Université Bordeaux 1 — **MHT633 – Arithmétique et Cryptologie**
Mathématiques — Année 2008–2009

Partiel du Lundi 16 mars 2009
Durée 1h20. Documents interdits.

Une lettre de l'alphabet est identifiée à un élément de l'anneau $A = \mathbb{Z}/26\mathbb{Z}$ à l'aide du tableau

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 – [Chiffrement affine]
On fixe deux éléments a et b de $A = \mathbb{Z}/26\mathbb{Z}$; à la clé $K = (a, b)$, on associe la fonction de chiffrement

$$\begin{array}{rccc} e_K & : & A & \longrightarrow A \\ & & x & \longmapsto ax + b. \end{array}$$

1) Quelles sont les valeurs de a qui permettent d'obtenir une fonction de chiffrement inversible ?

2) On chiffre par blocs de taille 1 ; le clair « UN » est chiffré « OR ». Retrouver la clé de chiffrement.

3) Déterminer le clair du texte chiffré « GJESH », pour la clé ci-dessus.

Exercice 2 – [Hill affine]
On considère M une matrice 2×2 à coefficients dans $A = \mathbb{Z}/26\mathbb{Z}$, inversible, et B un vecteur ligne de longueur 2 à coefficients dans A. À la clé $K = (M, B)$, on associe la fonction de chiffrement

$$\begin{array}{rccc} e_K & : & A^2 & \longrightarrow A^2 \\ & & X & \longmapsto XM + B, \end{array}$$

où A^2 désigne l'ensemble des vecteurs lignes de longueur 2 à coefficients dans A. Pour chiffrer un texte ayant un nombre pair de caractères, on chiffre successivement les blocs de longueur 2 du texte à l'aide de e_K.

1) Le mot « SIMPLE » a été chiffré « ZAEZQQ ». Retrouver la clé de chiffrement.

2) Déchiffrer « DM ».

Exercice 3 – [Pohlig-Hellman]
On identifie ici l'alphabet à $B := \{0, 1, \ldots, 25\}$ (même correspondance qu'en introduction) mais cette fois-ci B est considéré comme sous-ensemble de $\mathbb{Z}/29\mathbb{Z}$. On prend comme clé de chiffrement un entier e vérifiant $2 \leqslant e \leqslant 28$. La fonction de chiffrement est

$$m \longmapsto m^e \bmod \mathbb{Z}/29\mathbb{Z}.$$

1) Quels sont les choix de e qui permettent de définir un chiffrement injectif ?

2) On a chiffré « C » en « 14 ». Retrouver e.

3) Quelles sont les autres lettres dont le chiffrement permet de retrouver e ?