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 ?

Enigma

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 ?

Confidentialité, authentification, intégrité

socrative

Name _____
Date _____

Apprentis TD2

Score _____

1. Un attaquant dispose de 3 couples clairs/chiffrés (M1, C1), (M2, C2), (M3, C3). A partir de ces données, et de l'écoute de la consommation électrique, il parvient à déchiffrer un message C4. De quelle type d'attaque s'agit-il ?

(A) Attaque à chiffré seul.
✓ (B) Attaque à clair connu.
(C) Attaque à clair choisi, non adaptative.
(D) Attaque à clefs liées.
(E) Attaque à clair choisi, adaptative.
✓ (F) Attaque par canaux auxiliaires.

2. Il existe un système de chiffrement inconditionnellement sûr.

✓ (T) True
(F) False

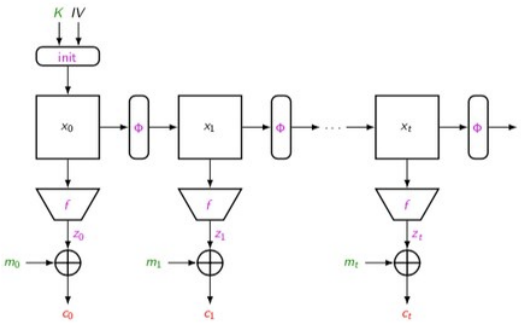
3. Si un attaquant est obligé d'effectuer 2^x opérations pour réaliser son attaque, on estime qu'il s'agit d'un niveau de sécurité raisonnable. Que vaut x ?

128

4. 128 bits est une taille de clef suffisante pour l'AES.

✓ (T) True
(F) False

5. Qu'est-ce que ceci ?



(A) Une fonction de hachage.
✓ (B) Un système de chiffrement à flot.
(C) Un système de chiffrement par bloc.
(D) L'état interne d'un MAC.
(E) Un Linear Feedback Shift Register (LFSR).

6. Que faut-il spécifier publiquement dans un chiffrement à flot (plusieurs réponses possibles) ?

- (A) La fonction de hachage.
- ✓ (B) La fonction de transition.
- (C) La fonction de tamis.
- ✓ (D) La fonction de filtrage.
- (E) La fonction d'état interne.
- (F) La fonction de transmission.

7. Un chiffrement par bloc ne chiffre que des messages de taille fixe. Que doit-on utiliser si l'on souhaite chiffrer une donnée d'une grande longueur ?

un mode opératoire

8. Le DES (Data Encryption Standard) est cassé depuis 1972.

- (T) True
- ✓ (F) False

9. Sélectionnez les phrases correctes.

- ✓ (A) Le DES est cassé par force brute.
- (B) Le Douple DES est cassé par force brute.
- ✓ (C) Une attaque Meet-in-the-middle casse le Douple DES.
- (D) Une attaque Man-in-the-middle casse le Double DES.
- (E) Une attaque Meet-in-the-middle casse le Triple DES.
- (F) Une attaque Man-in-the-middle casse le Triple DES.

10. L'AES (Advanced Encryption Standard) utilise :

- ✓ (A) Un cadencement de clef.
- ✓ (B) Des boîtes S, pour la non linéarité.
- ✓ (C) Des blocs de 128 bits.
- (D) Des réseaux de Feistel.
- ✓ (E) Des tailles de clef de 128 bits.
- (F) Une représentation dans un anneau Neuthérien.

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)

Rivest, Shamir et Adleman

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.

6. Que faut-il spécifier publiquement dans un chiffrement à flot (plusieurs réponses possibles) ?

(A) La fonction de hachage.

(B) La fonction de transition.

(C) La fonction de tamis.

(D) La fonction de filtrage.

(E) La fonction d'état interne.

(F) La fonction de transmission.

7. Un chiffrement par bloc ne chiffre que des messages de taille fixe. Que doit-on utiliser si l'on souhaite chiffrer une donnée d'une grande longueur ?

8. Le DES (Data Encryption Standard) est cassé depuis 1972.

(T) True

(F) False

9. Sélectionnez les phrases correctes.

(A) Le DES est cassé par force brute.

(B) Le Douple DES est cassé par force brute.

(C) Une attaque Meet-in-the-middle casse le Douple DES.

(D) Une attaque Man-in-the-middle casse le Double DES.

(E) Une attaque Meet-in-the-middle casse le Triple DES.

(F) Une attaque Man-in-the-middle casse le Triple DES.

10. L'AES (Advanced Encryption Standard) utilise :

(A) Un cadencement de clef.

(B) Des boîtes S, pour la non linéarité.

(C) Des blocs de 128 bits.

(D) Des réseaux de Feistel.

(E) Des tailles de clef de 128 bits.

(F) Une représentation dans un anneau Neuthérien.