Sécurisation des communications

Exercice 1 : Nombre de clés.

Un groupe de n personnes souhaitent communiquer entre elles, chacune, deux à deux. Elles souhaitent utiliser un moyen de communication sécurisé par un chiffrement symétrique. Combien de clés différentes seront nécessaires?

Exercice 2 : Méthode de chiffrement de Vigenère.

Si on appliquait cette méthode à un alphabet de 95 caractères (les caractères ascii) :

1. Combien de clés différentes peuvent exister avec 4 caractères?
2. 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?

Exercice 3 : Mots de passe

1. Combien de mots de passe différents de 10 caractères peuvent être générés à l'aide des 95 caractères ascii?
2. 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. Expliquer ce qu'est une attaque par recherche exhaustive.
4. 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 4 : RSA

1. (Optionnel) Quel est la valeur de 8^7 modulo 55? Appeler ce nombre n.
2. (Optionnel) Quel est l'inverse de n modulo 55? (rappel : $n \times inverse \equiv 1[n]$)
3. Dans un protocole de chiffrement asymétrique, les algorithmes de chiffrement et de déchiffrement sont-ils les mêmes?
4. Dans un protocole de chiffrement asymétrique, toutes les personnes possédant la clé publique de Bob peuvent lui envoyer un message?
5. Dans un protocole d'authentification, toutes les personnes possédant la clé publique de Bob peuvent vérifier sa signature émise?
6. Supposons que Bob envoie à Alice un message chiffré de la manière suivante: C = chiffrement(m,Bob_public_key). Est-ce qu'Alice peut authentifier Bob avec ce message?

Exercice 5 : Man in the middle

1. Décrire les échanges qui ont lieux lors d'un échange de clé Diffie-Hellman intercepté par une attaque man in the middle.
2. Décrire une tentative d'attaque man in the middle sur un protocole HTTPS.