Commencé le	jeudi 14 mars 2024, 14:00
État	Terminé
Terminé le	jeudi 14 mars 2024, 15:51
Temps mis	1 heure 50 min
Points	22,75/30,00
Note	**7,58** sur 10,00 (**75,83**%)

Question 1

Correct

Note de 1,00 sur 1,00

Alice envoie à Bob un message chiffré en utilisant le chiffrement de Vigenere.

Le message contient des lettres de A à Z sans chiffre, sans ponctuation ni espace.

La clé utilisée partagée par Alice et Bob est le mot de 4 lettres : MARS.

Alice a utilisé le codage suivant : A --> 0, B --> 1, C --> 2, ..., Z --> 25.

Elle a ensuite utilisé une addition modulo 26 pour calculer le message chiffré.

Après décodage, le message chiffré reçu par Bob est le suivant :

XATQNEIUQSKKGPVJ

Quel est le message que Bob va obtenir en déchiffrant ce message ?

Réponse : LACYBERCESTSUPER ✓

La réponse correcte est : LACYBERCESTSUPER

Question 2

Incorrect

Note de 0,00 sur 1,00

Alice et Bob échangent des messages de façon confidentielle en utilisant le chiffrement de Vernam (one-time pad).

Pour forger la clé de chiffrement, Alice et Bob ont choisi d'utiliser le livre « Les Misérables » de Victor Hugo.

Le choix du livre n'est connu que par Alice et Bob.

La clé est forgée en prenant séquentiellement les caractères des phrases du livre en enlevant les espaces et les signes de ponctuation.

Que peut-on dire du chiffrement utilisé par Alice et Bob ? (plusieurs réponses possibles)

- a. Le chiffrement n'est pas parfait car la clé n'a pas une entropie maximale
- b. Le chiffrement n'est pas parfait car un attaquant pourrait accéder à une bibliothèque et retrouver le livre ayant servi à forger la clé ✓
- c. Le chiffrement ne satisfait pas les principes de Kerckhoffs
- d. Le chiffrement est parfait si la longueur de la clé est égale à la longueur du message à chiffrer ✗

Votre réponse est incorrecte.

Les réponses correctes sont :
Le chiffrement n'est pas parfait car la clé n'a pas une entropie maximale,

Le chiffrement n'est pas parfait car un attaquant pourrait accéder à une bibliothèque et retrouver le livre ayant servi à forger la clé

Question 3

Correct

Note de 1,00 sur 1,00

On suppose qu'un mot de passe est forgé de la façon suivante :

Le mot de passe a une longueur fixe de 8 caractères

Chaque caractère est tiré aléatoirement dans l'ensemble des caractères minuscules (a à z) ou majuscules (A à Z)

Quelle est l'entropie du mot de passe ?

a. 5,70

b. 5,95

c. 45,60 ✓

d. 37,60

Votre réponse est correcte.

Réponse :

Soit S l'entropie de la source qui génère le mot de passe :

H(S) = Log2(52) = 5,70

Mot de passe de 8 caractères (source markovienne) : 8 * H(S) = 8 * 5,70 = 45,60

La réponse correcte est :
45,60

Question 4

Correct

Note de 1,00 sur 1,00

Les hypothèses sont identiques à celles de la question précédente

On suppose donc qu'un mot de passe est forgé de la façon suivante :

Le mot de passe a une longueur fixe de 8 caractères

Chaque caractère est tiré aléatoirement dans l'ensemble des caractères minuscules (a à z) ou majuscules (A à Z)

On considère un attaquant pouvant tester 1 000 000 (10^6) mots de passe par seconde

Dans le cas pire, combien de temps sera nécessaire pour que l'attaquant casse le mot de passe ?

a. Environ 68 jours

b. Environ 750 jours

c. Environ 620 jours ✓

d. Environ 232 jours

e. Environ 136 jours

f. Environ 20 jours

g. Environ 22 jours

h. Environ 15 jours

Votre réponse est correcte.

Nombre de mots de passe à tester = 52^8 = 53 459 728 531 456

Nombre de secondes nécessaires pour teste tous les mots de passe :

53 459 728 531 456 / 1 000 000 = 53 459 728 secondes

Temps nécessaire en années : 53 459 728 / (60 * 60 * 24) = 618,75 jours

La réponse correcte est :
Environ 620 jours

Question 5

Correct

Note de 1,00 sur 1,00

Les hypothèses sont identiques à celles de la question 4.

