Département de Réseaux & Télécommunications
2ème année Master
Année 2023 – 2024
Matière : Sécurité des réseaux de communication

Enoncé + corrigé-type de l'examen final

Chargé de la matière : Mr. Laboudi Zakaria

Exercice 01 : questions de réflexion

1) Quand est-ce qu'on sécurise un réseau d'une organisation à travers des adresses privées RFC1918 ?

Les adresses privées RFC1918 sont utilisées pour créer des réseaux privés, notamment les réseaux locaux, étant donné qu'elles ne sont pas routables sur Internet.

2) Quand est-ce qu'on opte pour une architecture avec DMZ contre une architecture sans DMZ ?

On opte pour une architecture avec DMZ si l'organisation dispose d'un réseau local et veut également publier des services sur Internet (ex. serveurs mails, serveurs web, etc.). Sinon, on opte pour une architecture sans DMZ (i.e. on dispose uniquement d'un réseau local).

3) Un employé veut travailler à distance de chez lui ; comment procéder pour ce faire (étapes à suivre) ?

L'employé doit établir un **VPN d'accès à distance**. Deux étapes sont nécessaires :

a) un serveur de stockage en réseau (NAS)
b) le logiciel client installé sur une machine distante

4) Une application veut diffuser un même message (en termes de paquets) vers un groupe de récepteurs ; est-il possible d'intervenir :

(a) la cryptographie asymétrique

(b) la cryptographie symétrique

(c) la signature numérique

(a) On peut utiliser la cryptographie symétrique à condition que tous les récepteurs disposent de la même clé secrète.

(b) On ne peut pas utiliser la cryptographie asymétrique car le chiffrement est toujours réalisé à travers une clé publique d'un récepteur or chaque récepteur dispose de sa propre clé publique.

(c) On peut utiliser la signature numérique car elle est généralement réalisée à travers la clé privée de l'émetteur et vérifiée par sa clé publique au niveau du récepteur.

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) = (11, 3, 5) ➔ faux, car e n'est pas premier avec ϕ (n) = (n-1) × (q-1)

(b) (p, q, e) = (11, 9, 3) ➔ faux, car q n'est pas un nombre premier

(c) (p, q, e) = (7, 11, 9) ➔ faux, car e n'est pas premier avec ϕ (n) = (n-1) × (q-1)

(d) (p, q, e) = (5, 3, 11) ➔ faux, car e > ϕ (n)

(e) (p, q, e) = (5, 7, 3) ➔ faux, car e n'est pas premier avec ϕ (n) = (n-1) × (q-1)

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) ?

On utilise le protocole SSH pour accéder aux machines à distance. Pour ce faire, le serveur (machine du centre de calcul) et le client (machine du hercheur) mettent en place un canal sécurisé, ensuite، le client s'identifie auprès du serveur afin de pouvoir lancer des commandes en toute sécurité.

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

Les deux organisations doivent établir un **VPN site-à-site**.

Exercice 02 : cryptographie et signature numérique par RSA

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

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

- Pour Alice :

Le module RSA n = p × q = 51

L'indicatrice d'Euler ϕ (n) = (n-1) × (q-1) = 32

- Pour Bob :

Le module RSA n = p × q = 33

L'indicatrice d'Euler ϕ (n) = (n-1) × (q-1) = 22

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

- Pour Alice :

La clé publique (n, e) = (51, 3)

La clé privée (n, d) = (51, 11) (d est obtenu en appliquant l'algorithme d'Euclide étendu)

- Pour Bob :

La clé publique (n, e) = (33, 3)

La clé privée (n, d) = (33, 7) (d est obtenu en appliquant l'algorithme d'Euclide étendu)

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

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

$C(m) = m^e \bmod n = 2^3 \bmod 33 = 8$

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

$m = C(m)^d \bmod n = 8^7 \bmod 33 = 2$

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) ?

$S(C(m)) = C(m)^d \bmod n = 8^{11} \bmod 51 = 2$

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

$V(S(C(m))) = S(C(m))^e \bmod n = 2^3 \bmod 51 = 8 = C(m)$

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) ?

C (S (C (m))) = S (C (m))^{e} mod n = 2^{3} mod 33 = 8

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

S (C (m)) = S (C (m))^{d} mod n = 8^{7} mod 33 = 2

6) Refaire les questions 3 et 4 en considérant le message m = (2, 3).

6.1) Calculer la valeur du message chiffré C (m = 3) ?

C (m) = m^{e} mod n = 3^{3} mod 33 = 27

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

m = C (m)^{d} mod n = 27^{7} mod 33 = 3

6.3) Calculer la valeur de la signature numérique liée au message chiffré C (m = 3) ?

S (C (m)) = C (m)^{d} mod n = 27^{11} mod 51 = 3

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

V (S (C (m))) = S (C (m))^{e} mod n = 3^{3} mod 51 = 27 = C (m)

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

7.1) Quelle est la taille de la signature numérique ?

La taille de la signature est n car à chaque valeur v_i il correspond une signature S (v_i)

7.2) Quel problème sera posé dans ce cas ?

Cela pose un problème de performance lors des échanges de données dans le réseau car la taille d'un message m= (v_1, v_2, …, v_n) est doublée (message + signature).

7.3) Proposer une solution à ce problème.

La solution est d'intervenir une fonction de hachage pour rendre la taille de la signature indépendante de la taille des messages échangés (signature de taille fixe).

Bon courage