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

FEUILLE D'EXERCICES n° 2

Systèmes de chiffrement symétriques anciens

On rappelle que dans le cas de l'alphabet usuel à 26 lettres on utilise 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	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]
Étant donnés deux entiers a et b, une lettre de l'alphabet est identifiée à un élément x de l'anneau $\mathbb{Z}/26\mathbb{Z}$ et est chiffrée en $ax + b$.

1) Montrez que la fonction de chiffrement est inversible ssi $a \mod 26 \in (\mathbb{Z}/26\mathbb{Z})^*$ et calculez son inverse. Précisez les données $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ de ce système de chiffrement. Quel est le cardinal de $\mathcal{K}$?

2) Un chiffrement affine dont vous ne connaissez pas la clé a chiffré le texte clair `hahaha` en `nonono`. Retrouvez la clé. (Il s'agit d'une attaque à texte clair connu). Calculez la clé de déchiffrement.

3) Montrez que la composée de deux chiffrements affines est encore un chiffrement affine.

4) Montrez qu'un chiffrement par décalage est un cas particulier de chiffrement affine. Montrez qu'un chiffrement affine est un cas particulier de chiffrement de substitution.

5) Généralisez la définition d'un système de chiffrement affine sur l'anneau $A = \mathbb{Z}/m\mathbb{Z}$. Généralisez l'attaque précédente : que doit avoir en sa possession un attaquant pour calculer la clé ?

Exercice 2 – [Matrices à coefficients dans un anneau]
Soit $(A, +, \cdot)$ un anneau commutatif et unitaire.

1) Montrez que l'ensemble des matrices à n lignes et n colonnes, à coefficients dans A, est un anneau pour l'addition et la multiplication des matrices. On le note $M_n(A)$.

2) Montrez que $M \in M_n(A)$ est inversible si et seulement si $\det(A)$ est inversible dans A.

3) Pour $n = 2$, montrez que $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ est inversible dans $M_2(A)$ si et seulement si $ad - bc \in A^*$ et que dans ce cas

$$M^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

4) On note $\mathrm{GL}_n(A)$ le groupe des matrices inversibles de $M_n(A)$. Montrez que l'ordre de $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ où p est un nombre premier est $(p^2-1)(p^2-p)$. [*Cherchez quelles conditions les colonnes d'une matrice inversible doivent satisfaire.*]

5) Généralisation : montrez que

$$|\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})| = (p^n - 1)(p^n - p)(p^n - p^2)\dots(p^n - p^{n-1}).$$

Exercice 3 – [Chiffrement de Hill]
Soit $K \in \mathrm{GL}_n(A)$, on définit

$$\begin{aligned} e_K : A^n &\to A^n \\ x &\mapsto xK \end{aligned}$$

1) Montrez qu'on définit ainsi un système de chiffrement symétrique dont on précisera les données $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$.

2) Exemple numérique : `YIFZMA` est un texte chiffré par un chiffrement de Hill avec $n = 2$ et $A = \mathbb{Z}/26\mathbb{Z}$, de matrice $K = \left(\begin{smallmatrix} 9 & 13 \\ 2 & 3 \end{smallmatrix}\right)$. Retrouvez le clair.

3) Eve a volé la machine à chiffrer de Bob, qui utilise un chiffrement de Hill avec une matrice 2×2 sur $\mathbb{Z}/26\mathbb{Z}$. Elle tente une attaque à texte choisi : le texte clair `ba` est chiffré en `HC` et le texte clair `zz` est chiffré en `GT`. Quelle est la clé ? Quelle est la clé de déchiffrement ? Que pensez-vous des choix de Eve ?

4) Généralisez l'attaque de Eve (à clair choisi) à un système de chiffrement de Hill quelconque.

5) Montrez que la composée de deux chiffrements de Hill est encore un chiffrement de Hill. Vous considèrerez le cas de matrices de même taille, puis de tailles différentes.

6) Montrez qu'un chiffrement par permutation est un cas particulier d'un chiffrement de Hill.

Exercice 4 – [Chiffrement de Hill affine]
Soit $K \in \mathrm{GL}_n(A)$ et $b \in A^n$. On définit

$$\begin{aligned} e_K : A^n &\to A^n \\ x &\mapsto xK + b \end{aligned}$$

1) Montrez qu'on définit ainsi un système de chiffrement symétrique dont on précisera les données $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$.

2) Généralisez l'attaque sur le chiffrement de Hill à ce système.

Exercice 5 – `GEZXDS` est un texte chiffré par un chiffrement de Hill de matrice 2×2. Le clair est `solved`. Trouvez la clé. Calculez ensuite la clé de déchiffrement.

Exercice 6 – (Extrait du DS 2007) Déchiffrer le texte suivant, chiffré avec le chiffrement affine :

`JGMGJGUFEOVMHTGMENGVFEGJJGM`

On donnera la clef de chiffrement ainsi que la clef de déchiffrement.