

ejer1.pdf



Albadic



Teoría de números y criptografía



4º Grado en Matemáticas



Facultad de Ciencias
Universidad de Granada

Ejercicio 1

Consideremos el cifrado por bloques MiniAES descrito en el ejercicio 2.1.

- 1. Calcula $E_{dni}(0x01234567)$ usando el modo CBC e IV = 0x0001.
- 2. Calcula $E_{dni}(0x01234567)$ usando el modo CFB, r=11, y vector de inicialización IV = 0x0001

Apartado 1

El modo CFB nos dice:

 $c_{[0]} \in \mathbb{B}^N$. En este caso $c_{[0]} = IV$.

Dividimos el mensaje por bloques $m = m_{[1]} \cdot m_{[2]} \cdots m_{[l]}$ con $m_{[i]} \in \mathbb{B}^r$.

for i = 1, ..., l do

 $c_{[i]} = E_k(m_{[i]} \oplus c_{[i-1]})$

return $c_{[0]} \cdots c_{[l]}$ Como $c_{[0]} = IV = 0x0001 = 0000\,0000\,0000\,0001\,in\,\mathbb{B}^16$

A continuación dividimos el mensaje en bloques de 16 dígitos.

$$m = 0x01234567 = \overbrace{0000000100100011}^{m_1} \overbrace{0100010100111}^{m_2}$$

Por tanto obtenemos que l=3 dni mód 65536=51644 que en binario sería 11001001101111100, que tiene 16 dígitos.

Entonces k = 11001001101111100

A continuación realizaremos el método Mini AES. k = 0xC9BC

$$w_0 = k_0 = C = 12 = 1100 = \alpha^3 + \alpha^2$$

$$w_1 = k_1 = 9 = 1001 = \alpha^3 + 1$$

$$w_2 = k_2 = B = 11 = 1011 = \alpha^3 + \alpha + 1$$

$$w_3 = k_3 = C = 12 = 1100 = \alpha^3 + \alpha^2$$

$$w_4 = w_0 + \gamma(w_3) + 0001 = (\alpha^3 + \alpha^2) + (\alpha^3 + 1) + 1 = \alpha^2 = 0100$$

$$w_5 = w_1 + w_4 = \alpha^3 + \alpha^2 + 1 = 1101$$

$$w_6 = w_5 + w_1 = \alpha^3 + \alpha^2 + 1\alpha^3 + 1 = \alpha^2 = 0100$$

$$w_{7} - w_{9} + w_{9} - \alpha^{2} + \alpha^{3} + \alpha^{2} - \alpha^{3} - 1000$$

$$w_7 = w_6 + w_3 = \alpha^2 + \alpha^3 + \alpha^2 = \alpha^3 = 1000$$

$$w_8 = w_4 + \gamma(w_7) + 0010 = \alpha^2 + \alpha^3 + \alpha^2 + \alpha = \alpha^3 + \alpha = 1010$$

$$w_9 = w_5 + w_8 = \alpha^3 + \alpha^2 + 1\alpha^3 + \alpha = \alpha^2 + \alpha + 1 = 0111$$

$$w_{10} = w_6 + w_9 = \alpha^2 + \alpha^2 + \alpha + 1 = \alpha + 1 = 0011$$

$$w_{11} = w_7 + w_{10} = \alpha^3 + \alpha + 1 = 1011$$

Para calcular $c_{[1]}$ haremos $E_k(m_{[1]} \oplus c_{[0]}) = E_k(00000001001100011 \oplus 0000000000000000) =$ $E_k(0000000100100010)$

Aplicamos
$$\sigma_k$$

$$\sigma_{k_0} \left(\begin{array}{ccc} 0000 & 0010 \\ 0001 & 0010 \end{array} \right) = \left(\begin{array}{ccc} 0000 & 0010 \\ 0001 & 0010 \end{array} \right) + \left(\begin{array}{ccc} 1100 & 1011 \\ 1001 & 1100 \end{array} \right) = \left(\begin{array}{ccc} 1100 & 1001 \\ 1000 & 1110 \end{array} \right)$$

Aplicamos γ .

$$\gamma \left(\begin{array}{cc} 1100 & 1001 \\ 1000 & 1110 \end{array} \right) = \left(\begin{array}{cc} 1001 & 1110 \\ 1100 & 0101 \end{array} \right)$$

$$\pi \left(\begin{array}{cc} 1001 & 1110 \\ 1100 & 0101 \end{array} \right) = \left(\begin{array}{cc} 1001 & 1110 \\ 0101 & 1100 \end{array} \right)$$

