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.
⟵ codez votre numéro de login ci-contre, et écrivez votre nom et prénom ci-dessous.

Nom et prénom :

.....

Remarque : On considère que "chiffre/chiffrement de César" et "chiffrement par décalage" sont des synonymes.

Question [Q1] Combien 50 possède-t'il de diviseurs sur $\mathbb{Z}$?

- ■ 12
- ☐ Aucune des réponses proposées
- ☐ 3
- ☐ 6
- ☐ 2
- ☐ 4
- ☐ 8

Question [Q2] Quelle est la valeur du **quotient** dans la division euclidienne de 30 par -11 ?

- ■ -2
- ☐ 2
- ☐ -3
- ☐ 3

Question [Q3] Quelle est la valeur du **reste** dans la division euclidienne de -33 par 9 ?

- ■ 3
- ☐ -3
- ☐ 5
- ☐ -5
- ☐ 4
- ☐ -4
- ☐ 6
- ☐ -6

Question [Q4] Quel est le pgcd de 162 et 24 ?

- ■ 6
- ☐ 24
- ☐ 3
- ☐ 1
- ☐ 12
- ☐ 8
- ☐ 2
- ☐ Aucune des réponses proposées

Question [Q5] D'après le théorème de Bézout, il existe un couple $(u, v) \in \mathbb{Z}^2$ tel que $162u + 24v = pgcd(162, 24)$. Quelle est la valeur de v obtenue avec l'algorithme d'Euclide étendu ?

- [x] 7
- [ ] -7
- [ ] 1
- [ ] -1
- [ ] 24
- [ ] -24
- [ ] -5
- [ ] 5
- [ ] aucune des réponses proposées

Question [Q6] Quelle affirmation est **fausse** ?

- [ ] Dans $\mathbb{Z}/5\mathbb{Z}$, $27 \in \overline{2}$
- [ ] Dans $\mathbb{Z}/6\mathbb{Z}$, $-3 \in \overline{3}$
- [ ] Dans $\mathbb{Z}/5\mathbb{Z}$, -12 et 8 appartiennent à la même classe d'équivalence
- [x] Dans $\mathbb{Z}/6\mathbb{Z}$, 20 et 12 appartiennent à la même classe d'équivalence

Question [Q7] On se place dans $\mathbb{Z}/9\mathbb{Z}$, quelle affirmation est **vraie** ?

- [ ] L'opposé de $\overline{5}$ est $\overline{5}$
- [ ] $\overline{3} \times \overline{5} = \overline{5}$
- [ ] 8 et -8 appartiennent à la même classe d'équivalence
- [x] $\overline{3} - \overline{10} = \overline{2}$

Question [Q8] Quelle affirmation est **fausse** ?

- [ ] L'attaque par brute force est adaptée dans le cas d'un chiffrement par décalage.
- [x] Dans un chiffrement par décalage avec une clef de 6, un x du message en clair est remplacé par un r dans le chiffré.
- [ ] Il existe strictement moins de 26^2 clefs possible pour un chiffrement affine.
- [ ] Le chiffrement affine est un chiffrement par substitution monoalphabétique.

Question [Q9] A quoi est égal l'ensemble $(\mathbb{Z}/9\mathbb{Z})^*$?

- [ ] $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$
- [x] $\{1, 2, 4, 5, 7, 8\}$
- [ ] $\{1, 2, 3, 4, 5, 6, 7, 8\}$
- [ ] $\{1, 3, 6\}$

Question [Q10] Quel est l'**inverse** de $\overline{4}$ dans $\mathbb{Z}/9\mathbb{Z}$?

- [ ] $\overline{5}$
- [ ] Pas inversible dans $\mathbb{Z}/9\mathbb{Z}$
- [ ] $\overline{8}$
- [ ] $\overline{2}$
- [ ] $\overline{3}$
- [ ] $\overline{4}$
- [x] $\overline{7}$
- [ ] $\overline{6}$
- [ ] $\overline{1}$