Les réponses doivent être détaillées et justifiées.

Exercice 1

Chiffrement de César :

- Chiffrer le message
  "RENDEZ VOUS DEMAIN MIDI" en utilisant le chiffrement de César avec $k = 7$.
  → Mot chiffré : YLUKLG CVBZ KLTHPU TPKP.

- Si le message en clair est "RENDEZ VOUS DEMAIN MIDI" et le message chiffré en utilisant un chiffrement de César est "UHQGHC YRXVGHPDLQ PLGL"
  Donner la clé utilisée.
  → La clé utilisée est : $k = 3$

Chiffrement Affine :

- Chiffrer le mot PUT et le mot TER en utilisant le chiffrement affine avec $a = 13$ et $b = 4$.

  → *Le message chiffré de "PUT" est "RER"*
  → *Le message chiffré de "TER" est "RER"*

  Expliquer pourquoi ce chiffrement n'est pas convenable.
  → 13 n'est pas premier avec 26, alors il est impossible de déchiffrer.

- Déchiffrer le mot UCR chiffré en utilisant le chiffrement affine avec $a = 9$ et $b = 2$
  → Le mot chiffré est : CAT.

Chiffrement de Hill :

- Chiffrer le mot $MATH$ en utilisant le chiffrement de Hill avec clé la matrice suivante :
$$A = \begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$$
→ Le mot chiffré est : EIRO.
- Expliquer comment on déchiffre.
→ On déchiffre en utilisant l'inverse de la matrice de chiffrement A (voir le cours).

Exercice 2

- Expliquer comment on chiffre avec le RSA.
→ Voir le cours (réponse détaillée).
- On considère le chiffrement RSA avec $(n = 85, e = 5)$ comme clé publique.
- Chiffrer le message 9 en utilisant la clé publique $(n = 85, e = 5)$
→ $9^5 \equiv 59[85]$
- Déchiffrer le message 40.
→ La clé privée $(d, \varphi(n)) = (13, 64)$.
→ Déchiffrement : $40^{13} \equiv 10[64]$.

Exercice 3

Alice choisit $(n = 253, e = 3)$ comme clé publique, elle veut faire un virement de

$$229DA$$

- Que doit-elle faire.
- Comment la banque peut savoir la somme.
→ Voir le cours.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

q	r	s	t	u	v	w	x	y	z
16	17	18	19	20	21	22	23	24	25