# DS du 1er avril 2010

Durée 1h30 - documents autorisés

Ce sujet comprend trois exercices indépendants.

## Exercice 1. *Chiffrement de Hill*

Voici le codage numérique des 26 lettres utilisé dans cet exercice :

| $A$ | $B$ | $C$ | $D$ | $E$ | $F$ | $G$ | $H$ | $I$ | $J$ | $K$ | $L$ | $M$ | $N$ | $O$ | $P$ | $Q$ | $R$ | $S$ | $T$ | $U$ | $V$ | $W$ | $X$ | $Y$ | $Z$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |

Le procédé de chiffrement de Hill consiste à chiffrer des blocs de $p$ lettres du texte clair, en les multipliant par une matrice carrée d'ordre $p$. Ainsi, si on désigne par $m_1, m_2, \ldots, m_p$ $p$ lettres consécutives du texte clair, chacune d'elles étant représentée par son équivalent numérique selon la table ci-dessus, et par $c_1, c_2, \ldots, c_p$ les $p$ lettres consécutives correspondantes dans le texte chiffré, on a la relation

$$\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_p \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1p} \\ a_{21} & a_{22} & \ldots & a_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ a_{p1} & a_{p2} & \ldots & a_{1p} \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_p \end{pmatrix} \pmod{26}.$$

où les coefficients $a_{ij}$ de la matrice sont des nombres entiers compris entre 0 et 25. Les calculs se font selon les règles usuelles du calcul matriciel, avec une arithmétique modulo 26. La matrice utilisée dans ce procédé est la clé de chiffrement.

Dans tout cet exercice on considère le cas $p = 2$, et on note $\mathcal{M}_2(\mathbb{Z}/26\mathbb{Z})$ l'ensemble des matrices carrées d'ordre 2 à coefficients modulo 26.

On rappelle que

1. le déterminant d'une matrice carrée d'ordre 2 est
$$\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = a_{11}a_{22} - a_{12}a_{21},$$
2. et celui d'un produit de deux matrices $A$ et $B$ est le produit des déterminants des deux matrices
$$\det(AB) = (\det A)(\det B).$$

**Question 1.** Soit $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ une matrice. On pose $A^* = \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}$. Calculez le produit $AA^*$ des deux matrices, et en déduire une condition nécessaire et suffisante pour que $A$ soit inversible dans $\mathcal{M}_2(\mathbb{Z}/26\mathbb{Z})$, et exprimez alors la matrice inverse $A^{-1}$.

**Question 2.** Des deux matrices ci-dessous une est inversible l'autre non. Quelle est celle qui est inversible, et quel est son inverse ?

$$A_1 = \begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix} \quad A_2 = \begin{pmatrix} 25 & 2 \\ 6 & 1 \end{pmatrix}$$

**Question 3.** Quelle condition nécessaire et suffisante doit vérifier la matrice utilisée dans le procédé de chiffrement de Hill, pour qu'il soit possible de déchiffrer ?

**Question 4.** Déchiffrez le message `PJKH` qui a été obtenu par le procédé de Hill avec la matrice inversible de la question 2 pour clé de chiffrement.

**Question 5.** Le message clair $\mathbf{m}$ = `TOUT` a été chiffré en $\mathbf{c}$ = `RIEN`. Pouvez-vous déterminer la clé de chiffrement ?

Pour vérifier, décryptez le message `XGLB`.

**Question 6.** Expliquez en quoi le travail effectué dans la question précédente montre que le chiffrement de Hill est inutilisable pour assurer la confidentialité des échanges d'information de nos jours.

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

TABLE 1 – Table de multiplication dans $\mathbb{Z}/26\mathbb{Z}$

**Exercice 2.** *Chiffrement par blocs*

**Question 1.** Après avoir rappelé ce qu'est le schéma de Feistel, indiquez quel est son intérêt.

**Question 2.** Que pensez–vous du chiffrement obtenu en supprimant la phase de transformation par les boîtes-S à chaque tour du DES ?

**Question 3.** Lorsqu'on chiffre deux fois le même fichier à l'aide de la même clé avec du DES, obtient–on toujours le même chiffré ?

**Question 4.** Vous disposez d'une fonction de chiffrement par blocs, mais vous n'avez pas la procédure de déchiffrement. Comment pouvez–vous construire un système complet de chiffrement et déchiffrement par blocs ?

**Exercice 3.** *Corps finis*

**Question 1.** Parmi les polynômes suivants, de $\mathbb{F}_2[X]$, un seul est irréductible. Dîtes lequel en expliquant pourquoi.

$$P_1(X) = X^6+X^4+1,\ P_2(X) = X^6+X^5+X+1,\ P_3(X) = X^6+X^3+1,\ P_4(X) = X^6+X^5+X^4+X^3+1.$$

**Question 2.** Soit $P(X)$ le polynôme irréductible de la question précédente. On considère le corps $\mathbb{F}_{64} = \mathbb{F}_2[X]/P(X)$. Soient les deux éléments de ce corps : $\alpha = X$ et $\beta = X^5 + X^3 + X + 1$. Calculez le produit $\alpha\beta$ dans $\mathbb{F}_{64}$.

**Question 3.** $\alpha$ est-il un élément primitif ?

**Question 4.** Combien y a -t-il d'éléments primitifs dans $\mathbb{F}_{64}^*$ ?

**Question 5.** Décrivez une méthode probabiliste par tirage au sort pour trouver dans $\mathbb{F}_{64}^*$ un élément primitif, et estimez le nombre d'essais que devra effectuer en moyenne votre algorithme.