Commencé le	lundi 22 avril 2024, 09:12
État	Terminé
Terminé le	lundi 22 avril 2024, 09:21
Temps mis	8 min 50 s
Points	23,00/23,00
Note	**10,00** sur 10,00 (**100**%)

Question 1

Correct

Note de 1,00 sur 1,00

Si Alice veut envoyer un message confidentiel à Bob en utilisant le chiffrement RSA, quelle opération doit-elle faire?

Veuillez choisir une réponse.

a. Chiffrer avec la clé privée d'Alice

b. Chiffrer avec la clé privée de Bob

c. Chiffrer avec la clé publique d'Alice

d. Chiffrer avec la clé publique de Bob ✓

e. Chiffrer avec un secret partagé

Votre réponse est correcte.

La réponse correcte est : Chiffrer avec la clé publique de Bob

Question 2

Correct

Note de 1,00 sur 1,00

Si Alice veut prouver à tout le monde qu'un document a vraiment été produit par elle, quelle opération doit-elle faire ?

Veuillez choisir une réponse.

a. Chiffrer avec sa clé publique

b. Chiffrer avec un secret partagé

c. Chiffrer avec sa clé privée ✓

d. Utiliser une fonction de hachage cryptographique

e. Utiliser un certificat

Votre réponse est correcte.

La réponse correcte est : Chiffrer avec sa clé privée

Question 3

Correct

Note de 1,00 sur 1,00

Les chiffrements probabilistes tels qu'El-Gamal ou le chiffrement à courbes elliptiques sont très vulnérables aux attaques par dictionnaire

Veuillez choisir une réponse.

- Vrai
- Faux ✓

La réponse correcte est « Faux ».

Question 4

Correct

Note de 1,00 sur 1,00

L'utilisation de RSA doit être privilégiée par rapport à l'utilisation d'AES puisque la longueur d'une clé RSA est plus grande que la longueur d'une clé AES.

Veuillez choisir une réponse.

- Vrai
- Faux ✓

La réponse correcte est « Faux ».

Question 5

Correct

Note de 1,00 sur 1,00

Pour utiliser El-Gamal ou les chiffrements à courbe elliptiques, puisque la valeur aléatoire peut être n'importe quelle valeur et que vous n'avez pas à la conserver, le choix de la valeur aléatoire est peu important.

Veuillez choisir une réponse.

- Vrai
- Faux ✓

La réponse correcte est « Faux ».

Question 6

Correct

Note de 1,00 sur 1,00

Si on arrivait à construire un ordinateur quantique ayant seulement quelques milliers de bits quantiques (« qubit ») de mémoire, il serait possible de réaliser une attaque par force brute sur l'algorithme AES-256 en quelques minutes.

Veuillez choisir une réponse.

- Vrai
- Faux ✓

La réponse correcte est « Faux ».

Question 7

Correct

Note de 1,00 sur 1,00

Si on arrivait à construire un ordinateur quantique ayant seulement quelques milliers de bits quantiques (« qubit ») de mémoire, il serait possible de réaliser en quelques secondes une attaque par factorisation sur tous les algorithmes de clé publique utilisés présentement.

Veuillez choisir une réponse.

- Vrai ✓
- Faux

La réponse correcte est « Vrai ».

Question 8

Correct

Note de 1,00 sur 1,00

L'algorithme cryptographique à clé publique de El-Gamal peut être défini sur n'importe quel groupe, même s'il n'est pas commutatif.

Veuillez choisir une réponse.

- Vrai ✓
- Faux

La réponse correcte est « Vrai ».

Question 9

Correct

Note de 1,00 sur 1,00

L'ajout de 3 bits de clé double l'effort de cryptanalyse sur l'algorithme RSA par les meilleures méthodes connues pour ce faire.

Veuillez choisir une réponse.

- Vrai ✓
- Faux

La réponse correcte est « Vrai ».

Question 10

Correct

Note de 1,00 sur 1,00

La découverte d'un algorithme permettant de générer efficacement et rapidement des collisions dans les fonctions de hachage cryptographique commune telles que MD5 et SHA-1 permettrait à un pirate informatique de pouvoir intercepter toutes les communications entre n'importe quel site bancaire et les clients qui s'y connecte.

Veuillez choisir une réponse.

- Vrai
- Faux ✓

La réponse correcte est « Faux ».

Question 11

Correct

Note de 1,00 sur 1,00

La raison principale pour laquelle il est utile d'utiliser des algorithmes de cryptographie à courbes elliptiques est parce qu'il est possible d'obtenir un niveau de sécurité équivalent en utilisant des clés cryptographiques plus petites, ce qui a des avantages en termes de performance.

Veuillez choisir une réponse.

- Vrai ✓
- Faux

La réponse correcte est « Vrai ».

Question 12

Correct

Note de 1,00 sur 1,00

Les algorithmes de stéganographie qui permettent de cacher des messages textes dans des images constituent un outil de sécurité informatique permettant d'atteindre des objectifs de confidentialité

Veuillez choisir une réponse.

- Vrai ✓
- Faux

La réponse correcte est « Vrai ».

Question 13

Correct

Note de 1,00 sur 1,00

Laquelle de ces notions n'est pas une propriété de la signature numérique :

Veuillez choisir une réponse.

- a. Authenticité
- b. Confidentialité ✓
- c. Intégrité
- d. Non répudiabilité

Votre réponse est correcte.

La réponse correcte est : Confidentialité

Question 14

Correct

Note de 1,00 sur 1,00

Parmi les raisons évoquées ci-dessous, quelle est la raison principale pour laquelle il est utile d'inclure un préambule dans un texte que nous allons signer numériquement ?

