Documents autorisés : cours, TD, notes manuscrites, calculatrice. **Durée** : 1h 30.

Barème indicatif : 2 + 2 + 2 + 3 + 5 + 3 + 3

Exercice 1

Inverse modulaire

Déterminer si l'inverse de $\overline{25}$ existe dans $\mathbb{Z}/27\mathbb{Z}$. Si c'est le cas, préciser l'inverse avec un représentant dans $[\![0, 26]\!]$. Expliquer.

Exercice 2

Petit théorème de Fermat

Montrer que le nombre premier 2 039 divise $2\,025^{2\,038} - 1$. Expliquer.

Exercice 3

Théorème du reste chinois

Résoudre dans $\mathbb{Z}$: $\begin{cases} x \equiv 5 \,(\mathrm{mod}\, 11) \\ x \equiv 6 \,(\mathrm{mod}\, 14) \end{cases}$

Exercice 4

Clés inverses

L'alphabet choisi est $\mathcal{A}_0 = \{A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z\}$ avec $n = |\mathcal{A}_0| = 26$.

On code chacun des symboles de l'alphabet en le remplaçant par son rang dans l'alphabet de la manière suivante.

Symbole	A	B	C	D	E	F	G	H	I	J	K	L	M
Rang x	0	1	2	3	4	5	6	7	8	9	10	11	12
Symbole	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Rang x	13	14	15	16	17	18	19	20	21	22	23	24	25

1. Dans le chiffrement de César, on prend la clé $k = F$. Déterminer la clé inverse k^{-1} (clé de déchiffrement) exprimée sous la forme d'un symbole. Expliquer.
2. Dans le chiffrement de Vigenère, on prend la clé $k = CUBES$. Déterminer la clé inverse k^{-1} exprimée sous la forme d'une suite de symboles. Expliquer.

Exercice 5

Chiffrement RSA

On choisit $p = 7$ et $q = 11$.

1. Préciser le module $n = pq$ et $m = (p-1)(q-1)$.
2. On choisit $c = 53$. Déterminer d tel que $cd \equiv 1 \pmod{m}$, $d \in [\![0; m-1]\!]$. Expliquer.

3. On souhaite déchiffrer le nombre $m_c = 5$.
   (a) Décomposer d en base 2.
   (b) Calculer $5^i \pmod n$ avec $i \in \{2^j\}$, $j \in [\![1, 4]\!]$ (donner le représentant dans $[\![0; n-1]\!]$). Reproduire et compléter le tableau suivant.

j	1	2	3	4
$5^{2^j} \pmod n$				

   (c) En déduire le message déchiffré $m_d \equiv 5^d \pmod n$. On donnera le représentant dans $[\![0; n-1]\!]$.

Exercice 6

Chiffrement affine
L'alphabet choisi est $\mathcal{A}_0 = \{A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z\}$ avec $n = |\mathcal{A}_0| = 26$.
On code chacun des symboles de l'alphabet en le remplaçant par son rang dans l'alphabet de la manière suivante.

Symbole	A	B	C	D	E	F	G	H	I	J	K	L	M
Rang x	0	1	2	3	4	5	6	7	8	9	10	11	12
Symbole	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Rang x	13	14	15	16	17	18	19	20	21	22	23	24	25

On note la clé de chiffrement $k = (a, b) \in \mathbb{Z}^2$ avec $A = \overline{a}$ inversible dans $\mathbb{Z}/n\mathbb{Z}$.
La fonction de chiffrement associée s'écrit $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ définie par $f(X) = AX + B$ avec $B = \overline{b}$.
Le message AP a été chiffré CH.

1. Déterminer la clé de chiffrement $k = (a, b)$ avec a et b dans $[\![0, n-1]\!]$. Expliquer.
2. Déterminer le message déchiffré du texte chiffré HW pour la clé trouvée.
   Indication : on pourra d'abord préciser la clé inverse $k^{-1} = (a', b')$.

Exercice 7

Chiffrement de Hill
On note $\mathcal{A} = \{A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z, *\}$ ($*$ représente l'espace) et $n = |\mathcal{A}| = 27$.
On code chacun des symboles de l'alphabet en le remplaçant par son rang dans l'alphabet de la manière suivante.

Symbole	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Rang x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
Symbole	O	P	Q	R	S	T	U	V	W	X	Y	Z	*	
Rang x	14	15	16	17	18	19	20	21	22	23	24	25	26	

Dans le chiffrement de Hill, on prend la clé $M = \begin{pmatrix} \overline{3} & \overline{10} \\ \overline{14} & \overline{19} \end{pmatrix}$.

1. Chiffrer le mot BU. Expliquer.

2. Déterminer la clé inverse M^{-1}. Expliquer.
   Les représentants des coefficients de M^{-1} seront pris dans $[\![0, n-1]\!]$.
3. Déchiffrer le mot KL. Expliquer.