NOM : GROUPE :

R3.09 - Cryptographie et sécurité
Contrôle Terminal

Nom du responsable :	A. Ridard
Date du contrôle :	Mercredi 19 octobre 2022
Durée du contrôle :	1h30
Nombre total de pages :	7 pages : **1 à 4** + **5 à 7**
Impression :	A4 recto-verso agrafé (1 point)
Documents autorisés :	A4 recto-verso manuscrit
Calculatrice autorisée :	Oui
Réponses :	Directement sur le sujet

Exercice 1.

1. En utilisant **l'algorithme d'Euclide étendu**, déterminer $pgcd(255, 141)$ et une identité de Bézout.

2. (a) Décomposer en facteurs premiers 120 et 252.

   (b) En déduire le pgcd et le ppcm de 120 et 252.

Exercice 2.

1. Dresser la table de multiplication de $\mathbb{Z}/8\mathbb{Z}$.

×	0	1	2	3	4	5	6	7
0								
1								
2								
3								
4								
5								
6								
7								

2. Résoudre les équations suivantes **modulo 8** :
   (a) $5x + 2 \equiv 4$

   (b) $6x - 3 \equiv 0$

(c) $2x - 6 \equiv 6$

(d) $x^2 - 6 \equiv 3$

(e) $x^2 - 2x + 1 \equiv 4$

NOM : GROUPE :

Exercice 3.

Dans les deux premiers chiffrements, une lettre est représentée par son rang dans l'alphabet en partant de 0.

1. On considère la fonction de **chiffrement affine** suivante :

$$\begin{array}{rccc} \mathrm{E}_k : & \mathbb{Z}/26\mathbb{Z} & \longrightarrow & \mathbb{Z}/26\mathbb{Z} \\ & m_i & \longmapsto & c_i = 21m_i + 5 \end{array}$$

   (a) Chiffrer le message "LN".

   (b) Déchiffrer le message "AJO".

2. On considère la fonction de **chiffrement de Hill** suivante :

$$\begin{array}{rccc} E_k : & (\mathbb{Z}/26\mathbb{Z})^2 & \longrightarrow & (\mathbb{Z}/26\mathbb{Z})^2 \\ & \begin{pmatrix} m_i \\ m_{i+1} \end{pmatrix} & \longmapsto & \begin{pmatrix} c_i \\ c_{i+1} \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 1 & 5 \end{pmatrix} \begin{pmatrix} m_i \\ m_{i+1} \end{pmatrix} \end{array}$$

(a) Chiffrer le message "LN".

(b) Déchiffrer le message "DVAX".

3. On considère la fonction de **chiffrement RSA** suivante :

$$\begin{array}{rccc} \mathrm{E}_k : & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ & m_i & \longmapsto & c_i = m_i^e \end{array}$$

avec $n = pq = 11 \times 13$ et $e = 7$

(a) Déterminer la clé privée (n, d) où d est l'inverse de e modulo $\varphi(n)$.

(b) Déchiffrer le message "123".