Page 1

Ac S

Sécurité Informatique

1CS — Contrôle intermédiaire — Mardi 05.04.2016 — Durrée 1h

Nom : ..... Groupe : .....

Prénom : .....

Aucune, une ou plusieurs réponses sont possibles aux questions suivantes :

Barème 0.5 pt : *réponse juste*, -0,25pt : *réponse fausse*, 0 : *non cochée*.

(0.5pt) **1.** Quelle est parmi ces transformations celle qui procure le plus grand pourcentage de sécurité à l'AES ?
- [x] A SubByte.
- [ ] B MixColumn.
- [ ] C Key Expansion.

(0.5pt) **2.** Une recherche exhaustive sur les 56 bits d'une clé DES nécessite environ 112 heures. Combien de temps faudrait-il approximativement pour une clé de 64 bits?
- [ ] A 128 heures.
- [ ] B 128 jours.
- [x] C plus de 3 ans.

(0.5pt) **3.** Dans les systèmes de cryptographie modernes les algorithmes sont publics.
- [x] A vrai.
- [ ] B Faux.

(0.5pt) **4.** Un spyware est :
- [x] A. un logiciel.
- [ ] B. Un type de SPAM.
- [ ] C. Un virus.

(0.5pt) **5.** Un SCADA est :
- [x] A. Un courrier electronique.
- [ ] B. Un ver qui attaque les systèmes SCADA.
- [ ] C. Une publicité.

(0.5pt) **6.** Le chiffrement de Hill nécessite une clé dont la forme est :
- [x] A Une matrice carrée.
- [ ] B Un nombre modulo 26.
- [ ] C Une matrice quelconque avec des éléments modulo 26.

(0.5pt) **7.** La Round CONstant matrix est utilisée dans :
- [x] A La diversification des clés.
- [ ] B La transformation SubByte.
- [ ] C La transformation MixColumns.

(0.5pt) **8.** L'adressage de la table S-Box se fait par une adresse de :
- [x] A 8 bits.
- [ ] B 16 bits.
- [ ] C 256 bits.

(0.5pt) **9.** En sécurité informatique, un Zombi désigne un ordinateur:
- [x] A. Contrôlé à l'insu de son utilisateur par un cybercriminel.
- [x] B. qui peut être infesté par un ver ou un cheval de Troie.
- [ ] C. qui appartient à un black hat.

(0.5pt) **10.** Dans le cas d'un chiffrement AES avec une clé de 256 bits, on utilise :
- [ ] A. 14 sous clés de 256 bits.
- [x] B. Des sous clés de 128 bits.
- [x] C. Des blocs de donné de 128 bits.

Acs

(0.5pt) **11.** Trouvez le ou les intrus :

- ○ **A.** Les vers.
- ○ **B.** Les virus exécutables.
- ○ **C.** Les trojans.
- ● **D.** Avast.
- ○ **E.** Les virus de boot.

(0.5pt) **12.** Un Ver informatique :

- ● **A.** C'est un logiciel malveillant nécessitant des connexion réseaux pour se propager.
- ● **B.** N'a pas besoin d'un programme hôte pour se reproduire.
- ● **C.** Exploite les différentes ressources de l'ordinateur qui l'héberge pour assurer sa reproduction.
- ○ **D.** Me permet de formater l'ordinateur.

(0.5pt) **13.** Dans le cas du chiffrement asymétrique, qui utilise la clé secrète ?

- ○ **A.** L'expéditeur.
- ● **B.** Le destinataire.
- ○ **C.** Les deux.

(0.5pt) **14.** Quel est le nom du dispositif logiciel contrôlant les flux d'informations entre votre ordinateur et le réseau ?

- ○ **A.** La carte wifi.
- ○ **B.** Le gateway.
- ● **C.** Le firewall (pare-feu).
- ○ **D.** L'anti-virus.

(0.5pt) **15.** Un Firewall (pare-feu) :

- ○ **A.** Vérifie la présence de virus sur mon ordinateur.
- ● **B.** Bloque des connexions non désirées à mon ordinateur.
- ○ **C.** Efface les spams dans mon courriel.

(0.5pt) **16.** Trouvez le ou les intrus.

- ○ **A.** IDEA
- ○ **B.** DES
- ● **C.** RC4
- ○ **D.** Blowfish
- ○ **E.** Serpent

(0.5pt) **17.** Trouvez le ou les intrus.

- ○ **A.** MEHARI
- ○ **B.** EBIOS
- ○ **C.** ISO 17799
- ● **D.** IEEE 754

(0.5pt) **18.** Trouvez le ou les intrus.

- ○ **A.** Kerberos
- ○ **B.** SSL
- ● **C.** TCP/IP

(0.5pt) **19.** Un Virus exécutable .. :

- ○ **A.** et un Trojan c'est la même chose.
- ● **B.** bloque les fichiers exécutables.
- ○ **C.** prend le contrôle de mon ordinateur.

(0.5pt) **20.** Les logiciels espions (spyware) et publicitaires (adware) peuvent arriver sur votre ordinateur :

- ○ **A.** En téléchargeant et en installant des programmes.
- ○ **B.** En surfant sur un site web.
- ● **C.** Les deux réponses ci-dessus.