socrative

Name _____
Date _____

Apprentis Telecom TD1

Score _____

1. Vocabulaire : Parmi ces phrases, laquelle ou lesquelles sont correctes ?

(A) L'ennemi a déchiffré un message.

(B) J'ai crypté et envoyé mon numéro de carte bancaire.

(C) Mon correspondant a déchiffré mon message. Nous espérons que personne d'autre n'a pu le décrypter.

(D) La NSA vient de proposer un décryptage du DES en moins de 5 minutes.

2. Un attaquant actif peut détruire un message qui transite.

(T) True

(F) False

3. Un attaquant passif peut briser l'intégrité d'un message.

(T) True

(F) False

4. Dans un protocole de **chiffrement symétrique**, celui qui détient une information secrète est (plusieurs réponses possibles) :

(A) L'émetteur

(B) Le destinataire

(C) Tout le monde

(D) Celui qui signe

(E) Celui qui vérifie la signature

5. Dans un protocole de **signature asymétrique**, celui qui détient une information secrète est (plusieurs réponses possibles) :

(A) L'émetteur

(B) Le destinataire

(C) Tout le monde

(D) Celui qui signe

(E) Celui qui vérifie la signature

6. Dans un protocole de **chiffrement asymétrique**, celui qui détient une information secrète est (plusieurs réponses possibles) :

(A) L'émetteur

(B) Le destinataire

(C) Tout le monde

(D) Celui qui signe

(E) Celui qui vérifie la signature

7. Pour un attaquant, il est plus difficile de trouver une collision sur une fonction de hachage, que de trouver un premier antécédent.

(T) True

(F) False

8. Comment s'appelait la machine utilisées par les Allemands pendant la Seconde Guerre Mondiale pour chiffrer leurs communications ?

9. Qu'est-ce que le principe de Kerckhoff (1883) ?

(A) Les spécifications d'un système de chiffrement ne doivent pas être publiques.

(B) Nul autre que le destinataire d'un chiffrement asymétrique ne doit détenir la clef secrète.

(C) La clef publique doit toujours être publique.

(D) La sécurité d'un cryptosystème ne doit reposer que sur le secret de la clef.

(E) Il ne faut jamais utiliser deux fois de suite la même clef pour un chiffrement symétrique.

(F) Il n'existe aucun cryptosystème qui soit inconditionnellement sûr.

10. Quel est le nom des 3 besoins principaux auquel répond la cryptologie ?