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.

2. **B** répond à **A**. Donnez précisément les messages envoyés (Y inclure le message déchiffré)

3. On apprend que **C** avait dérobé la clef KB’ **avant** cet échange de messages. Quelle(s) caractéristique(s) de sécurité sont alors compromises ?

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 ?

5. Est-il possible de limiter l’impact de la perte d’une clef privée après l’échange de messages ? Comment ?