Examen Final d'introduction à la sécurité des technologies émergentes. Le 13/01/2025. Durée : 1h30

Nom et Prénom :……..……

Partie I : Choisissez la bonne réponse (une seule réponse est correcte).

1. La cybersécurité vise principalement à protéger :
A. La vitesse des systèmes
B. La confidentialité, l'intégrité et la disponibilité
C. Les performances matérielles
D. Les applications open source
✅**Réponse : B**

2. Une **menace** est :
A. Une faiblesse interne
B. Un événement pouvant exploiter une vulnérabilité
C. Une politique de sécurité
D. Un mécanisme de chiffrement
✅**Réponse : B**

3. La formule correcte du risque est :
A. R = P + I
B. R = P × I
C. R = P − I
D. R = I / P
✅**Réponse : B**

4. L'utilisation de l'IA en cybersécurité permet principalement :
A. De supprimer les pare-feu
B. D'analyser de grands volumes de données automatiquement
C. D'éliminer le chiffrement
D. De bloquer tous les utilisateurs
✅**Réponse : B**

5. Dans un modèle IoT, le graphe G = (V, E) représente :
A. Les clés cryptographiques
B. Les attaques connues
C. Les objets connectés et leurs connexions
D. Les protocoles réseau
✅**Réponse : C**

6. L'objectif principal de l'automatisation en cybersécurité est :
A. Réduire les coûts humains uniquement
B. Réagir rapidement avant propagation de l'attaque
C. Supprimer l'authentification
D. Éviter le chiffrement
✅**Réponse : B**

7. Le TMR (Temps Moyen de Réponse) est défini par :
A. TMR = Td × Ta
B. TMR = Td + Ta + Tc
C. TMR = Tc − Td
D. TMR = Ta / Td
✅**Réponse : B**

8. Une entropie élevée signifie :
A. Une clé plus courte
B. Une clé plus prévisible
C. Une incertitude cryptographique élevée
D. Une clé non chiffrée
✅**Réponse : C**

9. La sécurité du cloud repose principalement sur :
A. Compression, sauvegarde, virtualisation
B. Chiffrement, authentification, redondance
C. Pare-feu uniquement
D. Accès public
✅**Réponse : B**

10. Pourquoi l'IoT augmente-t-il la surface d'attaque ?
A. Les objets sont isolés
B. Chaque objet est un point d'entrée potentiel
C. Les objets sont chiffrés
D. Les objets utilisent TLS
✅**Réponse : B**

11. Le principe fondamental du Zero Trust est :
A. Faire confiance au réseau interne
B. Ne jamais faire confiance, toujours vérifier
C. Autoriser par défaut
D. Chiffrer uniquement l'extérieur
✅**Réponse : B**

12. Le composant qui **applique** la décision d'accès est :
A. PDP
B. PIP
C. PEP
D. SIEM
✅**Réponse : C**

13. Dans Zero Trust, la confiance T(u) est :
A. Fixe
B. Binaire
C. Probabiliste et contextuelle
D. Permanente
✅**Réponse : C**

14. Si T(u) < T_min, l'accès est :

A. Autorisé
B. Chiffré
C. Refusé
D. Journalisé seulement
✅**Réponse : C**

15. La segmentation réseau permet de :
A. Augmenter la bande passante
B. Réduire la surface d'attaque
C. Supprimer les journaux
D. Désactiver TLS
✅**Réponse : B**

16. Dans la théorie des graphes appliquée à ZTA, le réseau sécurisé est :
A. Le graphe initial
B. Un sous-graphe autorisé
C. Un graphe complet
D. Un graphe aléatoire
✅**Réponse : B**

17. Le risque Zero Trust augmente lorsque :
A. La valeur de la ressource diminue
B. La confiance diminue
C. Le chiffrement augmente
D. Les logs augmentent
✅**Réponse : B**

18. Pourquoi TLS est-il indispensable en Zero Trust ?
A. Pour accélérer le trafic
B. Pour sécuriser même les flux internes
C. Pour remplacer MFA
D. Pour éviter les graphes
✅**Réponse : B**

19. Le PDP prend ses décisions en fonction de :
A. A uniquement
B. R uniquement
C. A, R et C
D. L'adresse IP seulement
✅**Réponse : C**