De plus, on suppose que l'attaquant dispose de l'information suivante :

Le mot de passe est composé de 7 caractères minuscules et de 1 caractère majuscule

L'attaquant ne sait pas où se trouve le caractère majuscule,

Dans le cas pire, combien de temps sera nécessaire pour que l'attaquant casse le mot de passe ?

a. Environ 232 jours

b. Environ 20 jours ✓

c. Environ 620 jours

d. Environ 68 jours

e. Environ 750 jours

f. Environ 136 jours

g. Environ 15 jours

h. Environ 22 jours

Votre réponse est correcte.

Réponse :

Nombre de positions possibles pour le caractère majuscule : 8

Nombre de mots de passe à tester = 26^8 * 8 = 208 827 064 576 * 8 = 1 670 616 516 608

Nombre de secondes nécessaires pour teste tous les mots de passe :

1 670 616 516 608 / 1 000 000 = 1 670 617 secondes

Temps nécessaire en jours : 1 670 617 / (60 * 60 * 24) = 19,34 jours

La réponse correcte est :
Environ 20 jours

Question 6

Correct

Note de 1,00 sur 1,00

Les hypothèses sont identiques à celles de la question 4.

On suppose maintenant que l'attaquant dispose de l'information suivante :

Le mot de passe est composé de 6 caractères minuscules et de 2 caractères majuscules

L'attaquant ne sait pas ou se trouve les deux caractères majuscules.

Dans le cas pire, combien de temps sera nécessaire pour que l'attaquant casse le mot de passe ?

a. Environ 620 jours

b. Environ 15 jours

c. Environ 68 jours ✓

d. Environ 22 jours

e. Environ 136 jours

f. Environ 750 jours

g. Environ 20 jours

h. Environ 232 jours

Votre réponse est correcte.

Réponse :

Nombre de sous-ensembles de deux éléments dans ensemble de 8 éléments : 8 * 7 / 2 = 28

Nombre de mots de passe à tester = 26^8 * 28 = 208 827 064 576 * 28 = 5 847 157 808 128

Nombre de secondes nécessaires pour teste tous les mots de passe :

5 847 157 808 128 / 1 000 000 = 5 847 158 secondes

Temps nécessaire en jours : 5 847 158 / (60 * 60 * 24) = 67,67 jours

La réponse correcte est :
Environ 68 jours

Question 7

Correct

Note de 1,00 sur 1,00

Les hypothèses sont identiques à celles de la question 4.

On suppose maintenant que l'attaquant dispose des informations suivantes :

(1) Le mot de passe est composé au plus de 2 caractères majuscules

(2) Il y a 25% de chance que le mot de passe ne contienne aucune majuscule

(3) Il y a 25% de chance que le mot de passe ne contienne qu'une seule majuscule

(4) Il y a 50% de chance que le mot de passe contienne deux majuscules

On utilise les notations suivantes :

- A représente l'ensemble des mots de passe sans majuscule
- B représente l'ensemble des mots de passe avec une seule majuscule
- C représente l'ensemble des mots de passe avec deux majuscules

Parmi les possibilités suivantes, quelle est la stratégie la plus rapide pour que l'attaquant **ait 50% de chance** de casser le mot de passe :

a. Tester C puis B

b. Tester A puis B ✓

c. Tester C

d. Tester A puis C

Votre réponse est correcte.

Réponse :

L'ensemble A contient 26^8 mots de passe. En testant tous les mots de passe de A, l'attaquant obtient 25% de chance de casser le mot passe.

L'ensemble B contient 8 fois plus de passe que A. En testant B, l'attaquant obtient également 25% de chance de casser le mot de passe.

Enfin, l'ensemble C contient 28 fois plus de passe que A. En testant C, l'attaqun obtient également 50% de chance de casser le mot de passe.

La meilleure stratégie est donc de tester A puis B. L'attaquant a à tester 9 fois le nombre de mots de passe contenu dans A pour avoir 50% de chance de casser le mot de passe.

Toutes les autres stratégies nécessitent de tester plus de mots de passe pour atteindre 50% de chance.

La réponse correcte est :
Tester A puis B

Question 8

Correct

Note de 1,00 sur 1,00

Les hypothèses sont identiques à celles de la question 7.

