TP Certificat

On considère deux interlocuteurs **A** et **B**.

Chacun possède un couple clef publique/ clef privée : (KA, KA') et (KB, KB') respectivement. Ils communiquent au moyen de protocoles cryptographiques standards utilisant AES, RSA, et SHA256.

A envoie un message m à B

1. Expliquez le message $\mathbf{m_c}$ chiffré.

m= message plaintext , $\mathbf{m_c}$ le message chiffré , **H(m)** le haché , **Sign** le signé du haché

$m_c = C_{kA}(m) * RSA$

2. Quels sont les messages envoyés à **B**

$m_c = C_{kA}(m) * RSA$

$Sign = SHA256(m) * C_{kA'}$

3. Comment **B** peut-il s'assurer de ce que ce message vient de **A** ? (Bien vouloir détailler).

E= empreinte

Il compare l'égalité des empreintes :

$(Sign) * D_{kA} = h$

$D_{kB'}(m_c) * RSA = m$

$SHA256(m) = h'$

4. **A** souhaiterais à nouveau envoyer un message à **B** et apprend que la clé publique de **B** a été piratée mais que ce problème a été résolu par l'Ingénieur sécurité.
   Comment pourrait-il procéder pour s'assurer de ce que le message soit bien envoyé à **B** ? (Donnez-en une description détaillée)

1- Vérifier le certificat de B : la validité

a- SHA256 : hacher les informations contenues dans le certificat. = h

b- Déchiffrer la signature du certificat avec la clé publique de l'autorité certifiante (Récupération du haché) = h'

c- Comparer h & h'

d- Si h=h' certificat valide et donc la clé publique du B est valide

A peut envoyer le message

Sinon = il ne peut pas envoyer le message