TP Chiffrement

On considère deux interlocuteurs **A** et **B**.
Chacun possède un couple clef publique/ clef privée : (KA, KA') et (KB, KB') respectivement.
A envoie un message **m** à **B**

1. De quel chiffrement s'agit-il ?
2. Expliquez le message $\mathbf{m_c}$ chiffré. Avec quel algorithme de chiffrement a-t-on chiffrer ce message ?
3. **B** déchiffre le message de **A** et le nomme $\mathbf{m_d}$. Expliquez ce message déchiffré
4. **B** répond à **A** avec un message **m'**. Expliquez ce message. Avec quel algorithme peut-on chiffrer ce message ?
5. De quel chiffrement s'agit-il ?
6. Quels sont les avantages de ce type de chiffrement ? Quels en sont les inconvénients ?
7. Avec quel autre algorithme de chiffrement pouvait-il chiffrer ce message ?
8. **A** souhaiterais à nouveau envoyer un message à **B** et ne dispose plus des clés de **B**. Avec quelle clé peut-il envoyer un message à **B** ? Où peut-il la trouver par exemple ?
9. **A** génère une clé de session et souhaiterais l'envoyer à **B.** Comment procèdera-t-il ?
10. On apprend qu'un utilisateur **C** avait dérobé la clé publique de **B** avant cet échange quelle(s) caractéristique(s) de sécurité sont alors compromise(s) ?