On suppose donc que l'attaquant dispose de l'information suivante :

(1) Le mot de passe est composé au plus de 2 caractères majuscules

(2) Il y a 25% de chance que le mot de passe ne contienne aucune majuscule

(3) Il y a 25% de chance que le mot de passe ne contienne qu'une seule majuscule

(4) Il y a 50% de chance que le mot de passe contienne deux majuscules

En supposant que l'attaquant suit la stratégie la plus rapide, combien de temps sera nécessaire pour que l'attaquant **ait 50% de chance** de casser le mot de passe ?

- a. Environ 750 jours
- b. Environ 68 jours
- c. Environ 22 jours ✓
- d. Environ 620 jours
- e. Environ 232 jours
- f. Environ 136 jours
- g. Environ 20 jours
- h. Environ 15 jours

Votre réponse est correcte.

Réponse :

En testant tous les mots de passe de l'ensemble A, l'attaquant a 25% de chance de casser le mot de passe et en testant tous les mots de passe de B, l'attaquant a aussi 25% de casser le mot de passe.

Pour avoir 50% de chance, le nombre de mots de passe que l'attaquant doit tester est donc :

26^8 + 8 * 26^8 = 9 * 208 827 064 576 = 1 879 443 581 184

Nombre de secondes nécessaires pour tester les mots de passe :

1 879 443 581 184/ 1 000 000 = 1 879 444 secondes

Temps nécessaire en jours : 1 879 444 / (60 * 60 * 24) = 21,75 jours

La réponse correcte est : Environ 22 jours

Question 9

Correct

Note de 1,00 sur 1,00

Les hypothèses sont identiques à celles de la question 4.

On suppose maintenant que l'attaquant dispose des deux informations suivantes :

(1) Parmi les huit caractères composant le mot de passe, il y a nécessairement une majuscule

(2) Cette majuscule est en première position ou en dernière position

Combien de temps sera nécessaire pour que l'attaquant ait **50% de chance** de casser le mot de passe ?

- a. Environ 750 jours
- b. Environ 232 jours ✓
- c. Environ 22 jours
- d. Environ 620 jours
- e. Environ 20 jours
- f. Environ 136 jours
- g. Environ 15 jours
- h. Environ 68 jours

Votre réponse est correcte.

Réponse :

Nombre de mots de passe correspondant aux hypothèses :

Majuscule en première position : 26 * 52^7 = 26 729 864 265 728

Majuscule en dernière position et minuscule en première position (les autres cas ont déjà été testés) : 26 * 26 * 52^6 = 13 364 932 132 864

Nombre total de mots de passe à tester pour avoir 50% de chance :

(26 729 864 265 728 + 13 364 932 132 864) / 2 = 20 047 398 199 296

Nombre de secondes nécessaires pour teste tous les mots de passe :

20 047 398 199 296 / 1 000 000 = 20 047 398 secondes

Temps nécessaire en jours : 20 047 398 / (60 * 60 * 24) = 232 jours

La réponse correcte est :
Environ 232 jours

Question 10

Incorrect

Note de 0,00 sur 1,00

Entropie d'une source

On considère une source S qui génère des chaînes de bits (0 ou 1) de la façon suivante :

On suppose que la chaine de bits commence en position 1.

Si la position du bit dans la chaîne est impaire, alors il y a 70% de chance que le bit soit un 0 et 30% de chance que ce soit un 1.

Si la position du bit dans la chaîne est paire, alors : (1) si le bit précédent dans la chaîne est un 0, il y a 30% de chance que le bit soit un 0 et 70% de chance que le bit soit un 1 et (2) si le bit précédent dans la chaîne est un 1, il y a 40% de chance que le bit soit un 1 et 60% de chance que le bit soit un 0.

Quelle est l'entropie fréquentielle caractère par caractère de la source S ?

- a. 0,90 bit ✗
- b. 0,99 bit
- c. 0,75 bit
- d. 0,5 bit

Votre réponse est incorrecte.

Réponse :

Il s'agit de calculer la fréquence d'apparition des 0 et des 1 dans la chaîne générée par la source S.

La séquence « 00 » apparait dans 0,7 * 0,3 = 21% des cas.

La séquence « 01 » apparait dans 0,7 * 0,7 = 49% des cas.

La séquence « 10 » apparait dans 0,3 * 0,6 = 18% des cas.

