Licence 3 – MHT633 Université Bordeaux 1
2010/2011

Feuille 6 : Cryptographie symétrique 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 $\alpha^j = 1 + \alpha^i$. Montrer qu'un tel j est bien défini et qu'alors on a $\alpha^i = \alpha^j + 1$.
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 α à celui beaucoup plus simple de produits de puissances de α.

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. DES

Le Data Encryption Standard (DES) est un algorithme de chiffrement par bloc qui était l'algorithme standard utilisé avant l'AES de 1977 à 1999. Le DES utilise des clefs de 56 bits et chiffre un bloc de 64 bits en un autre bloc de 64 bits. Hormis deux permutations initiales et finales, c'est un schéma itératif dit de Feistel. À partir de la clef K de 56 bits, un algorithme de cadencement de clefs produit 16 clefs de tours de 48 bits, notées $K_1, K_2, \ldots, K_{16}$. Le message clair est découpé en deux blocs de 32 bits notés L_0 et R_0. On effectue ensuite 16 tours en utilisant une fonction f prenant en entrée un sous bloc de 32 bits et une clef de tour de 48 bits, et retournant un sous bloc de 32 bits. Plus précisément, au tour i, pour $i \in \{1, \ldots, 16\}$, on a

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

et le chiffré est la concaténation des sous blocs R_{16} et L_{16}.

1. Faire un dessin de l'algorithme de chiffrement.
2. Expliciter l'algorithme de déchiffrement. Est-il nécessaire que les fonctions $f(\cdot, K_i)$ soient bijectives ?
3. L'algorithme de cadencement de clefs du DES est tel que si on utilise le complément bit à bit $\bar{K}$ de la clef K alors on obtient les clefs de tours $\bar{K}_1$, $\bar{K}_2, \ldots, \bar{K}_{16}$. D'autre part, pour la fonction f on a la propriété $f(\bar{r}, \bar{k}) = f(r, k)$. Que peut on dire du chiffré d'un message $\bar{M}$ avec la clef $\bar{K}$?
4. Oscar obtient deux couples (M, C_1) et $(\bar{M}, C_2)$ où C_1 (resp. C_2) est le chiffré de M (resp. $\bar{M}$) avec le DES et une même clef K. Comment Oscar peut-il utiliser la propriété de complémentarité du DES pour améliorer l'attaque par recherche exhaustive ?