socrative

Name _____
Date _____

Apprentis TD3 Crypto Asym

Score _____

1. Les systèmes de chiffrement symétriques sont plus rapides que les systèmes de chiffrement asymétriques.

(T) True

(F) False

2. Les systèmes de chiffrement symétriques sont plus sûrs que les systèmes de chiffrement asymétriques.

(T) True

(F) False

3. La sécurité de RSA repose sur la difficulté de trouver des grands nombres premiers.

(T) True

(F) False

4. La technique de Diffie-Hellman permet de construire un secret commun que l'on appelle une clef.

(T) True

(F) False

5. La clef publique est toujours publique.

(T) True

(F) False

6. Les paires de clefs pour les protocoles basés sur le problème du logarithme discret dans les courbes elliptiques sont beaucoup plus petites que celles utilisées dans les protocoles basés sur le problème du logarithme discret dans les corps finis.

(T) True

(F) False

7. Pourquoi a-t-on besoin de cryptologie asymétrique ?

(A) Pour avoir des protocoles plus sécurisés.

(B) Pour permettre de créer des signatures.

(C) Pour ne pas communiquer sa clef publique.

(D) Pour s'échanger un secret commun sans information préalable.

(E) Pour avoir des protocoles plus rapides.

8. Comment s'appellent les créateurs de RSA ? (Pour la syntaxe, la réponse attendue est sous la forme : Alice, Bob et Charlie)

9. Dans RSA, le calcul du message m à la puissance l'exposant public e s'effectue

(A) modulo N

(B) modulo Phi(N) (l'indicatrice d'Euler de N)

(C) modulo Phi(N) (l'indicatrice d'Euclide de N)

10. Le plus grand entier, produit de deux facteurs premiers, factorisé est de l'ordre de :

(A) 700 bits

(B) 800 bits

(C) 900 bits

(D) 1024 bits

(E) 256 bits, comme les clefs de l'AES

11. Dans le groupe (Z/7Z)^* constitué des entiers non nuls modulo 7, si l'on prend 3 comme générateur, qui est un logarithme discret de 6 ?

(A) log_3(6) = 1

(B) log_3(6) = 2

(C) log_3(6) = 3

(D) log_3(6) = 4

(E) log_3(6) = 5

(F) log_3(6) = 6

(G) log_3(6) = 0

12. L'algorithme "Pas de Bébé, pas de Géant"

(A) casse RSA en O(C) si C est le modulo de RSA.

(B) casse RSA en O(sqrt(C)) si C est le modulo de RSA.

(C) casse Diffie-Hellman en O(C) si C est l'ordre du groupe considéré.

(D) casse Diffie-Hellman en O(sqrt(C)) si C est l'ordre du groupe considéré.