Veuillez choisir une réponse.

a. S'assurer que le contexte du document soit bien compris par la personne qui va le lire

b. Rendre plus difficile pour Ève de trouver un texte équivalent avec la même signature ✓

c. Permettre au vérificateur de s'assurer avec un degré raisonnable de confiance que le texte devant lui est bien celui qui a été signé, parmi l'ensemble infini de texte qui pourrait avoir la même signature

d. Il n'est pas nécessaire, ni recommandé d'inclure un préambule

Votre réponse est correcte.

La réponse correcte est : Rendre plus difficile pour Ève de trouver un texte équivalent avec la même signature

Question 15

Correct

Note de 1,00 sur 1,00

L'utilisation adéquate de bonnes fonctions de hachage cryptographique peut constituer une mesure efficace :

Veuillez choisir une réponse.

a. Pour réduire l'efficacité d'attaques visant à atteindre l'intégrité de biens informatiques ✓

b. Pour obtenir un niveau de sécurité équivalent contre des efforts de cryptanalyse, tout en utilisant des tailles de clés et de bloc de chiffrement plus petits

c. Construire des structures de données efficaces, où le temps de recherche est considérablement réduit

d. N'est plus du tout recommandé dans un contexte de sécurité informatique, étant donné les découvertes scientifiques récentes concernant les possibilités de découverte de collision dans MD5 et SHA-1

Votre réponse est correcte.

La réponse correcte est : Pour réduire l'efficacité d'attaques visant à atteindre l'intégrité de biens informatiques

Question 16

Correct

Note de 1,00 sur 1,00

Plusieurs protocoles utilisent un chiffrement asymétrique pour chiffrer une clé de chiffrement symétrique. La clé symétrique est ensuite utilisée pour le reste de la communication. Pourquoi introduire cette complexité ?

Veuillez choisir une réponse.

a. Ça permet de contrer l'attaque de force brute

b. On combine la rapidité de la cryptographie asymétrique avec la robustesse de la cryptographie symétrique

c. On combine l'avantage de performance de la cryptographie symétrique avec l'avantage au niveau de la distribution de clé de la cryptographie asymétrique ✓

d. On double la longueur effective de la clé de chiffrement

Votre réponse est correcte.

La réponse correcte est : On combine l'avantage de performance de la cryptographie symétrique avec l'avantage au niveau de la distribution de clé de la cryptographie asymétrique

Question 17

Correct

Note de 1,00 sur 1,00

Dans le cas d'une source avec une bonne entropie, quelle est la méthode la plus efficace pour attaquer RSA ?

Veuillez choisir une réponse.

a. Factorisation ✓

b. Attaque dictionnaire

c. Attaque de force brute

d. Inversement

e. Logarithme discret

Votre réponse est correcte.

La réponse correcte est : Factorisation

Question 18

Correct

Note de 1,00 sur 1,00

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

Veuillez choisir une réponse.

a. 56 bits
b. 64 bits
c. 128 bits
d. 256 bits
e. 2048 bits ✓

Votre réponse est correcte.

La réponse correcte est : 2048 bits

Question 19

Correct

Note de 1,00 sur 1,00

L'utilisation d'une infrastructure à clé publique (PKI) est souvent considérée essentielle pour l'opération sécuritaire avec un algorithme tel que RSA. De quelle attaque souhaite-t-on se protéger en implémentant ce type d'infrastructure ?

Veuillez choisir une réponse.

a. Débordement de mémoire tampon
b. Homme au milieu (man-in-the-middle) ✓
c. Factorisation
d. Déchiffrement
e. Débordement de compte de banque

Votre réponse est correcte.

La réponse correcte est : Homme au milieu (man-in-the-middle)

Question 20

Correct

Note de 1,00 sur 1,00

Considérant une fonction de hachage cryptographique résistante aux collisions, laquelle de ces affirmations est fausse ?

Veuillez choisir une réponse.

a. Il est difficile de générer un message qui possède exactement le même haché qu'un autre message

b. Il est difficile de trouver le message original à partir du haché

c. Une taille de haché de 256 bits est suffisante

d. Deux messages choisis au hasard ont 1 chance sur 128 d'être identique pour un haché de 128 bits ✓

Votre réponse est correcte.

La réponse correcte est : Deux messages choisis au hasard ont 1 chance sur 128 d'être identique pour un haché de 128 bits

Question 21

Correct

Note de 1,00 sur 1,00

Quelle est la différence principale et plus significative entre un système de gestion de clés publiques décentralisé et un système de gestion de clés publiques centralisés ?

Veuillez choisir une réponse.

a. Le fait que dans les systèmes hiérarchiques il y a des « racines de confiance » qui sont des autorités de certification dont les clés publiques sont reconnues par tous ✓

b. Le fait que dans les systèmes hiérarchiques des compagnies font de l'argent en signant des certificats de clés publiques

c. L'utilisation de cryptographie symétrique plutôt que de la cryptographie asymétrique

d. Les systèmes décentralisés utilisent des serveurs répartis un peu partout dans le monde pour stocker les certificats de clé publique de ses utilisateurs

Votre réponse est correcte.

La réponse correcte est : Le fait que dans les systèmes hiérarchiques il y a des « racines de confiance » qui sont des autorités de certification dont les clés publiques sont reconnues par tous

Question 22

Correct

Note de 1,00 sur 1,00

Lorsque le certificat d'une autorité racine est compromis, tous les certificats signés par cette autorité doivent être considérés compromis.

Veuillez choisir une réponse.

- Vrai ✓
- Faux

La réponse correcte est « Vrai ».

Question 23

Correct

Note de 1,00 sur 1,00

Lorsque le certificat d'une autorité racine est compromis, seules les communications vers les sites Web dont les certificats signés par cette autorité pourraient être interceptées.

Veuillez choisir une réponse.

- Vrai
- Faux ✓

La réponse correcte est « Faux ».