

**Devoir Surveillé, 6 mars 2019**  
**Durée 1h30, documents interdits**

*La qualité de la rédaction sera un facteur d'appréciation.*

**Exercice 1** – On considère un système de chiffrement où l'espace des messages clairs est  $\mathcal{M} = \{a, b, c\}$ , l'espace des messages chiffrés est  $\mathcal{C} = \{1, 2, 3, 4\}$  et celui des clés est  $\mathcal{K} = \{\text{i}, \text{ii}, \text{iii}, \text{iv}, \text{v}, \text{vi}, \text{vii}, \text{viii}\}$ . Le système est décrit par le tableau suivant :

$\mathcal{M} \setminus \mathcal{K}$	i	ii	iii	iv	v	vi	vii	viii
a	1	2	3	4	3	4	1	2
b	2	4	4	3	2	1	3	1
c	3	1	2	1	4	2	4	4

On suppose que les messages clairs et les clés sont équiprobables. On suppose aussi que la clé est indépendante du message clair.

- 1) Calculer  $P(M = c | C = 4)$  et en déduire que le système n'est pas à confidentialité parfaite.
- 2) Changer le contenu d'une seule case de manière à le rendre à confidentialité parfaite. Justifier.
- 3) Déterminer les probabilités d'imposture et de substitution du système initial, ainsi que celles du système transformé.

**Exercice 2** – Soient  $n$  un entier positif et  $E_K : \mathbb{F}_2^{2n} \rightarrow \mathbb{F}_2^{2n}$  une fonction de chiffrement à clé secrète  $K$  agissant sur des blocs de  $2n$  bits. Considérons la variante suivante du mode opératoire CFB. Le message clair est découpé en blocs de  $n$  bits :  $M = M_1 \| M_2 \| M_3 \| \dots$ , où  $M_i \in \mathbb{F}_2^n$  pour tout  $i$ . On choisit un vecteur initial  $V_0$  de  $2n$  bits puis pour  $i = 1, 2, 3, \dots$ , on pose :

- (1)  $C_i = M_i \oplus L_n(E_K(V_{i-1}))$
- (2)  $V_i = R_n(V_{i-1}) \| C_i$

où  $L_n(X)$  et  $R_n(X)$  désignent les parties gauches et droites (comportant  $n$  bits) de  $X \in \mathbb{F}_2^{2n}$ . Le chiffré est  $C = V_0 \| C_1 \| C_2 \| C_3 \| \dots$

- 1) Décrire l'algorithme de déchiffrement.
- 2) On chiffre  $M$  qui comporte au moins 5 blocs. Au cours de la transmission de  $C$ , le bloc  $C_1$  est altéré en  $C' \neq C_1$ , les autres blocs étant correctement transmis. Combien de blocs seront probablement erronés à l'issue du déchiffrement ?

**Exercice 3** – On rappelle que dans AES, la transformation **MixColumns** s'interprète comme une multiplication matricielle :

$$\begin{array}{|c|c|c|c|} \hline a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ \hline a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ \hline a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ \hline a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \\ \hline \end{array} \rightarrow \begin{array}{|c|c|c|c|} \hline b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} \\ \hline b_{1,0} & b_{1,1} & b_{1,2} & b_{1,3} \\ \hline b_{2,0} & b_{2,1} & b_{2,2} & b_{2,3} \\ \hline b_{3,0} & b_{3,1} & b_{3,2} & b_{3,3} \\ \hline \end{array}$$

où

$$\begin{pmatrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} \\ b_{1,0} & b_{1,1} & b_{1,2} & b_{1,3} \\ b_{2,0} & b_{2,1} & b_{2,2} & b_{2,3} \\ b_{3,0} & b_{3,1} & b_{3,2} & b_{3,3} \end{pmatrix} = \begin{pmatrix} \alpha & \alpha+1 & 1 & 1 \\ 1 & \alpha & \alpha+1 & 1 \\ 1 & 1 & \alpha & \alpha+1 \\ \alpha+1 & 1 & 1 & \alpha \end{pmatrix} \begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}$$

est le produit des matrices à coefficients dans  $\mathbb{F}_{256}$  et où  $\alpha$  est la classe de  $X$  dans

