Calcul du produit de deux mots en AES

Soit à calculer le produit des mots **P=`{03}{01}{01}{02}`** et **Q = `{0b}{0d}{09}{0e}`**

Rappels d'algèbre

Un octet en AES représente un élément du corps à 256 éléments K défini comme le quotient de l'algèbre des polynômes sur le corps à deux éléments, notée Z/2Z[X], quotientée par l'idéal engendré par le polynôme de degré 8 défini par $m[X] = X^8 + X^4 + X^3 + X + 1$ >.

Un élément de Z/2Z[X] peut se représenter comme une suite de bits (poids forts à gauche).
Notamment m[X] (par définition congru à 0) peut s'écrire `1 0001 1011`, ou en abrégé `{01}{1b}`.

Arithmétique dans K

- L'addition dans K est le XOR bit à bit, noté ⊕ .
- La multiplication dans K, notée • est la multiplication de polynômes dans Z/2Z[X] , suivie d'une réduction modulo <m>
- L'élément neutre de ⊕ est `{00}` (polynôme nul)
- L'élément neutre de • est `{01}` (polynôme constant 1}
- La multiplication par X (soit `0000 0010 = {02}`) est un décalage de bits de 1 cran vers la gauche, suivi si nécessaire d'une réduction modulo `{01}{1b}`.
- La multiplication par X^2 (soit `0000 0100 = {04}`) est un décalage de bits de 2 crans vers la gauche, suivi si nécessaire d'une réduction modulo `{01}{1b}`.
- La multiplication par X^3 (soit `0000 1000 = {08}`) est un décalage de bits de 3 crans vers la gauche, suivi si nécessaire d'une réduction modulo `{01}{1b}`.
- etc. etc.

Un mot de 4 octets en AES représente un élément de l'anneau K[X] des polynômes sur K, quotienté par l'idéal engendré par le polynôme X^4+1 .

Etape 1 : Multiplication de P et Q dans K[X]

[`{03}`X^3 + `{01}`X^2 + `{01}`X + `{02}` **]** **×** **[** `{0b}`X^3 + `{0d}`X^2 + `{09}`X + `{0e}` **]**

Terme constant	`{02}•{0e}`						
Terme en X	`{01}•{0e}`	⊕	`{02}•{09}`				
Terme en X^2	`{01}•{0e}`	⊕	`{01}•{09}`	⊕	`{02}•{0d}`		
Terme en X^3	`{03}•{0e}`	⊕	`{01}•{09}`	⊕	`{01}•{0d}`	⊕	`{02}•{0b}`
Terme en X^4			`{03}•{09}`	⊕	`{01}•{0d}`	⊕	`{01}•{0b}`
Terme en X^5					`{03}•{0d}`	⊕	`{01}•{0b}`
Terme en X^6							`{03}•{0b}`

Calculs intermédiaires

Multiplications par `{01}`

`{01}` est l'élément neutre de • . Donc on a toujours `{01}•{xx} = {xx}`

Multiplications par `{02}`

Multiplication par X donc décalage d'un cran vers la gauche

`{02}•{0e} = {02}• 0000 1110 = 0001 1100 = {1c}`
`{02}•{09} = {02}• 0000 1001 = 0001 0010 = {12}`
`{02}•{0d} = {02}• 0000 1101 = 0001 1010 = {1a}`
`{02}•{0b} = {02}• 0000 1011 = 0001 0110 = {16}`

Multiplications par `{03}`

On utilise la relation `{03}={02}⊕{01}`, donc `{03}•{xx} = {02}•{xx} ⊕ {xx}`

`{03}•{0e} = {1c}⊕{0e} = 0001 1100 ⊕ 0000 1110 = 0001 0010 = {12}`
`{03}•{09} = {12}⊕{09} = 0001 0010 ⊕ 0000 1001 = 0001 1011 = {1b}`
`{03}•{0d} = {1a}⊕{0d} = 0001 1010 ⊕ 0000 1101 = 0001 0111 = {17}`
`{03}•{0b} = {16}⊕{0b} = 0001 0110 ⊕ 0000 1011 = 0001 1101 = {1d}`

En reportant dans le produit des polynômes puis en effectuant les XOR bit à bit :

Terme constant **{1c}**

Terme en X `{0e}⊕{12} = 0000 1110 ⊕ 0001 0010 = 0001 1100 =` **{1c}**

Terme en X^2 `{0e}⊕{09}⊕{1a} = 0000 1110 ⊕ 0000 1001 ⊕ 0001 1010`
`= 0001 1101 =` **{1d}**

Terme en X^3 `{12}⊕{09}⊕{0d}⊕{16}`
`= 0001 0010 ⊕ 0000 1001 ⊕ 0000 1101 ⊕ 0001 0110`
`= 0000 0000 =` **{00}**

Terme en X^4 `{1b}⊕{0d}⊕{0b} =` **{1d}**

Immédiat car `{1b}⊕{0b}={10}`

Terme en X^5 `{17}⊕{0b} = 0001 0111 ⊕ 0000 1011 = 0001 1100 =` **{1c}**

Terme en X^6 **{1d}**

Donc au final **[** $\{03\}X^3+\{01\}X^2+\{01\}X+\{02\}$ **]** **×** **[** $\{0b\}X^3+\{0d\}X^2+\{09\}X+\{0e\}$ **]**

= **[** $\{1d\}X^6+\{1c\}X^5+\{1d\}X^4+\{00\}X^3+\{1d\}X^2+\{1c\}X+\{1c\}$ **]**

Etape 2 : Réduction modulo X^4+1

On remarque que **[** $\{1d\}X^6+\{1c\}X^5+\{1d\}X^2+\{1c\}X$ **]** **=** **[** X^4+1 **]** **×** **[** $\{1d\}X^2+\{1c\}X$ **]**

Donc les termes de degré 6,5,2,1 s'éliminent mutuellement. Il reste $\{1d\}X^4 + \{1c\}$

En y ajoutant $\{1d\}(X^4+1)$ il reste $\{1d\}\oplus\{1d\}X^4 + \{1c\}\oplus\{1d\}$.

Avec `{1d}⊕{1d}={00}` et `{1c}⊕{1d}=0001 1100 ⊕ 0001 1101 = 0000 0001` , il reste

[$\{03\}X^3+\{01\}X^2+\{01\}X+\{02\}$ **]** **×** **[** $\{0b\}X^3+\{0d\}X^2+\{09\}X+\{0e\}$ **]** **= 1.**

Donc :

`[{03}{01}{01}{02}]×[{0b}{0d}{09}{0e}] = [{00}{00}{00}{01}]`