Aplicamos θ .

$$\theta \begin{pmatrix} \alpha^3 + 1 & \alpha^3 + \alpha^2 + \alpha \\ \alpha^2 + 1 & \alpha^3 + \alpha^2 \end{pmatrix} = \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha & \alpha + 1 \end{pmatrix} * \begin{pmatrix} \alpha^3 + 1 & \alpha^3 + \alpha^2 + \alpha \\ \alpha^2 + 1 & \alpha^3 + \alpha^2 \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha & \alpha + 1 \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha^2 + 1 & \alpha^3 + \alpha^2 \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha & \alpha + 1 \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha^2 + 1 & \alpha^3 + \alpha^2 \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha & \alpha + 1 \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha^2 + 1 & \alpha^3 + \alpha^2 \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha & \alpha + 1 \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha^2 + 1 & \alpha^3 + \alpha^2 \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha & \alpha + 1 \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha^2 + 1 & \alpha^3 + \alpha^2 \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha^2 + 1 & \alpha^3 + \alpha^2 \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha + 1 & \alpha \end{pmatrix} = \theta \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha +$$

Reservados todos los derechos. No se permite la explotación económica ni la transformación de esta obra. Queda permitida la impresión en su totalidad.



$$\begin{pmatrix} \alpha^3 + \alpha^2 + \alpha & \alpha^3 + \alpha \\ \alpha^3 + \alpha^2 + \alpha & \alpha^3 \end{pmatrix} = \begin{pmatrix} 0010 & 1010 \\ 1110 & 1000 \end{pmatrix}$$
 Aplicamos σ_{k_1} .
$$\sigma_{k_1} \begin{pmatrix} 0010 & 1010 \\ 1110 & 1000 \end{pmatrix} = \begin{pmatrix} 0010 & 1010 \\ 1110 & 1000 \end{pmatrix} + \begin{pmatrix} 0100 & 0100 \\ 1101 & 1000 \end{pmatrix} = \begin{pmatrix} 0111 & 1110 \\ 0011 & 0000 \end{pmatrix}$$
 Aplicamos τ_{k_1} .
$$\gamma \begin{pmatrix} 0110 & 1110 \\ 0011 & 0000 \end{pmatrix} = \begin{pmatrix} 1011 & 0101 \\ 0011 & 0011 \end{pmatrix}$$
 Aplicamos π_{k_2} .
$$\pi \begin{pmatrix} 1011 & 0101 \\ 0011 & 0111 \end{pmatrix} = \begin{pmatrix} 1011 & 0101 \\ 0011 & 0111 \end{pmatrix} + \begin{pmatrix} 1010 & 0011 \\ 0111 & 1011 \end{pmatrix} = \begin{pmatrix} 0001 & 0110 \\ 0100 & 1100 \end{pmatrix}$$
 Por tanto $c_{11} = E_k(000000010010001) = 000101000110100$. Calculemos abora $c_{22} = E_k(m_{[2]}\oplus c_{[1]}) = E_k(01000010110011) + \begin{pmatrix} 1100 & 1011 \\ 1001 & 1100 \end{pmatrix} = \begin{pmatrix} 1001 & 1001 \\ 0001 & 1011 \end{pmatrix} + \begin{pmatrix} 1100 & 1011 \\ 1001 & 1100 \end{pmatrix} = \begin{pmatrix} 1001 & 1011 \\ 1000 & 0111 \end{pmatrix}$ Aplicamos σ_{k_0}
$$\sigma_{k_0} \begin{pmatrix} 0101 & 0000 \\ 0001 & 1011 \end{pmatrix} = \begin{pmatrix} 0110 & 0000 \\ 0001 & 1011 \end{pmatrix} + \begin{pmatrix} 1110 & 0110 \\ 1000 & 0111 \end{pmatrix} = \begin{pmatrix} 1110 & 0110 \\ 1000 & 0111 \end{pmatrix}$$
 Aplicamos τ_{k_0}
$$\pi \begin{pmatrix} 1110 & 0110 \\ 1000 & 0001 \end{pmatrix} = \begin{pmatrix} 1110 & 0110 \\ 0000 & 1100 \end{pmatrix}$$
 Aplicamos θ_{k_0}
$$\theta \begin{pmatrix} \alpha^3 + \alpha^2 + \alpha & \alpha^2 + \alpha \\ 0 & \alpha^3 + \alpha^2 \end{pmatrix} = \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha & \alpha + 1 \end{pmatrix} * \begin{pmatrix} \alpha^3 + \alpha^2 + \alpha & \alpha^2 + \alpha \\ 0 & \alpha^3 + \alpha^2 \end{pmatrix} = \begin{pmatrix} \alpha^3 + \alpha^2 + \alpha + \alpha & \alpha^2 + \alpha \\ 0 & \alpha^3 + \alpha^2 + \alpha \end{pmatrix} = \begin{pmatrix} 110 & 0101 \\ 0000 & 1101 \end{pmatrix} + \begin{pmatrix} 0101 & 0001 \\ 1101 & 1010 \end{pmatrix} + \begin{pmatrix} 0101 & 0001 \\ 1111 & 1111 \end{pmatrix}$$
 Aplicamos σ_{k_0} .
$$\sigma_{k_1} \begin{pmatrix} 0001 & 0001 \\ 0010 & 0101 \end{pmatrix} = \begin{pmatrix} 0001 & 0001 \\ 1111 & 1111 \end{pmatrix} + \begin{pmatrix} 0100 & 0100 \\ 1101 & 1000 \end{pmatrix} = \begin{pmatrix} 0101 & 0101 \\ 0010 & 0111 \end{pmatrix}$$
 Aplicamos τ_{k_0} .
$$\sigma_{k_1} \begin{pmatrix} 0001 & 0101 \\ 0010 & 0111 \end{pmatrix} = \begin{pmatrix} 0010 & 0010 \\ 1111 & 1000 \end{pmatrix} + \begin{pmatrix} 0101 & 0101 \\ 1111 & 1000 \end{pmatrix} = \begin{pmatrix} 0101 & 0101 \\ 0010 & 0111 \end{pmatrix}$$
 Aplicamos τ_{k_0} .
$$\sigma_{k_1} \begin{pmatrix} 0001 & 0101 \\ 1111 & 1000 \end{pmatrix} = \begin{pmatrix} 0010 & 0010 \\ 0010 & 0111 \end{pmatrix} + \begin{pmatrix} 0101 & 0001 \\ 1111 & 1000 \end{pmatrix} = \begin{pmatrix} 0101 & 0001 \\ 0010 & 0111 \end{pmatrix}$$
 Aplicamos τ_{k_0} .
$$\sigma_{k_0} \begin{pmatrix} 0001 & 0010 \\ 0010 & 0111 \end{pmatrix} = \begin{pmatrix} 0010 & 0010 \\ 0000 & 1111 \end{pmatrix} + \begin{pmatrix} 0101 & 0001 \\ 0010 & 0111 \end{pmatrix} = \begin{pmatrix} 0101 & 0000 \\ 0010 & 0111 \end{pmatrix}$$
 Aplicamos τ_{k_0} .
$$\sigma_{k_0} \begin{pmatrix} 0001 & 0010 \\ 0001 & 0111 \end{pmatrix} = \begin{pmatrix} 0001 & 0010 \\ 0001 & 0111 \end{pmatrix} + \begin{pmatrix} 0001 & 0011 \\ 0010 & 0111 \end{pmatrix} =$$

