Département de Réseaux & Télécommunications
2ème année Master
Année 2024 – 2025
Matière : Sécurité des réseaux de communication

Corrigé-type de l'examen final

Exercice 01 : questions de réflexion

1) Quelle est la différence principale entre une architecture avec DMZ et une architecture sans DMZ ?

Réponse : (0.5pt)

La différence principale entre une architecture avec DMZ et une architecture sans DMZ réside dans le fait que dans la première, le réseau local (zone interne) est directement lié à la zone externe en passant par le pare-feu tandis que dans la deuxième le réseau local (zone interne) est isolé de la zone externe en rajoutant une zone intermédiaire qui contient les services fournies (zone démilitarisée).

2) Donner un avantage et un inconvénient des architectures avec DMZ simple et en cascade ?

Réponse : (0.5pt)

	DMZ simple	DMZ en cascade
Avantage	Faible coût	Plus de sécurité
Inconvénient	Moins de sécurité	Coût élevé

3) Un employé est tombé malade, comment peut-on faire pour qu'il puisse travailler sans se présenter ?

Réponse : utiliser un VPN de type remote-access. **(0.5pt)**

4) Quel est le rôle d'un IDS ? Pourquoi le pare-feu ne suffit pas à lui seul ?

Réponse :

Le rôle principal d'un IDS est la détection des anomalies et des comportements malicieux. **(0.25pt)**

Le pare-feu ne suffit pas à lui seul car il ne fait pas d'analyse du trafic sur le réseau notamment vis-à-vis les risques provenant de l'intérieur. **(0.25pt)**

5) Soit un système RSA utilisant les nombres ***p***, ***q*** et ***e*** vus dans le cours et le TD. Est-il possible d'affecter les valeurs suivantes (justifier dans le cas où la réponse est négative).

(a) (p, q, e) = (3, 7, 5)

(b) (p, q, e) = (11, 3, 9)

(c) (p, q, e) = (7, 11, 9)

(d) (p, q, e) = (5, 9, 11)

(e) (p, q, e) = (5, 7, 3)

Réponse : (1pt)

(a) vrai (b) vrai (c, d, e) faux

6) Dans une université, le centre de calcul dispose d'un cluster destiné aux chercheurs pour effectuer des calculs intensifs à distance ; comment procéder pour ce faire (étapes à suivre) ?

Réponse : utiliser le protocole SSH. **(0.5pt)**

7) Deux universités veulent que les postes de leurs LANs puissent communiquer entre eux ; comment procéder pour ce faire (étapes à suivre) ?

Réponse : établir un VPN de type site-to-site. **(0.5pt)**

8) Quelle est la différence entre la cryptographie et la signature numérique ? Comment peuvent-elles s'appliquer ensemble ?

Réponse : (0.5pt)

- La cryptographie est un processus de chiffrement des données afin de garantir la confidentialité des données.
- La signature numérique est un processus qui inclut un mécanisme (ex. les fonctions de hachage) afin de garantir l'authentification et l'intégrité des données.

Ces deux principes peuvent être utilisés en combinaison comme suit : chiffrer les données par le biais de la clé publique du destinataire, signer le message chiffré par le biais de la clé privée de l'expéditeur et enfin chiffrer la signature numérique par le biais de la clé publique du destinataire. **(0.5pt)**

9) Quel est le rôle d'un certificat ?

Réponse : assurer l'authentification des entités à travers leurs clés publiques. **(0.5pt)**

Exercice 2

Alice et Bob utilisent chacun un système RSA en utilisant les paramètres suivants : Alice : (p = 11, q = 3 et e = 7) et Bob : (p = 3, q = 17 et e = 3).

1) Quelles sont les valeurs du module RSA et de l'indicatrice d'Euler pour chacun des deux systèmes (d'Alice et Bob) ?

Réponse : (2pts)

- Alice :

Module RSA $\phi\, n_{Alice} = p \times q = 33$; l'indicatrice d'Euler $\phi\,(n)_{Alice} = (p-1)\times(q-1) = 20$

- Bob :

Module RSA ϕ $n_{Bob} = p \times q = 51$; l'indicatrice d'Euler $\phi(n)_{Bob} = (p-1) \times (q-1) = 32$

2) Quelles sont les valeurs de la clé publique et la clé privée d'Alice et de Bob ?

