El cos finit $GF(2^8)$

Els elements d'aquest cos són els **bytes**. Els expressaren en forma binària, hexadecimal o polinòmica, segons convingui.

El byte $\mathtt{b_7b_6b_5b_4b_3b_2b_1b_0}$ serà el polinomi $b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$.

Per exemple, `01010111=0x57` serà $x^6 + x^4 + x^2 + x + 1$.

Suma

La suma de dos elements del cos és la suma de polinomis binaris. Per exemple, `01010111+10000011` serà

$$(x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) = x^7 + x^6 + x^4 + x^2 = \mathtt{11010100}$$

Es correspon amb la operació XOR, que es denotarà $\oplus$. L'element neutre de la suma és `00000000=0x00`.

Multiplicació

Per fer el producte de dos elements del cos cal fer el producte de polinomis binaris i després prendre el residu de la divisió per $\mathbf{m = x^8 + x^4 + x^3 + x + 1}$. Per exemple,

$$\begin{aligned}(x^6 + x^4 + x^2 + x + 1)(x^7 + x + 1) &= x^{13} + x^{11} + x^9 + x^8 + x^7 + \\ &\quad x^7 + x^5 + x^3 + x^2 + x + \\ &\quad x^6 + x^4 + x^2 + x + 1 \\ &= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1\end{aligned}$$

$$x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \pmod{x^8 + x^4 + x^3 + x + 1} = x^7 + x^6 + 1.$$

L'element neutre de la multiplicació és `00000001=0x01`.

A $GF(2^8)$, tot element diferent del `0x00`, té invers multiplicatiu. L'invers del polinomi a és l'únic polinomi b tal que

$$a\,b = 1 \mod m.$$

Es pot calcular usant l'algorisme d'Euclides estès.

També podem escriure els elements diferents del `0x00` com a potència d'un generador. Per exemple, si $g = x + 1 = \mathtt{00000011} = \mathtt{0x03}$, llavors

$$GF(2^8) = \{g, g^2, \ldots, g^{254}, g^{255}(= g^0 = 1)\} \cup \{0\}$$

El producte de dos elements $a = g^i$ i $b = g^j$, diferents de `0x00`, és $ab = g^i g^j = g^{i+j}$, i l'invers de a és $a^{-1} = (g^i)^{-1} = g^{-i} = g^{255-i}$. En aquest cas, la multiplicació i el càlcul de l'invers es redueixen a la cerca en una taula de 255 elements.

Entrega

1. Definiu les següents funcions:

   `GF_product_p`(byte `a`, byte `b`)

   entrada: `a` i `b` són bytes que representen elements del cos;
   sortida: un byte que és el producte en el cos de `a` i `b` fent servir la definició en termes de polinomis.

   `GF_tables`()

   entrada:
   sortida: dues taules (*exponencial* i *logaritme*), una que a la posició i tingui $a = g^i$ ($g =$ `0x03`) i una altra que a la posició a tingui i tal que $a = g^i$.

   `GF_product_t`(byte `a`, byte `b`)

   entrada: `a` i `b` són bytes que representen elements del cos;
   sortida: un byte que és el producte en el cos de `a` i `b` fent servir la les taules *exponencial* i *logaritme*.

   `GF_product_p_02`(byte `a`)

   entrada: `a` byte que representa un element del cos;
   sortida: un byte que és el producte optimitzat en el cos de `a` i `0x02` fent servir la definició en termes de polinomis.

   `GF_product_t_02`(byte `a`)

   entrada: `a` byte que representa un element del cos;
   sortida: un byte que és el producte optimitzat en el cos de `a` i `0x02` fent servir la les taules *exponencial* i *logaritme*.

   `GF_product_p_03`(byte `a`), `GF_product_t_03`(byte `a`)
   `GF_product_p_09`(byte `a`), `GF_product_t_09`(byte `a`)
   `GF_product_p_0B`(byte `a`), `GF_product_t_0B`(byte `a`)
   `GF_product_p_0D`(byte `a`), `GF_product_t_0D`(byte `a`)
   `GF_product_p_0E`(byte `a`), `GF_product_t_0E`(byte `a`)
   definides de manera anàloga.

2. Feu taules comparatives dels temps d'execució fent servir les diferents funcions:

   - `GF_product_p` *vs* `GF_product_t`, `GF_product_p_02` *vs* `GF_product_t_02`, `GF_product_p_03` *vs* `GF_product_t_03`...
   - `GF_product_p(a,0x02)` *vs* `GF_product_p_02(a)`, `GF_product_p(a,0x03)` *vs* `GF_product_p_03(a)`...
   - `GF_product_t(a,0x02)` *vs* `GF_product_t_02(a)`, `GF_product_t(a,0x03)` *vs* `GF_product_t_03(a)`...

3. Definiu una funció `GF_generador()` que doni tots el generadors del cos finit.
4. Definiu

   `GF_invers`(byte `a`)

   entrada: `a` byte que representa un element del cos;
   sortida: `0x00` si `a=0x00`, invers d'`a` en el cos si `a!=0x00`.

Referències

Federal Information Processing Standards Publication 197: ADVANCED ENCRYPTION STANDARD (AES)