

FEUILLE D'EXERCICES n° 6
Cryptographie classique 2

On rappelle la numérotation des lettres de l'alphabet :

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Exercice 1 –

- 1) Définir le chiffrement affine. Montrer que le chiffrement par décalage est un cas particulier.
- 2) Montrer que l'équation $ax \equiv b \pmod{m}$ a une unique solution dans $\mathbb{Z}/m\mathbb{Z}$ si et seulement si $(a, m) = 1$.
- 3) Exprimer le nombre de clés possibles à l'aide de la fonction indicatrice d'Euler.
- 4) Coder le message **La rencontre est prévue à la cafétéria** à l'aide de cette méthode et de la clé $K = (a, b) = (7, 2)$.
- 5) Déterminer la fonction de décryptage associée à K .

Exercice 2 – Le message **Quelle est la clef** a été chiffré par un chiffrement affine et le résultat est **CMYJJYYUDJOGJYH**. Déterminer la clé du message.

Exercice 3 –

- 1) Définir le chiffrement de Hill.
- 2) Coder le message **La rencontre est prévue à la cafétéria** à l'aide de cette méthode et de la clé suivante

$$K = \begin{pmatrix} 1 & 2 & 3 & 0 \\ 2 & 0 & 1 & 0 \\ 3 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

- 3) Décoder le message **CJLRYMLPQUNETBQJJHME** sachant qu'il a été créé avec la clé précédente.

Exercice 4 – On suppose que le message **C'est fini** est codé par la méthode de Hill avec $m = 2$. On obtient le message **UYSJVPZL**. Déterminer la clé du codage.