Réponse : (2pts)

- Alice :

On cherche d avec : $e \times d + k \times \phi(n)_{Alice} = 1$

$d = 3$

Clé $publique_{Alice} = (33, 7)$

Clé $privée_{Alice} = (33, 3)$

- Bob :

On cherche d avec : $e \times d + k \times \phi(n)_{Bob} = 1$

$d = 11$

Clé $publique_{Bob} = (51, 3)$

Clé $privée_{Bob} = (51, 11)$

3) Alice veut envoyer un message m = 2 à Bob.

3.1) Calculer la valeur du message chiffré C (m) ?

Réponse : $C(m) = m^e \bmod n_{Bob} = 2^3 \bmod 51 = 8$ **(1pt)**

3.2) Lors de réception du message, comment Bob peut-il déchiffrer le message reçu ?

Réponse : $m = C(m)^d \bmod n_{Bob} = 8^{11} \bmod 51 = 2$ **(1pt)**

4) On considère maintenant qu'Alice veut envoyer le message m = 2 à Bob en rajoutant une signature numérique.

4.1) Calculer la valeur de la signature numérique liée au message chiffré C (m) ?

Réponse : $S(C(m)) = C(m)^d \bmod n_{Alice} = 8^3 \bmod 33 = 17$ **(1pt)**

4.2) Lors de réception du message, comment Bob peut-il s'assurer que le message reçu est effectivement de la part d'Alice ?

Réponse : $C(m) = S(C(m))^e \bmod n_{Alice} = 17^7 \bmod 33 = 8$ **(1pt)**

5) On considère maintenant qu'Alice veut envoyer le message m = 2 à Bob en rajoutant une signature numérique que seul Bob peut la vérifier.

5.1) Calculer la valeur de la signature numérique liée au message chiffré C (m) ?

Réponse : $C(S(C(m))) = S(C(m))^e \bmod \bmod n_{Bob} = 17^3 \bmod 51 = 17$ **(1pt)**

5.2) Lors de réception du message, comment Bob peut-il s'assurer que le message reçu est effectivement de la part d'Alice ?

Réponse : $S(C(m)) = C(S(C(m)))^d \bmod n_{Bob} = 17^{11} \bmod 51 = 17$ **(1pt)**

6.1) Alice veut envoyer un message m = 3 à Bob.

6.1.1) Calculer la valeur du message chiffré C (m) ?

Réponse : $C(m) = m^e \bmod n_{Bob} = 3^3 \bmod 51 = 27$ **(0.5pt)**

6.1.2) Lors de réception du message, comment Bob peut-il déchiffrer le message reçu ?

Réponse : $m = C(m)^d \bmod n_{Bob} = 27^{11} \bmod 51 = 3$ **(0.5pt)**

6.2) On considère maintenant qu'Alice veut envoyer le message m = 3 à Bob en rajoutant une signature numérique.

6.2.1) Calculer la valeur de la signature numérique liée au message chiffré C (m) ?

Réponse : $S(C(m)) = C(m)^d \bmod n_{Alice} = 27^3 \bmod 33 = 15$ **(0.5pt)**

6.2.2) Lors de réception du message, comment Bob peut-il s'assurer que le message reçu est effectivement de la part d'Alice ?

Réponse : $C(m) = S(C(m))^e \bmod n_{Alice} = 15^7 \bmod 33 = 27$ **(0.5pt)**

6.3) On considère maintenant qu'Alice veut envoyer le message m = 3 à Bob en rajoutant une signature numérique que seul Bob peut la vérifier.

6.3.1) Calculer la valeur de la signature numérique liée au message chiffré C (m) ?

Réponse : $C(S(C(m))) = S(C(m))^e \bmod \bmod n_{Bob} = 15^3 \bmod 51 = 9$ **(0.5pt)**

6.3.2) Lors de réception du message, comment Bob peut-il s'assurer que le message reçu est effectivement de la part d'Alice ?

Réponse : $S(C(m)) = C(S(C(m)))^d \bmod n_{Bob} = 9^{11} \bmod 51 = 15$ **(0.5pt)**

7) On suppose qu'Alice veut envoyer un message $m = (v_1, v_2, \ldots, v_n)$ à Bob.

7.1) Quelle est la taille de la signature numérique ?

Réponse : la taille de la signature numérique est *n*. **(0.5pt)**

7.2) Quel problème sera posé dans ce cas ?

Réponse : le problème posé est la taille de la signature qui influe négativement sur la transmission des données **(0.5pt)**

7.3) Proposer une solution à ce problème.

Réponse : la solution est d'utiliser une fonction de hachage pour rendre la signature numérique de taille fixe, en dépendant du contenu du message *m* et non pas sa taille. **(0.5pt)**