Échanges sécurisés de données
QCM de révision

L'objectif de ce QCM est de réviser l'ensemble des concepts étudiés au cours du module. Plusieurs réponses sont possibles.

1. La science qui étudie la faiblesse des algorithmes de chiffrement est :
   A - La cryptographie
   B - La cryptanalyse
   C - La cryptologie

2. La sécurité d'un chiffrement dépend :
   A - De l'algorithme utilisé
   B - De la taille de la clé de chiffrement
   C - Du média de transport
   D - De la confidentialité de la clé de chiffrement

3. Le chiffrement à clé symétrique utilise :
   A - 1 clé secrète
   B - 1 clé de session
   C - 1 clé privée

4. Lequel de ces algorithmes n'est pas utilisé pour le chiffrement symétrique :
   A - AES
   B - DES
   C - RSA

5. Lors de l'envoi d'un message, le chiffrement symétrique permet :
   A - D'assurer la confidentialité des données
   B - De garantir l'authentification de l'émetteur
   C - Les deux

6. Quel est l'intrus :
   A - MD5
   B - DSA
   C - BLOWFISH

7. Le chiffrement asymétrique est aussi appelé :
A - Chiffrement à clés secrètes
B - Chiffrement à clé publique
C - Chiffrement à clé de session

8. Une clé privée peut correspondre à plusieurs clés publiques ?
A - Vrai
B - Faux
C - C'est l'inverse

9. Dans le cas du chiffrement d'un message, qui utilise la clé publique ?
A - L'expéditeur
B - Le destinataire
C - Les deux

10. Dans le cas de la signature électronique, qui utilise la clé privée ?
A - L'expéditeur
B - Le destinataire
C - Les deux

11. L'intégrité d'un message peut être assurée par :
A - Le hachage des données uniquement
B - Le chiffrement des données uniquement
C-Obligatoirement un chiffrement des données et une signature électronique
D - L'utilisation d'un certificat

12. Quel est l'inconvénient des algorithmes de chiffrement asymétrique ?
A - Ils ne permettent pas l'authentification
B - Ils demandent énormément de ressources machines
C - La clé publique est connue de tous

13. Qu'est-ce qui permet de garantir une clé publique ?
A - Une clé de session
B - L'authentification de l'expéditeur
C - Un certificat
D - Une signature électronique

14. Un certificat peut contenir :
- **A -** La clé privée de l'utilisateur ou de la machine authentifiée
- **B -** La clé publique de l'utilisateur ou de la machine authentifiée
- **C -** La clé publique de l'autorité de certification

15. Lequel de ces algorithmes est un algorithme de hachage ?
- **A -** IDEA
- **B -** SSL
- **C -** SHA

16. La norme actuelle des certificats est :
- **A -** X802.11
- **B -** X509V3
- **C -** LDAP

17. Une autorité de certification signe les certificats qu'elle délivre avec :
- **A -** Sa clé privée
- **B -** Sa clé publique
- **C -** La clé publique du propriétaire du certificat

18. Un algorithme de hachage :
- **A -** Utilise une clé secrète
- **B -** Nécessite l'utilisation d'un certificat
- **C -** Est non réversible
- **D -** Léger et rapide à exécuter

19. Dans les systèmes de cryptographie modernes les algorithmes sont :
- **A** - Publics
- **B** - Privés

20. Une clé privée :
- **A** - Ne doit jamais circuler sur un réseau
- **B** - Peut circuler sur un réseau

21. Ma clé publique peut être distribuée à tous mes correspondants :
- **A** - Vrai
- **B** - Faux

22. Pour envoyer un message confidentiel :
- **A** - Je le chiffre avec ma clé privée
- **B** - Je le chiffre avec la clé publique de mon correspondant
- **C** - Je le chiffre avec ma clé publique

23. Pour signer un message, je chiffre le hash du message
- **A** - Avec la clé publique de mon correspondant
- **B** - Avec ma clé publique
- **C** - Avec ma clé privée

24. Un protocole de chiffrement à clé publique :
- **A** - Est très rapide et permet de chiffrer de grandes masses données
- **B** - Est assez lent et doit être réservé à des cas particuliers

25. Un protocole de chiffrement à clé secrète :
- **A** - Est très rapide et permet de chiffrer de grandes masses données
- **B** - Est assez lent et doit être réservé à des cas particuliers

26. La blockchain permet :
- **A** – D'accroitre la sécurité des échanges
- **B** – De se passer du tiers de confiance nécessaire à l'authentification
- **C** – D'optimiser les délais de traitement en faisant appel à un réseau proche
- **D** – De réduire le risque d'altération du registre

27. Le réseau TOR permet :
- **A** – De dissimuler son adresse IP
- **B** – De se passer du tiers de confiance nécessaire à l'authentification
- **C** – De dissimuler l'adresse IP du serveur
- **D** – De réduire le risque d'altération des enregistrements

28. Un VPN permet :
- **A** – D'accroitre la sécurité des échanges
- **B** – De se passer du tiers de confiance
- **C** – D'optimiser les délais de traitement en faisant appel à un réseau proche
- **D** – De cacher son adresse IP

29. Six personnes (A B C D E F) souhaitent s'échanger des documents confidentiels deux à deux en utilisant un chiffrement symétrique. Combien de clés sont nécessaires :

A - 5
B - 12
C - 15
D - 25

30. Six personnes (A B C D E F) souhaitent s'échanger des documents confidentiels deux à deux en utilisant un chiffrement asymétrique. Combien de clés sont nécessaires :

A - 5
B - 12
C - 15
D - 25