Notes de TD de Sécurité internet et réseaux

Yann Miguel

24 septembre 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