Cryptologie
MHT203

Feuille d'exercices 6
Cryptographie classique 2

On rappelle qu'on a la numérotation des lettres de l'alphabet suivante :

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
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

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

Exercice 2.
Le message suivant a été chiffré par un chiffrement affine et le résultat est donné ci-dessous. Déterminer la clé du message.
QUELLE EST LA CLEF
CMYJJYYUDJOGJYH

Exercice 3.
a. Définir le chiffrement de Hill.
b. Coder le message "la rencontre est prévue à la cafétéria" à l'aide de cette méthode et de la clé suivante

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

c. 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.