MODULE CRYPTOSYSTÈMES ET SÉCURITÉ INFORMATIQUE

Examen Final

Durée : 2h15

Nom	:	.....
Prénom	:	.....

Élément 1 – *Cryptosystèmes*

Exercice 1 (*Chiffrement HILL*)

Décrypter le texte suivant qui a été obtenu en appliquant le chiffrement de HILL sur des blocs de taille 2 sur un mot de la langue française :

$$gzatzxjihvbreosu$$

sachant que le chiffrement du mot `chiffrer` avec la même clé donne le chiffré $jvfrtqnb$.

N.B. On travail sur le corps $(\mathbb{Z}/26\mathbb{Z})$

Exercice 2 (*Chiffrement RSA*)

Alice souhaite maintenant utiliser le système de chiffrement RSA. Pour créer sa clé RSA, Alice choisit les nombres premiers $p = 29$ et $q = 41$, et $e = 3$ comme exposant de chiffrement.

1. Calculez l'exposant de déchiffrement d.
2. Précisez la clé publique et la clé privée d'Alice.
3. Bob veut transmettre le message $x = 20$ à Alice. Calculez son chiffré.
4. Alice a reçu le chiffré $c = 2$. Que doit-elle calculer pour obtenir le clair x ? (on ne demande pas dans cette question d'exécuter le calcul).
   Maintenant vous allez aider Alice à déchiffrer $c = 2$ en utilisant le théorème des restes chinois.
5. Calculez une relation de Bezout entre p et q.
6. Montrez que $2^d = 2^{19} \ mod \ p$ (indication : utilisez le petit théorème de Fermat).
7. Calculez $2^{19} \ mod \ p$ (indication : utilisez le moins possible de multiplications et réduisez modulo p à chaque fois..)
8. Utilisez le théorème chinois pour déduire des questions précédentes la valeur de $2^d \ mod \ 1189$ et en déduire x.

Élément 2 – *Sécurité Informatique*

Exercice 1

1. Citez les différentes type des systèmes de détection d'intrusion ?

   .....
   .....
   .....
   .....
   .....

2. Dessinez un exemple d'architecture réseau à trois zones utilisant les Pare-feu ?

   .....
   .....
   .....
   .....
   .....

3. Donnez les deux besoins pour utiliser les fonctions de masquage et de translation d'adresse ? Citez quelques technique pour réponde à ces besoins ?

   .....
   .....
   .....
   .....
   .....

4. Citez en détails les principaux protocoles de tunneling VPN ?

   .....
   .....
   .....
   .....
   .....

5. Décririez-vous le fonctionnement du protocole SAML (Avec un schéma) ?

.....
.....
.....
.....
.....

6. Citez trois référentiels relatifs à la sécurité des Systèmes d'Information ?

.....
.....

Exercice 2 (*QCM*)

1. La stéganographie est l'art de
   - ☐ cacher une message
   - ☐ chiffrer une message
   - ☐ crypter une message
2. L'authentification est processus qui garantit que
   - ☐ la personne demandant l'accès est l'utilisateur prévu
   - ☐ la donnée demandé pendant un l'accès est disponible
   - ☐ l'attaquant demandant l'autorisation d'accès à un service
3. Que signifie ECC ?
   - ☐ Elliptique Curve Cryptography
   - ☐ Elliptique Connexe Cryptography
   - ☐ Elliptique Curve Cryptology
4. Les étapes de chiffrement AES sont :
   - ☐ XOR du bloc entrant avec la sous-clé
   - ☐ Substitution (D-Box)
   - ☐ Décalage de lignes
   - ☐ Mélange des colonnes
5. Les protocoles de chiffrement du WiFi :
   - ☐ WEP
   - ☐ RSA
   - ☐ WPA
   - ☐ WPA2
6. Les objectifs fondamentaux de l'ingénierie sociale
   - ☐ Commettre une fraude
   - ☐ Rendre un service non disponible
   - ☐ Intrusion réseau
   - ☐ chiffrer les données personnels
7. Les vulnérabilités des infrastructures
   - ☐ Sabotage
   - ☐ Phishing
   - ☐ Écoute clandestine
   - ☐ Vishing
8. Les précautions pour sécuriser un site web
   - ☐ Utiliser des mots de passe complexes
   - ☐ Installer un certificat SSL pour passer votre site en HTTP
   - ☐ Choisissez le bon hébergeur
9. Le fonctionnement de SIEM comme bien d'étapes
   - ☐ 1
   - ☐ 3
   - ☐ 4
   - ☐ 5
10. Les risques liés aux supports amovibles
    - ☐ Perte d'informations
    - ☐ Introduction de logiciels malveillants
    - ☐ Perte financière

11. Le nombre des différences entre crypto-monnaie est
    - ☐ 1
    - ☐ 2
    - ☐ 3
    - ☐ 4
12. Les différentes attaques touchant réseaux sociaux
    - ☐ Ingénierie sociale
    - ☐ Phishing
    - ☐ Usurpation d'identité de marque
    - ☐ Propagation des application légitime
13. Les technologies pour la sécurisation des Web Services
    - ☐ WS-Security
    - ☐ L'architecture GXE
    - ☐ AXIS
    - ☐ Rampart légitime
14. Les outiles les plus importants dans la sécurisation des smartphones sont :
    - ☐ Détecteurs de rootkits
    - ☐ MSSM
    - ☐ La Chain Of Trust
15. Les méthodes classique pour mettre fin aux attaques DOS et DDOS
    - ☐ Le Blackholing
    - ☐ BC
    - ☐ Optimisation de la bande passante
16. Mesures pour sécuriser un réseau IoT
    - ☐ Bloquer les adresses IP non autorisées.
    - ☐ Utiliser des Firewalls, des IDS et des IPS
    - ☐ Faire les mises à jour régulières des Objets connectés seulement.
17. Types d'attaques de PHISHING
    - ☐ Spear phishing
    - ☐ Waling
    - ☐ Vishing
    - ☐ Pharming
18. Les services du Cloud
    - ☐ IaaS
    - ☐ CaaS
    - ☐ PaaS
    - ☐ SaaS
19. Nombre de risques liés aux développements la Blockchain
    - ☐ 4
    - ☐ 6
    - ☐ 8
20. Les attaques qui touchent la couche physique sont
    - ☐ Attaque active
    - ☐ Attaque passive
    - ☐ Attaque hybride
21. Les risques lies au télétravail
    - ☐ PHISIHNG
    - ☐ Les faux ordres de virement
    - ☐ Ransomware
22. Le processus de Pen-Test est divisé en
    - ☐ 4 étapes.
    - ☐ 5 étapes.
    - ☐ 6 étapes.
23. Les Vulnérabilités logicielles sont
    - ☐ Débordement de tampon
    - ☐ Injection SQL
    - ☐ Cross-Site coding
24. Étapes pour cacher son adresse email
    - ☐ remplacer - masquer - Chiffrer (ROT13)
    - ☐ masquer - remplacer - Chiffrer (ROT13)
    - ☐ Chiffrer (ROT13) - masquer - remplacer
25. La cybersécurité est la pratique consistant à
    - ☐ protéger les systèmes, les réseaux et les programmes
    - ☐ Tester les systèmes, les réseaux et les programmes
    - ☐ Chiffrer les systèmes, les réseaux et les programmes
26. Le dangers de ransomware est
    - ☐ Atteinte à la réputation
    - ☐ fichiers perdus
    - ☐ Argent gagné par rançon

Bon Courage