Nom et prénom :

. . . . . .

Mathématiques pour la cryptographie
ENSIBS - S5 - 2022/2023

Contrôle

Durée : 50 minutes.

Les réponses devront toujours être justifiées. Les documents, les ordinateurs et les autres appareils électroniques sont interdits

---

Cocher la (ou les) bonne(s) réponse(s) aux questions à choix multiples.

Question 1. ***(Cours)*** *Donner l'énoncé complet du théorème d'identité de Bézout.*

. . . . . .
. . . . . .
. . . . . .

Question 2. ***(Cours)*** *Alice décide d'utiliser le cryptosystème RSA pour envoyer un message confidentiel M à Bob. La clé publique de Bob est (e, n) et sa clé privée est d.*

(a) *Quelle condition le message M doit remplir et comment elle le chiffre ?*

. . . . . .
. . . . . .

(b) *Supposons que Bob a reçu le message chiffré C. Comment il le déchiffre ?*

. . . . . .
. . . . . .

Question 3. *Un nombre pair ne peut pas être premier.*

☐ *Vrai* | ☐ *Faux*

Question 4. *Cocher les nombres qui ne sont pas premiers.*

☐ 9	☐ 98	☐ 57
☐ 55	☐ 0	☐ 1
☐ 11	☐ -7	☐ 79

Question 5. *Sachant que*

$$2052 = 17 \times 136 - 260,$$

quel est le reste de la division euclidienne de 2052 *par* 136 *?*

☐ 15
☐ 17
☐ *aucune des autres réponses proposées*
☐ 12
☐ -260

Question 6. *Soient $a, b, c \in \mathbb{N}$. Si $a|c$ et $b|c$ alors $ab|c$.*

☐ *Vrai* | ☐ *Faux*

Justifier : . . . . . .

Question 7. *Soient $a \in \mathbb{N}$ et p un nombre premier. Si $p|a^2$ alors $p|a$.*

☐ *Vrai* | ☐ *Faux*

Justifier : . . . . . .
. . . . . .

Exercice 1. *Résoudre dans $\mathbb{Z}$ le système*

$$\begin{cases} x \equiv 1\,[35] \\ x \equiv 2\,[24] \end{cases}.$$

Indication : $35 \times 11 - 24 \times 16 = 1$.

Exercice 2. *Supposons que $n = 101 \times 113$, $e_1 = 8765$, et $e_2 = 7653$. Note :* 101 *et* 113 *sont des nombres premiers.*

(1) Calculer $\varphi(n)$.

(2) Lequel de e_1 et e_2 est un choix valide de clé de chiffrement RSA (pour le module n). Justifier votre réponse.

(3) Pour l'exposant de cryptage valide, calculer la clé privée d, l'exposant de décryptage correspondant.

(4) En utilisant d, déchiffrer le message chiffré $c = 3233$.
Indication : calculer $c^8 \pmod n$.

Exercice 3. *Factoriser le nombre RSA $n = 3\,844\,384\,501$ comme produit de deux nombres premiers distincts sachant que*

$$3\,117\,761\,185^2 \equiv 1 \pmod n.$$