Sécurisation des communications

Exercice 1 : Nombre de clés.

1. Un groupe de n personnes souhaitent communiquer entre elles au moyen de communications sécurisées par un chiffrement symétrique. Elles souhaitent pouvoir communiquer deux à deux. Combien de clés différentes seront nécessaires ?
2. Combien de clés différentes seront nécessaires avec un chiffrement asymétrique ?

Exercice 2 : Mots de passe.

1. Expliquer ce qu'est une attaque par recherche exhaustive
2. On dispose d'un alphabet de 95 caractères (les caractères ascii) pour définir un mot de passe.
   a. Combien de clés différentes peuvent exister avec 4 caractères?
   b. Combien de temps cela prendrait-il au maximum pour déchiffrer un message par recherche exhaustive (force brute), si le temps de calcul pour le déchiffrement est de 1 milliseconde par clé?
   c. Combien de clés différentes peuvent exister avec 10 caractères?
   d. Avec un ordinateur capable de tester 1 million de mots de passe par seconde, combien de temps cela lui prendra t-il pour explorer l'ensemble des combinaisons?
3. Pour les propriétaires d'un site internet, vaut-il mieux conserver dans la base de données, les mots de passe des clients, ou bien le hachage de chacun de ces mots de passe?

Exercice 3 : Chiffrement asymétrique.

Un utilisateur B souhaite échanger un message chiffré avec un utilisateur A en utilisant un chiffrement asymétrique. A possède une clé publique (AKpub) et une clé privée (AKpriv). B possède une clé publique (BKpub) et une clé privée (Bkpriv).

1. B souhaite chiffrer un message m afin de pouvoir l'envoyer à A :
   a. Quelle clé va être utilisée par B pour chiffrer le message m ?
   b. Quelle clé va être utilisée par A pour déchiffrer le message m ?
2. B souhaite signer son message avant de l'envoyer à A.
   a. Quelle clé va être utilisée par B pour signer le message m ?
   b. Quelle clé va être utilisée par A pour vérifier la signature du message m ?

Exercice 4 : Man in the middle.

1. Décrire les échanges qui ont lieux lors d'un échange de clés Diffie-Hellman intercepté par une attaque man in the middle.
2. Expliquez en quelques lignes le principe du protocole HTTPS (on s'intéressera uniquement à l'aspect Sécurité du protocole)
3. Décrire une tentative d'attaque man in the middle sur un protocole HTTPS.