Travaux Dirigés de MT10

Calculs dans F(2^8)

Ce TD poursuit le TD précédent avec des calculs dans F(2^8) qui est le corps utilisé pour l'AES. Les éléments de corps sont donc les polynômes à coefficients dans Z/2Z de degré maximal 7, le polynôme modulo étant $m(x) = x^8 + x^4 + x^3 + x + 1$ qui est bien irréductible comme on peut s'en convaincre en poursuivant la démarche esquissée dans le TD précédent.
Les éléments du corps sont assimilés à l'octet équivalent à leurs coefficients que l'on écrira en Hexa entre accolades dans ce TD :
$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ est par exemple l'octet {FF}
Le polynôme modulo s'écrit donc sur deux octets : {01}{1B}

1) Afin de déterminer le nombre de constructions possibles de F(2^8), donner tous les sous-corps de F(2^8)
   Réponse : ce sont tous les F(2^n) où n est un diviseur de 8 soit donc F(2^1), F(2^2) et F(2^4). Ainsi on peut construire F(2^8) comme extension de degré 8 de F(2) avec un polynôme de degré 8 à coefficients dans F(2), extension de degré 4 de F(4) avec un polynôme de degré 4 à coefficients dans F(4) ou comme extension de degré 2 de F(16) avec un polynôme de degré 2 à coefficients dans F(16). On observe de F(256) contient donc F(2), F(4) et F(16), mais pas F(8)

2) Les éléments de F(2^8) étant racines du polynôme x^{256}-x qui doit être le produit de tous les polynômes de construction possibles de F(2^8) et de tous ses sous-corps (sans oublier x et x+1 dont les racines sont les éléments de Z/2Z), déterminer le nombre de polynômes possibles permettant de construire F(2^8)
   Réponse : x^{256}-x va donc se mettre sous la forme du produit de x(x+1) dont les racines sont les éléments de F(2), par x^2+x+1 dont les deux racines de F(4) qui ne sont pas dans F(2), pas $(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$ dont les 12 racines sont les éléments de F(16) qui ne sont pas dans F(4) et donc pas non plus dans F(2), par tous les polynômes de degré 8 dont les racines sont donc les 240 éléments de F(256) qui ne sont pas dans F(16) donc pas non plus dans F(4) ni dans F(2). Il y a donc 240/8=30 tels polynômes qui sont les 30 polynômes de construction possibles de F(16) en tant qu'extension de degré 8 de F(2). Le produit de ces 30 polynômes (degré total 240), par $x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$ (degré total 16) donne bien un polynôme de degré 256 qui est donc nécessairement x^{256}-x

3) En effectuant la multiplication polynomiale modulo m(x), effectuer dans la construction de F(2^8) choisie pour l'AES la multiplication {19}*{3F}

Réponse :
{19} = 00011001 = x^4+x^3+1
{3F} = 00111111 = $x^5+x^4+x^3+x^2+x+1$
$(x^4+x^3+1)(x^5+x^4+x^3+x^2+x+1) = x^9+ x^5+ x^4+ x^2+x+1$
*à quoi on ajoute (retranche) x*m(x) il reste donc seulement 1*
{19}{3F}=01*

4) Effectuer la division polynômiale de m(x) par x^4+x^3+1

Réponse : Il suffit de poser pour trouver que le quotient vaut $x^4+x^3+ x^2+x+1$ et le reste $x^3+ x^2$ soit m={01}{1B} = {19}{1F}+{0C}*

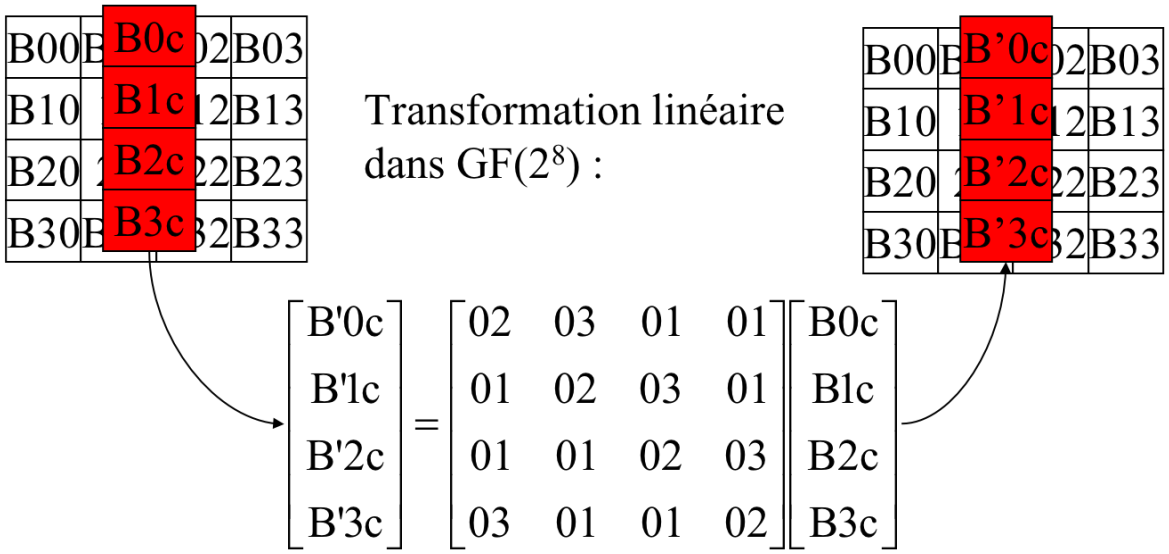
5) La division précédente est la première étape d'un algorithme d'Euclide qui amènera à trouver le pgcd de {01}{1B} et de {19}, dont on sait qu'il vaudra 1 puisque le polynôme {01}{1B} a été choisi irréductible. Mais en remontant les coefficients de Bezout (Algorithme d'Euclide étendu), on trouve l'inverse modulo m(x) de {19} donc l'inverse de {19} dans notre corps fini F(2^8). Effectuer ces calculs.

