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.

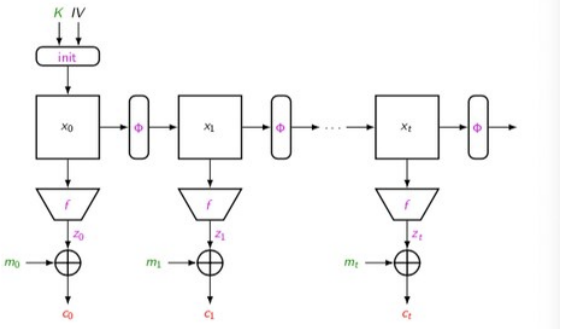
(T) True
(F) False

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 ?

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 ?

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.