………………………………………………………………………………
d=……………………………………………………………………………………………

2. On suppose que p=59, q=101 et e=11, calculer d.

/1

……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………

Signatures des Surveillants

Nom : ……………………… Prénom :……………………..

N° CIN : ……………………………………………………

N° d'inscription : ……………………………………………

Salle n° :…………………. Place n° :………………..

Signature de l'étudiant

✂- -

3. Alice envoie deux messages M1 et M2 en clair à Bob en associant à chaque message la signature effectuée avec sa clé privée K_{PrA}

Alice —— M1, Sig_K_{PrA}(M1) ——→ **Bob**
—— M2, Sig_K_{PrA}(M2) ——→

a. Montrer que Sig_K_{PrA}(M1*M2)= Sig_K_{PrA}(M1)* Sig_K_{PrA}(M2)

/0.5
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………

b. Un attaquant écoute les échanges et souhaiterait injecter un faux message pour l'envoyer à Bob en prétendant que c'est de la part d'Alice. Pour cela, il envoie le message suivant :

Alice M1*M2, Sig_K_{PrA}(M1)*Sig_K_{PrA}(M2) → **Bob**

Attaquant

Est-ce que cette attaque va réussir (c'est-à-dire que Bob va vraiment croire que c'est Alice qui a généré ce message) ? Expliquer.

/0.5
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………

Exercice 4 :

Vous êtes en charge de sécuriser le système d'information d'une université. Vous identifiez 2 sortes d'attaquants : interne au réseau et externe au réseau.

1. Sur une échelle de 1 à 4, estimez la capacité de chaque attaquant dans le cas où :
   a. L'université est la faculté des lettres de La Manouba

/0.5
Capacité de l'attaquant interne : ……………………………………………………………
Capacité de l'attaquant externe : ……………………………………………………………

   b. L'université est l'ENSI

/0.5
Capacité de l'attaquant interne : ……………………………………………………………
Capacité de l'attaquant externe : ……………………………………………………………

2. Lors d'une réunion de travail, vous expliquez à vos supérieurs, qui n'ont que des connaissances générales en informatique, les principes de certains concepts utilisés dans le domaine de la sécurité:

/2
Scan des ports : ……………………………………………………………………………
……………………………………………………………………………………………
Firewall : …………………………………………………………………………………
……………………………………………………………………………………………
IDS : ………………………………………………………………………………………
……………………………………………………………………………………………
Brute force : ………………………………………………………………………………
……………………………………………………………………………………………