

Exercice 1

- 1- Définir ces trois termes :
Disponibilité
Confidentialité
L'intégrité
- 2- Citez 2 types d'attaques Man in the middle l'homme du milieu)
- 3- Parmi les mots de passe suivants, quels sont ceux qui sont les plus sécurisés ?
☐ caroline
☐ 24031988
☐ UV67!rvO
☐ r78ww23X
☐ motdepasse
- 4- Que permet de faire un pare-feu ?
- 5- Quelle est la différence entre une ACL étendue et ACL standard
- 6- Quelle est la différence entre le cryptage symétrique et le cryptage asymétrique ?
- 7- Remplir le tableau suivant à partir des mots ci-dessous :

Cryptage symétrique	Cryptage asymétrique	Fonction de hachage

RSA, DES, Code de César, MD5, AES, SHA-224

- 8- A quoi sert le hachage
- 9- La fonction de hachage SHA-512 produit un haché de 512 bits qui se compose des caractères hexadécimaux. Combien de caractères y-a-t-il dans ce haché ?
- 10- Donner un exemple d'un logiciel de la cryptographie (permet de crypter des messages ou des fichiers)
- 11- Quel est le rôle d'une signature électronique ?
- 12- Définir un certificat numérique
- 13- Un certificat numérique permet de garantir :
☐ Disponibilité
☐ Confidentialité
☐ Intégrité
☐ Non-répudiation
☐ Authentification
- 14- Une signature numérique permet de garantir :
☐ Disponibilité
☐ Confidentialité
☐ Intégrité
☐ Non-répudiation
☐ Authentification
- 15- La cryptographie permet de garantir :

Sécuriser une infrastructure digitale

- ☐ Disponibilité
- ☐ Confidentialité
- ☐ Intégrité
- ☐ Non-répudiation
- ☐ Authentification

16- Une fonction de hachage permet de garantir :

- ☐ Disponibilité
- ☐ Confidentialité
- ☐ Intégrité
- ☐ Non-répudiation
- ☐ Authentification

17-Définir une autorité de certificat.

Exercice 2

- 1-** En utilisant un codage de César dont la clef est 12, coder le texte : «JE SUIS UN STAGIAIRE IDOSR»
- 2-** En utilisant un codage de César dont la clef est 5, décoder le texte : «JCFRJS IJ KNS IJ RTIZQJ»
- 3-** En utilisant un code de Viginère de la clé « ISTA » Crypter le message suivant :
SECURITE INFORMATIQUE