Commencé le	jeudi 1 février 2024, 14:34
État	Terminé
Terminé le	jeudi 14 mars 2024, 14:05
Temps mis	41 jours 22 heures
Points	15,00/15,00
Note	**10,00** sur 10,00 (**100**%)

Question 1

Correct

Note de 1,00 sur 1,00

En considérant un chiffrement 3DES en mode chiffrement par bloc (Electronic Code Book), lequel de ces encodages limite au maximum les chances de l'attaquant ?

Veuillez choisir une réponse.

a. Un encodage binaire sur un nombre de bits égal à l'entropie avec bourrage de zéros

b. Un bourrage de zéros suivi d'un encodage ASCII

c. Un encodage binaire sur un nombre de bits égal à l'entropie avec bourrage aléatoire ✓

d. Un encodage ASCII avec bourrage aléatoire

e. Un encodage binaire sur un nombre de bits égal à l'entropie avec bourrage de uns

Votre réponse est correcte.

La réponse correcte est : Un encodage binaire sur un nombre de bits égal à l'entropie avec bourrage aléatoire

Question 2

Correct

Note de 1,00 sur 1,00

Vous disposez d'une source parfaitement aléatoire qui produit des messages de 64 bits. Vous êtes contraint à faire passer vos messages dans un canal chiffré par 3DES utilisé en mode bloc (Electronic Code Book). Comment vous assurer que l'utilisation du mode bloc ne compromet pas la sécurité de vos données ?

Veuillez choisir une réponse.

a. Compresser la source

b. Utiliser du bourrage aléatoire

c. Faire un XOR du message chiffré avec un vecteur d'initialisation.

d. Chiffrer une seconde fois

e. Aucune de ces techniques n'est nécessaire tant que l'attaquant ne peut pas faire d'attaque à texte connu ✓

Votre réponse est correcte.

La réponse correcte est : Aucune de ces techniques n'est nécessaire tant que l'attaquant ne peut pas faire d'attaque à texte connu

Question 3

Correct

Note de 1,00 sur 1,00

Quel est l'objectif principal de l'utilisation d'algorithme de chiffrement par bloc, tel que DES, en mode de chaînage de bloc (Cipher Bloc Chaining) ?

Veuillez choisir une réponse.

a. Éviter que deux blocs chiffrés se déchiffrent avec la même clé

b. Améliorer la vitesse de déchiffrement

c. Tromper les attaquants sur le mode de chiffrement

d. Prévenir que deux messages identiques donnent le même bloc chiffré ✓

e. Ajouter le nombre de bit du vecteur d'initialisation à la taille effective de la clé

Votre réponse est correcte.

La réponse correcte est : Prévenir que deux messages identiques donnent le même bloc chiffré

Question 4

Correct

Note de 1,00 sur 1,00

Vous êtes en possession d'une boîte noire qui fait 1 000 000 de déchiffrements à la seconde. Quel est le temps nécessaire pour monter une attaque par force brute à l'aide d'un texte connu (vous possédez un exemplaire chiffré et déchiffré du même texte) pour un algorithme ayant une taille effective de clé de 56 bits ?

Veuillez choisir une réponse.

- a. Approximativement 14 millions d'années
- b. Approximativement 1 000 ans
- c. Approximativement 2 000 ans ✓
- d. Approximativement 5 700 ans
- e. Approximativement 11 400 ans

Votre réponse est correcte.

La réponse correcte est : Approximativement 2 000 ans

Question 5

Correct

Note de 1,00 sur 1,00

Il est "raisonnablement" possible de réaliser une attaque de force brute sur un algorithme de substitution mono alphabétique si l'alphabet de source ne contient que 28 lettres.

Veuillez choisir une réponse.

- Vrai
- Faux ✓

La réponse correcte est « Faux ».

Question 6

Correct

Note de 1,00 sur 1,00

Parmi les tailles de clés suivantes, laquelle est la plus appropriée pour un chiffrement AES ?

Veuillez choisir une réponse.

- a. 56 bits.
- b. 64 bits.
- c. 128 bits. ✓
- d. 2048 bits.