Réponse : les divisions suivantes sont $x^4+x^3+1 = (x^3+x^2)*x+1$ soit {19}={0C}{02}+{01} d'où {19}+{02}*[m+{19}*(1F}]={01} (rappel : nous sommes dans le monde merveilleux où la faute de signe n'existe pas). Soit {19}*[{01}+{02}*{1F}]={01}[m] reste à calculer donc {02}*{1F}=x*($x^4+x^3+x^2+x+1$)={3E} l'inverse de {19} est donc {3F} comme vérifié plus haut.*

6) Dans F(2^8), {03} = x+1 est un générateur du groupe multiplicatif F(2^8)* . On donne en annexe la table des puissances de ce générateur et la table de logarithme correspondante. Première table : l'exposant (élément de Z/255Z) est donné en décimal (premier chiffre sur la ligne, second chiffre sur la colonne), la puissance est dans la case correspondante (en Hexa mais désigne un élément de F(2^8) soit l'équivalent sous forme d'octet de l'expression polynomiale de cet élément). Vérifier les premières valeurs de cette table des puissances.
Seconde table les deux chiffres ligne colonne (LC) donnent un élément de F(2^8) en Hexa, et dans la case correspondante, le logarithme en décimal. En se servant de ces tables, refaire les calculs des questions précédentes (rappel les logarithmes s'additionnent donc modulo 255).

Réponse : $\log_{\{03\}}(\{19\})=113$, $\log_{\{03\}}(\{3F\})=142$ la somme des logarithmes vaut donc 255 et le produit vaut donc bien {01}

7) La troisième opération de l'algorithme AES est une opération linéaire sur les colonnes du tableau de 4*4 octets (128 bits) qui représente un bloc de message.



Cette opération est donc représentée par la matrice précédente (où les règles des produits matriciels sont les même que celles dont vous avez l'habitude étant entendu que les produits des éléments de matrice par les éléments du vecteur colonne sont des produits dans F(2^8))
Montrer que cette même opération peut être décrite en interprétant chaque colonne comme un polynôme à coefficients dans F(2^8) : la colonne c donnant : $B3c.x^3+B2c.x^2+B1c.x+B0c$ et en effectuant le produit modulo x^4+1 (qu'il serait d'ailleurs plus correct de noter {01}.x^4+{01}) de ce polynôme par le polynôme {03}.x^3+{01}.x^2+{01}.x+{02} (le résultat donnant le polynôme équivalent à la colonne mixée).

Solution : Le terme de degré 0 du résultat (donnant donc B'0c) est la somme des termes de degré 0 et de degré 4 du produit (car le modulo x^4+1 d'un terme en $A.x^4$ donne A où A est un

élément de $F(2^8)$: ajouter $A.(x^4+1)$ pour s'en convaincre). Il suffit donc de lire
*B'0c={02}*B0c+{03}*B1c+{01}*B2c+{01}*B3c*
Le terme de degré 1 du résultat est de même la somme des termes de degré 1 et de degré 5 d'où
*B'1c= {01}*B0c+{02}*B1c+{03}*B2c+{01}*B3c*
Le terme de degré 2 est la somme des termes de degrés 2 et 6
*B'2c={01}*B0c+{01}*B1c+{02}*B2c+{03}*B3c*
Le terme de degré 3 est la somme des termes de degrés 3
*B'3c={03}*B0c+{01}*B1c+{01}*B2c+{02}*B3c*
(Autre argument : constater qu'à chaque fois cela équivaut à un shift latéral à gauche).

8) Montrer que l'inverse modulo $\{01\}.x^4+\{01\}$ de $\{03\}.x^3+\{01\}.x^2+\{01\}.x+\{02\}$ existe (ce qui n'était pas évident car en fait $\{01\}.x^4+\{01\}$ n'est pas irréductible dans l'anneau des polynômes $F(2^8)[x]$) et vaut $\{0B\}.x^3+\{0D\}.x^2+\{09\}.x+\{0E\}$

Solution : Pas facile : il faut utiliser $\log_{\{03\}}(\{02\})=25$ et $\log_{\{03\}}(\{03\})=1$ pour calculer grâce à $\log_{\{03\}}(\{0E\})=223$ et $\log_{\{03\}}(\{09\})=199$
{02}{0E} : somme des logs 248 (F8) donc produit {1C}*
{03}{09} : somme des logs 200 (C8) donc produit {1B}*
Par conséquent le terme d'ordre 0 du produit (modulo $\{01\}.x^4+\{01\}$) vaut
{1C}+{1B}+{0D}+{0B} (rappel, l'addition représente le xor bit à bit), dont on voit immédiatement (en xor bit à bit 1+1=B+B=0, C+D=1) que cela donne bien {01}
Suite : faire pareil sur les autres lignes…