Notes de TD de Sécurité internet et réseaux

Yann Miguel

11 octobre 2021

Table des matières

1 TD 1

Question 1

Il y a 7 règles qui parlent de sécurité des systèmes et réseaux, alors qu'il n'y en a que une qui parle de cryptographie.
On peux donc en conclure qu'il est plus important de renforcer le système que de chiffrer les données.

Question 2

Messages envoyés par A:
- $C_{K_B}^{RSA}(k)$
- $C_{k}^{AES}(Q)$
- $C_{K'_A}^{RSA}(H^{SHA1}(Q))$

Messages envoyés par B:
- $C_{k}^{AES}(R)$
- $C_{K'_B}^{RSA}(H^{SHA1}(R))$

Question 3

Si C connaît la clé privée de B avant la communication, les caractéristiques de sécurité compromises sont:
- confidentialité
- authentification

Question 4

Si C ne connaît la clé privée de b aprs la communication, les caractéristiques de sécurité compromises sont:
- confidentialité

2 TD 2

Question 1

C'est un document vérifiant qu'une clef publique appartient bel et bien à un utilisateur donné.
Le principe de vérification de certificat consiste à faire vérifier la validité du certificat par une autorité reconnue, en commençant par vérifier la signature du certificat.
Les primitives cryptographiques utilisées sont les fonctions de hachage et le chiffrement par clef publique.

Question 2

Jeu A

Le certificat A-2, qui est celui contenant la clef d'empreinte, est un certificat auto-signé. Il a l'autorisation de signer des certificat, dû à l'argument CA:true. Cependant, on ne considère comme autorité que le certificat A-1, et, A-2 n'étant pas signé par A-1, on ne peux pas accepter la clef d'empreinte comme appartenant à l'utilisateur.

Jeu B

Le certificat B-2 est signé par un certificat inconnu. On ne peux donc pas accepter la clef d'empreinte comme appartenant à l'utilisateur.