Licence 3 – MHT633 Université Bordeaux 1
2009/2010

Feuille 6 : AES et Corps Finis

Exercice 1. Travail dans $\mathbb{F}_{16}$

1. Soit n un entier supérieur ou égale à 2. Quand $\mathbb{Z}/n\mathbb{Z}$ est il un corps ?
2. On note $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Trouver dans $\mathbb{F}_2[X]$ tous les polynômes irréductibles de degrés 1, 2, 3 et 4.
3. On considère le polynôme $P(X) = X^4 + X + 1$ qui est irréductible dans $\mathbb{F}_2[X]$ et l'on pose
$$\mathbb{F}_{16} = \mathbb{F}_2[X]/(P(X)),$$
qui est un corps à 16 éléments. Vérifier que $\alpha = X \bmod P(X)$ engendre $\mathbb{F}_{16}^*$. On dressera la liste des puissances de α sous la forme de 4-uplets $(\varepsilon_3, \varepsilon_2, \varepsilon_1, \varepsilon_0)$, où $\varepsilon_i \in \mathbb{F}_2$, représentant l'élément $\sum_{i=0}^{3} \varepsilon_i \alpha^i$. Par exemple
$$\alpha^5 = \alpha^2 + \alpha = (0, 1, 1, 0).$$
4. À l'aide de ce codage, coder $\alpha^{57} \cdot \alpha^{18}$ puis $\alpha^{13} + \alpha^{11} + \alpha^8 + \alpha^2 + 1$ et calculer les comme puissances de α.
5. Calculez l'inverse de $\alpha^2 + 1$ dans $\mathbb{F}_{16}$.
6. Identifier un corps à 4 éléments dans $\mathbb{F}_{16}$.
7. À chaque indice i $(1 \leq i \leq 14)$ on associe j $(1 \leq j \leq 14)$ tel que
$$\omega^j = 1 + \omega^i.$$
Montrer qu'un tel j est bien défini et qu'alors on a $\omega^i = \omega^j + 1$.
On écrira alors $i \longleftrightarrow j$ et on parlera de correspondance de Zech. Dresser la liste des correspondances de Zech de $\mathbb{F}_{16}$.
8. Montrer que le recours à ces correspondances peut ramener le calcul de sommes de puissances de ω à celui beaucoup plus simple de produits de puissances de ω.

Exercice 2. AES - Chiffrement

Le principe d'AES a été vu en cours et une feuille complémentaire a été donnée qui résume les différentes étapes du chiffrement.

1. Appliquer `SubBytes` à l'octet (00001001).

2. Appliquer `MixColumns` au tableau

$$\begin{pmatrix} (11000001) & (00000111) & (00000000) & (11111111) \\ (11000000) & (00001000) & (00011110) & (11111100) \\ (11000011) & (00000100) & (00000001) & (11100000) \\ (10001001) & (00000110) & (11000000) & (00010111) \end{pmatrix}.$$

On se contentera de calculer quelques nouveaux octets.

Exercice 3. AES - Déchiffrement

1. Définir la procédure inverse de chacune des procédures `SubBytes`, `ShiftRows`, `MixColumns` et `AddRoundKey`.
2. Montrer que l'on peut permuter `InvShiftRows` et `InvSubBytes`.
3. Indiquer comment modifier la clé de tour correspondante pour pouvoir permuter les procédures `AddRoundKey` et `InvMixColumns`.
4. Donner un découpage en tours pour le déchiffrement qui applique à chaque tour les procédures inverses des procédures de chiffrement *dans le même ordre que les procédures initiales*, en indiquant comment modifier l'expansion de clé (concaténation des clés de tour).

Exercice 4. Une attaque exhaustive de AES

On dispose d'un couple clair chiffré et on souhaite trouver la clé AES utilisée par une recherche exhaustive. On suppose donné un ordinateur capable de faire 2800 millions d'opérations par seconde et dans lequel est implémenté un algorithme qui teste une clé avec un coût de 1200 millions d'opérations.

1. Quel est le nombre moyen de clés à tester avant de trouver la bonne ?
2. Quel est le temps de calcul moyen pour trouver la clé avec un ordinateur ?
3. Quel est le temps de calcul moyen si l'on dispose de 400 millions de PC ?