TP - Chiffrement 2

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.

1. **A** envoie une question à **B**. Donnez précisément les messages envoyés.
   Soit q le message, M' le message chiffré, H(q) le Haché,
   Sign le chiffré du haché
   Les messages envoyés :
   $M' = C_{KB}(q) * RSA$
   $Sign = SHA256(q) * C_{KA'}$

2. **B** répond à **A**. Donnez précisément les messages envoyés (Y inclure le message déchiffré)
   $Mr = D_{KB'}(M') * RSA$
   $h = D_{KA}(Sign)$

   Calculons le haché de Mr : h' = SHA256(Mr)
   Comparer h et h'

   $M'' = C_{KA}(q') * RSA$
   $Sign = SHA256(q') * C_{KB'}$

3. On apprend que **C** avait dérobé la clef KB' **avant** cet échange de messages. Quelle(s) caractéristique(s) de sécurité sont alors compromises ?
Confidentialité, intégrité, authenticité, non-répuduation

4. Finalement, il s’avère que **C** n’avait obtenu la clef KB’ qu’**après** cet échange de messages.
Quelle(s) caractéristique(s) de sécurité sont maintenant compromises ?
Confidentialité

5. Est-il possible de limiter l’impact de la perte d’une clef privée après l’échange de messages ? Comment ?
Oui en utilisant des algorithmes de chiffrement robustes comme Diffie-Hellman