Partie B – Sécurisation

La base de données de Bob est hébergée sur un serveur auquel il accède depuis un client sur son ordinateur personnel. Pour sécuriser la connexion, un algorithme de chiffrement symétrique est utilisé.

7. Expliquer brièvement ce qu'est un algorithme de chiffrement symétrique.

La clé de chiffrement, notée C dans la suite, est choisie aléatoirement par le serveur à chaque connexion depuis un client. Afin que le chiffrement et le déchiffrement puisse se faire sans problème, le serveur doit envoyer au client la clé C de façon sécurisée.

8. Rappeler brièvement ce qu'est un algorithme de chiffrement asymétrique.

On suppose à présent que Bob possède une clé publique et une clé privée. La clé publique de Bob est supposée connue par le serveur.

9. Proposer alors une solution pour que le serveur puisse envoyer la clé C à l'ordinateur de Bob de façon sécurisée, c'est-à-dire pour que seul Bob puisse déchiffrer la clé envoyée.