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.
2. Quels sont les messages envoyés à **B**
3. Comment **B** peut-il s'assurer de ce que ce message vient de **A** ? (Bien vouloir détailler)
4. **A** souhaiterait 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 **A** ? (Donnez-en une description détaillée)