La séquence « 11 » apparait dans 0,3 * 0,4 = 12% des cas.

La probabilité d'apparition d'un 0 dans la chaîne est donc de :

(0,21 * 2 + 0,49 + 0,18) / 2 = 0,545

Et la probabilité d'apparition d'un 1 dans la chaîne est donc également de 0,455.

L'entropie caractère par caractère de la source S est donc :

Hf(S) = 0,545 * Log2(1/0,545) + 0,455 * Log2(1/0,455)

= 0,545 * 0,875672 + 0,455 * 1,13606 = 0,99

La réponse correcte est :
0,99 bit

Question 11

Correct

Note de 1,00 sur 1,00

Suite de la question 10.

La source S est markovienne.

- Vrai
- Faux ✓

La réponse correcte est « Faux ».

Question 12

Incorrect

Note de 0,00 sur 1,00

On considère la source S^2 identique à la source S mais qui génère des blocs de 2 bits (digrammes).

La source S^2 est-elle markovienne ?

- Vrai
- Faux ✗

La réponse correcte est « Vrai ».

Question 13

Correct

Note de 1,00 sur 1,00

On considère la source S^2 identique à la question 12.

Quelle est l'entropie de la source S^2 ?

a. 1,79 bit ✓

b. 1,55 bit

c. 1,25 bit

d. 1,98 bit

Votre réponse est correcte.

Réponse :

L'alphabet de la source S^2 est {00, 01, 10, 11}

On a :

P(S^2 = « 00 ») = 0,21

P(S^2 = « 01 ») = 0,49

P(S^2 = « 10 ») = 0,18

P(S^2 = « 11 ») = 0,12

En appliquant la formule de Shannon, on a :

H(S^2) = 0,21 Log2(1/0,21) + 0,49 Log2(1/0,49) + 0,18 Log2(1/0,18) + 0,12 Log2(1/0,12)

Donc H(S^2) = 0,21 * 2,25154 + 0,49 * 1,02915 + 0,18 * 2,47393 + 0,12 * 3,05889

= 1,789 bit

La réponse correcte est :
1,79 bit

Question 14

Correct

Note de 1,00 sur 1,00

On considère la source S^2 identique à la 13.

Quelle est l'entropie du langage associé à la source S ?

a. Egale à la moitié de l'entropie de la source S^2 ✓

b. Egale à l'entropie caractère par caractère de la source S

c. Egale à l'entropie de la source S^2

d. Aucune de ces réponses

Votre réponse est correcte.

Réponse :

On a H_L(S) = lim{b --> infini} (H(S^b) / b)

Si b = 2n (b est pair) alors H(S^2n) = n H(S^2) car S^2 est markovienne.

H_L(S) = lim{2n --> infini} (n H(S^2) / 2n) = H(S^2) / 2

Si b = 2n + 1 (b est impair) alors H(S^b) = n H(S^2) + 1

H_L(S) = lim{2n+1 --> infini} ((n H(S^2) + 1) / (2n + 1))

= lim (2n+1 --> infini} (n H(S^2) / (2n + 1)) + lim (2n+1 infini} (1 / (2n + 1))

Donc H_L(S) = H(S^2) / 2 + 0 = H(S^2) / 2

La réponse est donc : H_L(S) = H(S^2) / 2

La réponse correcte est :
Egale à la moitié de l'entropie de la source S^2

Question 15

Correct

Note de 1,00 sur 1,00

Lorsqu'un acteur malveillant récupère ou vole le SecureID d'authentification d'un employé d'une entreprise qu'il souhaite attaquer, lequel des attributs suivants de l'analyse de risque est affecté :

a. Intégrité
b. Capacité
c. Opportunité ✓
d. Motivation

Votre réponse est correcte.

La réponse correcte est :
Opportunité

Question 16

Incorrect

Note de 0,00 sur 1,00

Un pirate informatique infecte le serveur d'un site de réservation Allociné et y installe un virus qui infecte les machines de ceux qui visitent ce site avec un « keylogger », qui enregistre les mots de passe et cartes de crédit tapés sur les machines ainsi infectées, S'agit-il de :

a. Une vulnérabilité
b. Une menace ✗
c. Un risque
d. Une contremesure

Votre réponse est incorrecte.

