Commencé le	jeudi 25 janvier 2024, 13:55
État	Terminé
Terminé le	dimanche 21 avril 2024, 23:35
Temps mis	87 jours 8 heures
Points	7,00/18,00
Note	**3,89** sur 10,00 (**38,89**%)

Question 1

Correct

Note de 1,00 sur 1,00

Si on garde la méthode d'encodage secrète, il n'est pas nécessaire d'utiliser un chiffrement pour garantir la confidentialité

Veuillez choisir une réponse.

- Vrai
- Faux ✓

La réponse correcte est « Faux ».

Question 2

Correct

Note de 1,00 sur 1,00

Lequel de ces composants ne fait pas partie du modèle de Shannon révisé :

Veuillez choisir une réponse.

- a. Codage
- b. Chiffrement
- c. Compression ✓
- d. Canal

Votre réponse est correcte.

La réponse correcte est : Compression

Question 3

Correct

Note de 1,00 sur 1,00

Dans le modèle de Shannon, à laquelle de ces informations Ève n'a pas accès :

Veuillez choisir une réponse.

a. L'algorithme de chiffrement

b. Les paramètres de l'algorithme de codage

c. Le message transmis sur le canal

d. La clé de chiffrement ✓

Votre réponse est correcte.

La réponse correcte est : La clé de chiffrement

Question 4

Incorrect

Note de 0,00 sur 1,00

Un codage et un chiffrement sont tous deux des formes de translitérations

Veuillez choisir une réponse.

Vrai

Faux ✗

La réponse correcte est « Vrai ».

Question 5

Correct

Note de 1,00 sur 1,00

Il n'est pas mathématiquement correct de parler de l'entropie d'un texte. Il faut dans ce cas plutôt parler de « pseudo-entropie ».

Veuillez choisir une réponse.

Vrai ✓

Faux

La réponse correcte est « Vrai ».

Question 6

Non répondue

Noté sur 1,00

L'entropie d'une source qui émet chaque fois un symbole de l'alphabet grec (24 lettres) choisi au hasard est la même que celle qui émet chaque fois la prochaine lettre du texte de « Antigone », la fameuse pièce de théâtre du dramaturge grec du 5e siècle av. J.-C., Sophocle

Veuillez choisir une réponse.

- Vrai
- Faux

La réponse correcte est « Faux ».

Question 7

Correct

Note de 1,00 sur 1,00

La loi de Moore stipule que la puissance de calcul des ordinateurs disponibles sur le marché double à chaque 18 mois. Combien de bits de clés serait-il nécessaire d'ajouter à un algorithme de cryptographie symétrique à 128 bits pour compenser l'effet de la Loi de Moore sur une période de 9 ans.

Veuillez choisir une réponse.

- a. Il n'est pas nécessaire d'augmenter la taille de la clé
- b. 1 bit
- c. 6 bits ✓
- d. 128 bits

Votre réponse est correcte.

La réponse correcte est : 6 bits

Question 8

Correct

Note de 1,00 sur 1,00

Laquelle de ces sources génère le plus d'information ?

Veuillez choisir une réponse.

a. Une source qui génère pile avec une probabilité de 10% et face avec une probabilité de 90%.

b. Une source qui génère pile avec une probabilité de 30% et face avec une probabilité de 70%.

c. Une source qui génère pile avec une probabilité de 60% et face avec une probabilité de 40%.

d. Une source qui génère pile avec une probabilité de 50% et face avec une probabilité de 50%. ✓

e. Une source qui génère pile avec une probabilité de 80% et face avec une probabilité de 20%.

Votre réponse est correcte.

La réponse correcte est : Une source qui génère pile avec une probabilité de 50% et face avec une probabilité de 50%.

Question 9

Non répondue

Noté sur 1,00

Une source déterministe produisant 50% de 0 et 50% de 1 possède une entropie plus grande qu'une source markovienne produisant 75% de 0 et 25 % de 1.

Veuillez choisir une réponse.

Vrai

Faux

La réponse correcte est « Faux ».

Question 10

Non répondue

Noté sur 1,00

Laquelle de ces sources génère le plus d'information ?

Veuillez choisir une réponse.

a. Une source qui génère pile ou face en lançant une pièce de monnaie

b. Une source qui génère un chiffre de 1 à 6 en lançant un dé

c. Une source qui génère un chiffre de 1 à 6 de manière séquentielle (e.g. {1}, suivi de {2}, suivi de {3}, etc)

d. Une source qui génère pile ou face en alternance

e. Une source qui génère une chaîne de 10 caractères ASCII basée sur la vitesse de la lumière dans le vide

Votre réponse est incorrecte.

