R3.09 Cryptographie QCM 1 - Sujet A

☐0 ☐0 ☐0 ☐0 ☐0 ☐0 ☐0
☐1 ☐1 ☐1 ☐1 ☐1 ☐1 ☐1
☐2 ☐2 ☐2 ☐2 ☐2 ☐2 ☐2
☐3 ☐3 ☐3 ☐3 ☐3 ☐3 ☐3
☐4 ☐4 ☐4 ☐4 ☐4 ☐4 ☐4
☐5 ☐5 ☐5 ☐5 ☐5 ☐5 ☐5
☐6 ☐6 ☐6 ☐6 ☐6 ☐6 ☐6
☐7 ☐7 ☐7 ☐7 ☐7 ☐7 ☐7
☐8 ☐8 ☐8 ☐8 ☐8 ☐8 ☐8
☐9 ☐9 ☐9 ☐9 ☐9 ☐9 ☐9

Aucun document autorisé.
Une seule bonne réponse par question.
Les mauvaises réponses entraîneront des pertes de points (+2 par bonne réponse, -0.5 par mauvaise réponse).
⟵ codez votre numéro de login ci-contre, et écrivez votre nom et prénom ci-dessous.

Nom et prénom :

.....

Question [Q1] A quoi est égal l'ensemble des éléments inversibles de $(\mathbb{Z}/14\mathbb{Z})$, c'est-à-dire $(\mathbb{Z}/14\mathbb{Z})^*$?

- ☐ $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}$
- ■ $\{1, 3, 5, 9, 11, 13\}$
- ☐ $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}$
- ☐ $\{1, 2, 7, 11, 13\}$

Question [Q2] Parmi ces algorithmes de chiffrement, lequel **n'est pas** une méthode de cryptographie symétrique ?

- ■ le chiffrement RSA
- ☐ le chiffrement de Hill
- ☐ le chiffrement de Vigenère
- ☐ le chiffrement affine

Question [Q3] Quelle est la valeur dans $\mathbb{R}$ du déterminant de la matrice $\begin{pmatrix} 5 & 2 \\ -2 & 2 \end{pmatrix}$?

- ■ 14
- ☐ 6
- ☐ 0
- ☐ -6

Question [Q4] Quelle affirmation est vraie ? Sachant que le déterminant de la matrice M dans $\mathbb{R}$ vaut 21, M est inversible dans :

- ☐ $\mathbb{Z}/81\mathbb{Z}$
- ☐ $\mathbb{Z}/42\mathbb{Z}$
- ■ $\mathbb{Z}/32\mathbb{Z}$
- ☐ $\mathbb{Z}/7\mathbb{Z}$

Question [Q5] Quelle est la comatrice de $\begin{pmatrix} 5 & -3 \\ 2 & 4 \end{pmatrix}$?

- ☐ $\begin{pmatrix} 5 & -3 \\ 2 & 4 \end{pmatrix}$
- ☐ $\begin{pmatrix} 4 & 2 \\ -3 & 5 \end{pmatrix}$
- ■ $\begin{pmatrix} 4 & -2 \\ 3 & 5 \end{pmatrix}$
- ☐ $\begin{pmatrix} -4 & 2 \\ -3 & -5 \end{pmatrix}$
- ☐ $\begin{pmatrix} -4 & -2 \\ 3 & -5 \end{pmatrix}$

Question [Q6] Quelle affirmation est vraie ? Sachant que l'indice de coïncidence du français est égal à 0.0746, un message (en français) chiffré avec un indice de coïncidence de 0.0701 :

- ☐ n'a probablement pas été chiffré par substitution monoalphabétique
- ■ sera certainement sensible à une attaque par analyse de fréquence
- ☐ a certainement été chiffré avec le chiffrement de Vigenère

Question [Q7] Dans le chiffrement de Hill avec une clef de dimension 2×2, les deux lettres `"c"` du message en clair `"cavalcade"` seront-elles chiffrées par la même lettre ?

- ☐ Non
- ☐ Oui
- ■ Cela dépend de la valeur de la clef

Question [Q8] Dans le chiffrement de Vigenère avec une clef de longueur 3 composée de 3 lettres différentes, les deux lettres `"s"` du message en clair `"sous"` seront-elles chiffrées par la même lettre ?

- ☐ Non
- ■ Oui
- ☐ Cela dépend de la valeur de la clef

Question [Q9] Parmi ces algorithmes de chiffrement, lequel **appartient** à la famille des chiffrements par substitution monoalphabétique ?

- ☐ Chiffrement RSA
- ☐ Chiffrement de Hill
- ☐ Chiffrement de Vigenère
- ■ Chiffrement affine

Question [Q10] Quel est l'inverse de 35 dans $\mathbb{Z}/144\mathbb{Z}$?

- ■ 107
- ☐ 37
- ☐ 9
- ☐ 35 n'est pas inversible dans $\mathbb{Z}/144\mathbb{Z}$