DS Réseau S4

Nom : Prénom :

Exercice 1 : Sécurité

Décrivez les différentes étapes pour qu'un client puisse s'authentifier auprès d'un serveur.

a. Chiffrement symétrique. Le serveur et le client se partage une clé commune. Décrivez les différentes étapes le plus précisément possible.

b. Chiffrement asymétrique. Qui possède la clé privée ? La clé publique ? Pourquoi ? Décrivez les étapes d'authentification.

Exercice 2 : Certificat.

Vous vous connectez à un site web : https://www.toto.fr. Vous obtenez le certificat de ce site. Vous avez déjà en local le certificat de l'autorité de certification.

1. Au vu des deux certificats ci-dessous, le site est-il authentifié ou non ? Justifiez votre réponse. On suppose que l'on utilise l'algorithme rsa (m^e mod (n) / c^d mod (n)).

Certificat www.toto.fr
Nom du site : www.toto.fr
Numéro : 871435
Autorité de certification : tata

Certificat autorité de certification tata
Nom : tata
Numéro : 521998
Autorité de certification : titi

Clé publique (n,e) : (7,5)
Hashage du certificat : 3
Signature : 3

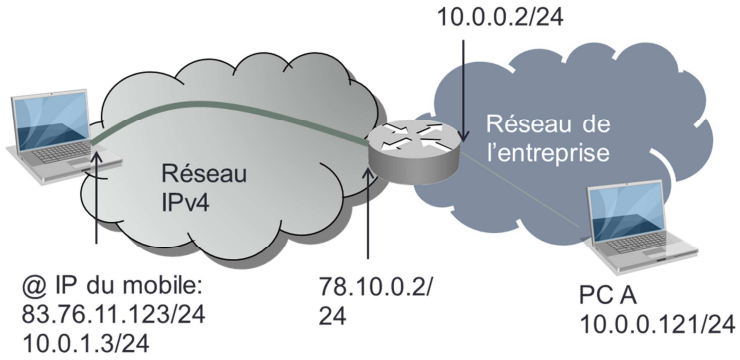
Clé publique (n,e): (20,5)
Hashage du certificat: 11
Signature : 19

Réponse :

2. Décrivez les différentes étapes permettant le chiffrement des données entre votre navigateur et le site www.toto.fr et inversement. Vous omettrez la partie authentification (déjà répondu à la question 1 – vous supposerez que le certificat était correct).

Exercice 3 : Tunnel

Nous considérons la topologie ci-dessous. Un tunnel a été établit entre le PC mobile et le serveur. Le tunnel est non sécurisé.



1. Décrivez les adresses IP (toutes) lors d'une communication entre le PC mobile et le PC A sur le réseau IPv4 (réseau Internet) et dans le réseau de l'entreprise.

2. Donnez la table de routage du nœud mobile.

Exercice 4 : DNS

Un serveur est responsable du domaine iut-toto.fr. Nous considérons le fichier de configuration suivant :

```
$TTL    86400
@       IN      SOA     localhost. root.localhost. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                          86400 )       ; Negative Cache TTL
;

@                       IN NS   localhost.
tata.iut-toto.fr.       IN NS   resir1.tata.iut-toto.fr.

resir1.tata.iut-toto.fr. IN A   192.168.0.16

machine1        IN A    132.1.1.1
machine2        IN A    132.1.1.2
machine3        IN A    132.1.1.3
machine4        IN A    132.1.1.4
```

```
machine5        IN A      132.1.1.5
                IN A      132.1.1.6
                IN A      132.1.1.7
                IN A      132.1.1.8
www             IN CNAME  machine1
ftp             IN CNAME  machine1
machine1        IN AAAA   2001::1
machine2        IN AAAA   2001::2
```

Questions :

1. Quelle est la réponse à une requête DNS pour machine1.iut-toto.fr ?

2. Quelle est la réponse à une requête DNS pour machine5.iut-toto.fr ?

3. Quelle est la réponse à une requête DNS pour ftp.iut-toto.fr ?

4. Quelle est la réponse à une requête DNS pour www.tata.iut-toto.fr ?

5. Quelle est la réponse à une requête DNS pour www.titi.tata.iut-toto.fr ?

<u>Exercice 5 : SNMP</u>

1. A quoi sert le protocole SNMP ? Qu'est-ce qu'il définit ?

2. Dans SNMP, qu’est-ce qu’un OID ?

3. Qu’est-ce que la MIB et comment est-elle structurée ?