Votre réponse est correcte.

La réponse correcte est : 128 bits.

Question 7

Correct

Note de 1,00 sur 1,00

Il n'est pas possible de réaliser une attaque de force brute par essai de toutes les clés pour l'algorithme AES avec une quantité de ressources raisonnable.

Veuillez choisir une réponse.

- Vrai ✓
- Faux

La réponse correcte est « Vrai ».

Question 8

Correct

Note de 1,00 sur 1,00

L'utilisation de l'algorithme de chiffrement 3DES est préférable à celle de l'algorithme AES car elle assure un niveau de protection adéquat et une meilleure performance

Veuillez choisir une réponse.

- Vrai
- Faux ✓

La réponse correcte est « Faux ».

Question 9

Correct

Note de 1,00 sur 1,00

Étant donné que le vecteur d'initialisation (IV) utilisé dans les algorithmes de chiffrement par flux est rendu public par Alice lorsqu'elle l'envoie à Bob, n'importe quelles valeurs peuvent être choisies par Alice pour l'IV lors de ses transmissions à Bob.

Veuillez choisir une réponse.

- Vrai
- Faux ✓

La réponse correcte est « Faux ».

Question 10

Correct

Note de 1,00 sur 1,00

Il n'est pas possible d'utiliser un algorithme à clé symétrique pour faire des signatures numériques.

Veuillez choisir une réponse.

- Vrai
- Faux ✓

La réponse correcte est « Faux ».

Question 11

Correct

Note de 1,00 sur 1,00

L'utilisation de la cryptanalyse fréquentielle permet d'avoir des gains considérables par rapport à l'utilisation de la force brute contre la méthode de chiffrement AES, même si l'entropie de la source est élevée.

Veuillez choisir une réponse.

- Vrai
- Faux ✓

La réponse correcte est « Faux ».

Question 12

Correct

Note de 1,00 sur 1,00

L'analyse fréquentielle est la meilleure méthode de cryptanalyse contre l'algorithme de chiffrement à masque jetable (connu aussi comme « one-time pad » ou algorithme de Vernam).

Veuillez choisir une réponse.

- Vrai
- Faux ✓

La réponse correcte est « Faux ».

Question 13

Correct

Note de 1,00 sur 1,00

L'algorithme du masque jetable est un algorithme de chiffrement dit « parfait », car la confidentialité du message est toujours assurée, quelle que soit l'entropie de la source générant le message, à condition que la clé soit aussi longue que le message et que celle-ci soit générée avec un maximum d'entropie.

Veuillez choisir une réponse.

- Vrai ✓
- Faux

La réponse correcte est « Vrai ».

Question 14

Correct

Note de 1,00 sur 1,00

L'algorithme du masque jetable est le seul algorithme dit « parfait » pour toutes ces raisons à l'exception de :

Veuillez choisir une réponse.

a. Sa sécurité est basée sur l'impossibilité mathématique de factoriser de grands chiffres entiers en temps polynomial. ✓

b. Quelle que soit l'entropie de la source, le message ne peut pas être déchiffré par force brute ni par analyse fréquentielle, en supposant que la clé à une entropie maximale est aussi longue que le message

c. Les opérations arithmétiques nécessaires peuvent être facilement implémentés en matériel, sur un microprocesseur et même facilement calculé par un humain.

d. Il suit le principe de « Kerckhoffs ».

Votre réponse est correcte.

La réponse correcte est : Sa sécurité est basée sur l'impossibilité mathématique de factoriser de grands chiffres entiers en temps polynomial.

Question 15

Correct

Note de 1,00 sur 1,00

Lors de l'utilisation de la technique du masque jetable (one-time pad) aussi connu sous le nom d'algorithme de Vernam, pour un texte de 2000 caractères ASCII, quelle sera la longueur de la clé ?

Veuillez choisir une réponse.

a. 64 bits

b. 128 bits

c. 2024 bits

d. 16000 bits ✓

e. 64000 bits

Votre réponse est correcte.

La réponse correcte est : 16000 bits