20. La politique du moindre privilège consiste à :
A. Donner tous les droits
B. Donner les droits minimum nécessaires
C. Supprimer les accès
D. Donner des droits temporaires illimités
✅**Réponse : B**

21. La blockchain est principalement :
A. Une base de données centralisée
B. Une base de données distribuée et immuable
C. Un serveur web
D. Un algorithme de chiffrement
✅**Réponse : B**

22. Chaque bloc d'une blockchain contient :
A. Un mot de passe
B. Un hash du bloc précédent
C. Une clé privée
D. Une adresse IP
✅**Réponse : B**

23. L'immuabilité de la blockchain repose sur :
A. Le chiffrement symétrique
B. Le hachage cryptographique
C. La compression
D. Le stockage cloud
✅**Réponse : B**

24. Quel est l'objectif principal d'un mécanisme de consensus ?
A. Accélérer le réseau
B. Synchroniser les horloges
C. Valider l'état du registre distribué
D. Chiffrer les blocs
✅**Réponse : C**

25. La blockchain publique se caractérise par :
A. Un accès restreint
B. Une autorité centrale
C. Une participation ouverte
D. Une base locale
✅**Réponse : C**

26. Pourquoi une attaque de type "réécriture de l'historique" est-elle difficile ?
A. À cause du chiffrement AES
B. À cause du hachage chaîné des blocs
C. À cause du cloud
D. À cause des pare-feu
✅**Réponse : B**

27. Le problème du "double spending" est résolu par :
A. Le chiffrement homomorphe
B. Le consensus distribué
C. Le stockage local
D. L'authentification simple
✅**Réponse : B**

28. Un smart contract est :
A. Un contrat papier
B. Un programme auto-exécutable sur la blockchain
C. Une clé privée
D. Un protocole réseau
✅**Réponse : B**

29. Quelle propriété rend la blockchain compatible avec le modèle Zero Trust ?
A. Centralisation
B. Transparence et vérification distribuée
C. Absence de chiffrement
D. Stockage local
✅**Réponse : B**

30. La principale limite actuelle des blockchains publiques est :
A. L'absence de sécurité
B. La scalabilité et le coût énergétique
C. Le manque de cryptographie
D. L'absence de consensus
✅**Réponse : B**

Partie I :

Exercice 2 (5 points):

On utilise Paillier simplifié :
p = 7
q = 11
g = 1 + n

r=1

1. Calculer n
2. Calculer λ = lcm(p−1, q−1)
3. Calculer μ
4. Chiffrer :
   m1 = 4
   m2 = 6
5. Vérifier :
   Enc(m1) × Enc(m2) mod n² = Enc(m1 + m2)

Solution

Le système de Paillier simplifié est défini par :

p = 7, q = 11,
g = 1 + n,
r = 1.

1. Calcul de n
   n = p × q = 7 × 11 = 77, n² = 5929
2. Calcul de λ
   λ = lcm(p − 1, q − 1) = lcm(6, 10) = 30.
3. Calcul de μ
   Pour g = 1 + n, on a :
   $\mu = \lambda^{-1} \bmod n$.

On cherche l'inverse de 30 modulo 77 :
30 × 18 = 540 ≡ 1 (mod 77).
Donc μ = 18.

4. Chiffrement
   Pour un message m, le chiffré est :

$c = g^m \cdot r^n \bmod n^2$.
Comme r = 1 et g = 1 + n, on obtient :
$c = (1 + n)^m \bmod n^2$.

Ici $n^2 = 77^2 = 5929$ et g = 78.

Pour $m_1 = 4$:
$c_1 = 78^4 \bmod 5929 = 309$.

Pour $m_2 = 6$:
$c_2 = 78^6 \bmod 5929 = 463$.

5. Vérification de la propriété homomorphe

On calcule :
$c_1 \cdot c_2 \bmod n^2 = 309 \times 463 \bmod 5929 = 771$.

Or $m_1 + m_2 = 4 + 6 = 10$, et
$Enc(10) = 78^{10} \bmod 5929 = 771$.

Donc :
Enc(4) × Enc(6) mod n² = Enc(10),
ce qui confirme la propriété additive du chiffrement de Paillier.

Réponses finales :

n = 77
λ = 30
μ = 18

Enc(4) = 309
Enc(6) = 463

Vérification :
309 × 463 mod 5929 = 771 = Enc(10).