La réponse correcte est :
Un risque

Question 17

Correct

Note de 1,00 sur 1,00

Dans les données du tableau ci-dessous, on vous demande d'indiquer l'erreur qui s'y est glissée,

Scénario	Capacité	Opportunité	Motivation	Probabilité	Impact	Risque
S1) Un cybercriminel réalise une attaque d'homme/femme du milieu pour réaliser une traite bancaire frauduleuse	4	2	3	2.67	4	10.68
S2) Un jeune homme acculé par des dettes réalise une attaque d'homme/femme du milieu pour réaliser une traite bancaire frauduleuse	3	2	3	3	4	12

a. Le risque de S2 est trop élevé

b. L'impact dans S2 est trop élevé

c. Le facteur motivation dans S2 est trop élevé

d. Les probabilités sont incorrectes ✓

e. Le calcul du risque ne prend pas en compte la probabilité

f. Le facteur capacité dans S2 est trop haut

Votre réponse est correcte.

La réponse correcte est :
Les probabilités sont incorrectes

Question 18

Incorrect

Note de 0,00 sur 1,00

Au cours des mois de mars et d'avril 2000, un ancien prestataire technique de la station d'épuration de Maroochy en Australie a pris le contrôle des systèmes de l'usine à des fins malveillantes, après que sa demande d'emploi ait été refusée. Il aurait ainsi détourné l'activité de plusieurs pompes en envoyant de fausses commandes. L'une des pompes aurait alors cessé de fonctionner, provoquant le déversement d'eaux usées dans les fonds marins, l'empoisonnement de la faune et de la flore locales, et la propagation d'odeurs nauséabondes aux alentours. Quel paramètre de la probabilité d'occurrence de cette attaque a facilité la tâche de l'attaquant :

- a. Capacité ✗
- b. Vulnérabilité
- c. Motivation
- d. Opportunité

Votre réponse est incorrecte.

La réponse correcte est :
Opportunité

Question 19

Correct

Note de 1,00 sur 1,00

Paula utilise un VPN pour établir une connexion chiffrée pour accéder à ses applications lorsqu'elle utilise le réseau public de l'aéroport.

Est-ce qu'il s'agit :

- a. D'un risque ?
- b. D'une menace ?
- c. D'une vulnérabilité ?
- d. D'une contremesure ? ✓

Votre réponse est correcte.

La réponse correcte est :
D'une contremesure ?

Question 20

Correct

Note de 1,00 sur 1,00

Sous Linux, pour définir les droits suivants sur le fichier « contrat » :

-rwxr-xr-- 1 Eloi RH 7627 Oct 1 12:50 contrat

Eloi doit exécuter la commande suivante :

a. chmod 751 contrat

b. chmod 654 contrat

c. chmod 754 contrat ✓

d. chmod 764 contrat

e. chmod 740 contrat

Votre réponse est correcte.

La réponse correcte est :
chmod 754 contrat

Question 21

Correct

Note de 1,00 sur 1,00

Sous Linux, la commande « chmod 751 contrat » est équivalente à la commande suivante :

a. chmod u=rwx, g=rx, o=r contrat

b. chmod u=rx, g=rx, o=x contrat

c. chmod u=rwx, g=rx, o=x contrat ✓

d. chmod u=rwx, g=rx, o=r contrat

Votre réponse est correcte.

La réponse correcte est :
chmod u=rwx, g=rx, o=x contrat

Question 22

Incorrect

Note de 0,00 sur 1,00

Une politique de contrôle d'accès dont toutes les règles sont des interdictions est une politique fermée.

- (●) Vrai ✗
- ( ) Faux

La réponse correcte est « Faux ».

Question 23

Correct

Note de 1,00 sur 1,00

Dans une politique RBAC, une session peut comporter plusieurs rôles activables et doit être associée à deux utilisateurs au plus.

- ( ) Vrai
- (●) Faux ✓

La réponse correcte est « Faux ».

Question 24

Correct

Note de 1,00 sur 1,00

Soit un rôle A avec un ensemble de droit d'accès C1, soit un rôle B muni d'un ensemble de droits d'accès C2. Le rôle D possède un ensemble de droits C3 et hérite des privilèges des rôles A et B. L'agent U s'est vu affecter le rôle D. Mais une contrainte supplémentaire de cette politique RBAC stipule que l'agent U ne peut utiliser les droits d'accès C1 et C2 dans une même session. Comment faut-il procéder pour satisfaire cette contrainte ?

a. D n'hérite plus de A

b. DSOD ✓

c. D n'hérite plus de B

d. SSOD

e. D n'hérite ni de A ni de B

Votre réponse est correcte.