$$\mathbb{F}_{256} = \mathbb{F}_2[X]/\langle X^8 + X^4 + X^3 + X + 1 \rangle.$$

Montrer qu'il existe un polynôme  $Q(X) \in \mathbb{F}_{256}[X]$  de degré  $\leq 3$ , polynôme que l'on explicitera, tel que pour tout  $0 \leq j \leq 3$ , on ait :

$$b_{0,j} + b_{1,j}X + b_{2,j}X^2 + b_{3,j}X^3 = Q(X)(a_{0,j} + a_{1,j}X + a_{2,j}X^2 + a_{3,j}X^3) \bmod (X^4 + 1).$$

**Exercice 4** – Soit  $(s_i)_{i \geq 0} \in \mathbb{F}_2^\mathbb{N}$  une suite engendrée par la relation

$$s_{i+k} = a_{k-1}s_{i+k-1} + \cdots + a_1s_{i+1} + a_0s_i,$$

où  $k \geq 1$ ,  $(a_0, a_1, \dots, a_{k-1}) \in \mathbb{F}_2^k$  et  $a_0 \neq 0$ . Comme  $a_0 \neq 0$ , la suite  $(s_i)_{i \geq 0}$  est périodique de période  $\pi$ . On note  $A$  la matrice associée :

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \\ a_0 & a_1 & \cdots & a_{k-2} & a_{k-1} \end{pmatrix},$$

$P(X) = X^k + a_{k-1}X^{k-1} + \cdots + a_1X + a_0$  son polynôme caractéristique et  $\alpha$  la classe de  $X$  dans l'anneau  $B = \mathbb{F}_2[X]/\langle P(X) \rangle$ .

Si  $P(X)$  est irréductible, on sait par le cours du premier semestre que  $\alpha \in B^\times$  et que la période  $\pi$  est égale à l'ordre de  $\alpha$  dans  $B^\times$  (lorsque la graine est non nulle). Ici, on cherche à généraliser ce résultat, en ne supposant plus  $P(X)$  irréductible.

1) Montrer que  $\alpha \in B^\times$ .

2) Soit  $r$  l'ordre de  $\alpha$  dans  $B^\times$ . Montrer qu'il existe  $Q(X) \in \mathbb{F}_2[X]$  tel que

$$X^r = 1 + Q(X)P(X).$$

3) En déduire que  $\pi$  divise  $r$ .

4) Donner un exemple dans lequel  $k = 3$  et  $1 < \pi < r$ .

5) On considère la relation de récurrence linéaire

$$s_{i+7} = s_{i+6} + s_{i+5} + s_{i+1} + s_i \text{ pour tout } i \geq 0. \quad (1)$$

Soient  $u = (u_i)_{i \geq 0}$  et  $v = (v_i)_{i \geq 0}$  les suites engendrées par cette relation de graines respectives  $(1, 0, 1, 1, 1, 0, 0)$  et  $(1, 1, 0, 1, 0, 1, 1)$ .

a) Quelles sont les périodes de  $u$  et  $v$  ?

b) Déterminer les séries génératrices de  $u$  et  $v$ . On les mettra sous forme de fractions rationnelles irréductibles<sup>1</sup>.

c) En déduire les plus courtes relations de récurrence linéaire définissant  $u$  et  $v$ .

d) Soit comme précédemment  $\alpha$  la classe de  $X$  dans l'anneau  $B = \mathbb{F}_2[X]/\langle P(X) \rangle$ , où  $P(X)$  est le polynôme caractéristique associé à la relation (1). Quel est l'ordre  $r$  de  $\alpha$  dans  $B^\times$  ?

e) Montrer que  $u + v$  obéit à la relation (1). La période de  $u + v$  est-elle égale à  $r$  ?

---

<sup>1</sup>On pourra admettre que dans  $\mathbb{F}_2[X]$  on a :  $X^{14} + X^{13} + X^9 + X^6 + X^5 + X^3 + X + 1 = (X + 1)(X^2 + X + 1)(X^3 + X^2 + 1)(X^4 + X^3 + 1)(X^4 + X^3 + X^2 + X + 1)$ .