QCM Cryptographie

Aucun document autorisé – Une seule bonne réponse par question.

1. Combien vaut 13^{18} mod 167 ?
    a. 11
    b. 91
    c. 128
    d. 32
2. Chiffrer ses données avec une clé secrète sert à assurer
    a. La non-répudiation
    b. L'intégrité
    c. La confidentialité
    d. L'authentification
3. Comment utilise-t-on les clés symétriques et asymétriques ensemble ?
    a. On utilise la clé asymétrique pour chiffrer la clé symétrique
    b. On utilise la clé symétrique pour amorcer le chiffrement, ensuite on chiffre le message avec la clé asymétrique
    c. Le message est d'abord chiffré avec la clé symétrique, puis par la clé asymétrique
    d. Le message est d'abord chiffré avec la clé asymétrique, puis par la clé symétrique
4. Lequel inconvénient des systèmes de chiffrement symétrique existe aussi dans les systèmes de chiffrement asymétriques ?
    a. Les correspondant doivent d'abord se connaitre
    b. On a besoin de stocker de façon sécurisée les clés privées pour chaque partie avec qui on communique
    c. Il est nécessaire de générer des nombres aléatoires de façon sécurisée
    d. Les correspondants doivent partager un secret avant d'entrer en communication
5. Bob veut envoyer un message chiffré à Alice. Qu'est-ce qui est vrai :
    a. Alice a besoin de la clé privée de Bob
    b. Alice a besoin de la clé publique de Bob
    c. Bob a besoin de la clé privée d'Alice
    d. Bob a besoin de la clé publique d'Alice
6. En parlant de cryptographie symétrique, laquelle de ces affirmations est fausses ?
    a. Elle n'assure pas la non-répudiation
    b. La gestion des clés est plus simple
    c. Ces algorithmes sont plus rapides que ceux de la cryptographie asymétrique
    d. Les clés utilisées pour chiffrer et déchiffrer sont les mêmes
7. Soit (n,e) la clé publique et (n,d) la clé privée (RSA) de Bob. Ce dernier a divulgué accidentellement la clé privée. Il décide de générer de nouvelles clés (n,e') et (n,d') en gardant le même module n. La sécurité sera-t-elle compromise ?
    a. Oui
    b. Non
    c. Non, si le nombre de chiffres dans e est au moins égal à la moitié du nombre de chiffres de n
    d. Cette opération est impossible
8. Le principe de Kerckhoff suppose que l'ennemi connaisse :
    a. La cryptographie
    b. La cryptanalyse
    c. L'algorithme utilisé
    d. La clé publique

9. 15 personnes désirent communiquer de façon confidentielle, chacune avec chaque autre, en utilisant un algorithme de chiffrement asymétrique. De combien de clés privées auront-elles besoin ?
    a. 225
    b. 15
    c. 105
    d. 14
10. Soit (n,e) = (133,25) une clé publique RSA. Quel est l'exposant d de la clé privée correspondante ?
    a. 9
    b. 13
    c. 21
    d. 97
11. Soit (n,e) = (899,23) une clé publique RSA. Quel sera le résultat de chiffrement du message M=30 ?
    a. 30
    b. 78
    c. 217
    d. 336
12. 15 personnes désirent communiquer de façon confidentielle, chacune avec chaque autre, en utilisant un algorithme de chiffrement symétrique. De combien de clés symétriques auront-elles besoin ?
    a. 225
    b. 15
    c. 105
    d. 14
13. Le premier échange des clés dans le protocole HTTPS se fait de la façon suivante
    a. Le client reçoit la clé publique du serveur, génère une clé symétrique aléatoire, chiffre la dernière avec la clé publique du serveur et l'envoie au serveur
    b. Le client génère une clé symétrique aléatoire, chiffre la dernière avec sa clé privée et l'envoie au serveur
    c. On utilise l'algorithme Diffier-Hellmann
    d. Le serveur génère une symétrique aléatoire, chiffre la dernière avec sa clé publique et l'envoie au client
14. Laquelle de ces fonctions est une fonction de hashage ?
    a. DES
    b. SHA 256
    c. AES 256
    d. RC5
15. Lequel de ces algorithmes n'est pas un chiffrement symétrique ?
    a. AES
    b. RC5
    c. IDEA
    d. RC4