La réponse correcte est :
DSOD

Question 25

Partiellement correct

Note de 0,75 sur 1,00

Soit la matrice d'accès suivante :

	Document 1	Document 2	Document 3
Lina	RX	RW	RW
Emile	X	-	RW
Ali	X	R	-

Dans cette matrice plusieurs flux indirects sont possibles

.

- [x] a. De Lina vers Ali ✓
- [ ] b. De Emile vers Ali
- [x] c. De Emile vers Lina ✗
- [x] d. De Lina vers Emile ✓
- [ ] e. De Ali vers Emile
- [ ] f. De Ali vers Lina

Votre réponse est partiellement correcte.

Vous avez sélectionné trop d'options.
Les réponses correctes sont :
De Lina vers Ali,

De Lina vers Emile

Question 26

Correct

Note de 1,00 sur 1,00

Si je procède à des activités peu sûres sur mon ordinateur et que j'installe moi-même des logiciels, je suis le seul à courir un risque.

- ○ Vrai
- ◉ Faux ✓

La réponse correcte est « Faux ».

Question 27

Partiellement correct

Note de 0,50 sur 1,00

Les données d'un hôpital sont stockées chiffrées par mesure de sécurité. Si le système informatique de cet hôpital subit une attaque de type rançon logiciel (chiffrement des données sans exfiltration). Quelles propriétés sont visées par cette attaque. (plusieurs réponses possibles) :

- [x] a. Intégrité ✓
- [x] b. Disponibilité ✓
- [ ] c. Confidentialité
- [ ] d. Authenticité
- [x] e. Imputabilité ✗

Votre réponse est partiellement correcte.

Vous avez sélectionné trop d'options.
Les réponses correctes sont :
Intégrité,

Disponibilité

Question 28

Partiellement correct

Note de 0,50 sur 1,00

Conformément à la définition donnée en cours de la propriété de la résilience, parmi les techniques suivantes, lesquelles assurent cette propriété.? (plusieurs réponses possibles)

- [ ] a. Authentification
- [x] b. Filtrage réseau ✗
- [x] c. La diversification fonctionnelle ✓
- [ ] d. Détection d'intrusion
- [x] e. La cible mouvante ✓

Votre réponse est partiellement correcte.

Vous avez sélectionné trop d'options.
Les réponses correctes sont :
La cible mouvante, La diversification fonctionnelle

Question 29

Correct

Note de 1,00 sur 1,00

On considère un alphabet A composé de 26 symboles correspondant aux lettres minuscules de « a » à « z ».

On considère le codage suivant :

Chaque symbole de l'alphabet A correspond à un nombre entre 0 à 25.

On suppose ensuite que chaque nombre ainsi obtenu est codé en binaire.

En supposant que le codage est sur 8 bits, combien de bits sont libres pour un bourrage aléatoire :

a. 3 bits ✓

b. 2 bits

c. 5 bits

d. 4 bits

Votre réponse est correcte.

Pour coder les 26 caractères, il faut utiliser 5 bits (2^5 = 32).

Comme le codage est sur 8 bits, il reste donc 8 - 5 = 3 bits pour le bourrage

La réponse correcte est :
3 bits

Question 30

Correct

Note de 1,00 sur 1,00

Suite de la question 29.

On considère une source S qui génère aléatoirement des chaînes de symboles pris au hasard dans l'alphabet A et qui les code en utilisant le codage de la question précédente.

On suppose que le bourrage utilisé est parfaitement aléatoire.

Quelle est l'entropie **d'un bloc de 64 bits** généré par S ?

a. 7,70 bits

b. 8 bits

c. 61,6 bits ✓

d. 64 bits

e. 37,6 bits

f. 24 bits

Votre réponse est correcte.

Entropie d'un octet (8 bits)

5 premiers bits : Log2(26) = 4,70

3 derniers : bourrage aléatoire d'entropie 3 bits

Total pour un octet : 4,70 + 3 = 7,70 bits

Entropie d'un bloc de 64 bits : 7,7 * 8 = 61,6 bits

La réponse correcte est :
61,6 bits