La réponse correcte est : Une source qui génère un chiffre de 1 à 6 en lançant un dé

Question 11

Correct

Note de 1,00 sur 1,00

Laquelle de ces sources génère le plus d'information ?

Veuillez choisir une réponse.

a. Une source markovienne déterministe

b. Une source markovienne aléatoire ✓

c. Une source non-markovienne déterministe

d. Une source non-markovienne aléatoire

e. Toutes ces sources génèrent la même quantité d'information

Votre réponse est correcte.

La réponse correcte est : Une source markovienne aléatoire

Question 12

Non répondue

Noté sur 1,00

Je suis entré en possession de dizaines de millions de pages de texte en anglais encodés en ASCII. Je calcule la pseudo-entropie moyenne par caractère de mon échantillon. Laquelle de ces valeurs est-ce que je devrais me rapprocher ?

Veuillez choisir une réponse.

a. Le taux de compression caractère par caractère

b. 8 bits

c. 1 bit

d. L'entropie du langage

e. Aucune de ces réponses

Votre réponse est incorrecte.

La réponse correcte est :
Aucune de ces réponses

Question 13

Non répondue

Noté sur 1,00

Pour une source donnée, lequel de ces codages présente le taux de compression non destructeur le plus élevé ?

Veuillez choisir une réponse.

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

b. Un encodage binaire sur un nombre de bits égal à la moitié de l'entropie

c. Un encodage ASCII avec un nombre de bytes égal à l'entropie

d. Un encodage ASCII avec un nombre de bytes égal à la moitié de l'entropie

e. Un encodage MP3

Votre réponse est incorrecte.

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

Question 14

Non répondue

Noté sur 1,00

Il est plus facile de faire de la cryptanalyse si le message à chiffrer est de l'anglais plutôt que les résultats des derniers tirages de la Loto 6/49.

Veuillez choisir une réponse.

- Vrai
- Faux

La réponse correcte est « Vrai ».

Question 15

Non répondue

Noté sur 1,00

L'entropie d'une source est maximale pour une source sans mémoire dont tous les symboles se retrouvent dans la même proportion dans un texte statistiquement représentatif de la source.

Veuillez choisir une réponse.

- Vrai
- Faux

La réponse correcte est « Vrai ».

Question 16

Non répondue

Noté sur 1,00

Choisissez la réponse la plus appropriée pour cette affirmation « Si l'algorithme de chiffrement est vulnérable, il est très facile de faire la cryptanalyse fréquentielle d'une source markovienne dont tous les caractères sont équiprobables ».

Veuillez choisir une réponse.

- a. Vrai, si l'algorithme est vulnérable, l'analyse fréquentielle n'est plus nécessaire
- b. Faux, la distribution statistique du texte chiffré ne présentera pas de variation significative de fréquences
- c. Vrai, il suffit de comparer les fréquences des caractères avec la fréquence des lettres en langue anglaise
- d. Faux, dès que le texte est chiffré, il est impossible de faire de l'analyse fréquentielle.
- e. Vrai, uniquement l'analyse des digrammes et des trigrammes sera affectée par les caractéristiques de la source

Votre réponse est incorrecte.

La réponse correcte est : Vrai, si l'algorithme est vulnérable, l'analyse fréquentielle n'est plus nécessaire

Question 17

Non répondue

Noté sur 1,00

Le principe qui dit que la sécurité d'un algorithme de cryptographie ne devrait dépendre que du secret de la clé

Veuillez choisir une réponse.

a. s'appelle le principe de Kerchoff

b. n'est pas un principe de sécurité informatique

c. a été énoncé par les inventeurs de l'algorithme RSA (Rivest, Shamir, Adleman)

d. ne s'applique qu'aux algorithmes de cryptographie à clé secrète

Votre réponse est incorrecte.

La réponse correcte est : s'appelle le principe de Kerchoff

Question 18

Non répondue

Noté sur 1,00

L'entropie peut être une mesure décrivant la difficulté de mener les attaques suivantes, à **l'exception** de :

Veuillez choisir une réponse.

a. Une attaque de crackage de mot de passe par force brute.

b. Une attaque de déni de service par SYN flooding.

c. Une attaque de « session hijacking » dans une application Web utilisant des jetons de session (session ID).

d. Une attaque de cryptanalyse par analyse fréquentielle.

Votre réponse est incorrecte.

La réponse correcte est : Une attaque de déni de service par SYN flooding.