Apartado 2

Para r=11 el modo CFB nos dice: $x_{[1]} \in \mathbb{B}^N$. En este caso $x_{[1]} = IV$.



Dividimos el mensaje por bloques $m = m_{[1]} \cdot m_{[2]} \cdots m_{[l]}$ con $m_{[i]} \in \mathbb{B}^r$.

for i = 1, ..., l do

 $m_{[i]} = c_{[i]} \oplus msb_{11}(E_k(x_{[i]}))$

 $x_{[i+1]} = lsb_{N-r}(x_{[i]})||c_{[i]}|$

return $m_{[1]} \cdots m_{[l]}$

Aplicamos γ .

Como
$$x_{[1]} = \stackrel{[1]}{IV} = 0x0001 = 0000\ 0000\ 0000\ 0001 \in \mathbb{B}^{16} \Longrightarrow N = 16 \Longrightarrow N - r = 16 - 11 = 5$$

Vemos que 0x01234567 tiene 32 dígitos, por tanto añadimos al final un 1 para que sean 33 y sea divisible por 11. Entonces:

$$m = 0x01234567 = \overbrace{0000\ 0001\ 001}^{m1} \underbrace{00011010001}_{00011010001} \underbrace{01011001111}_{01011111}$$

Por tanto obtenemos que $l=3\ dni\$ mód 65536 = 51644 que en binario sería 1100100110111100, que tiene 16 dígitos.

Entonces k = 11001001101111100

A continuación realizaremos el método Mini AES.

$$k = 0xC9BC$$

$$w_0 = k_0 = C = 12 = 1100 = \alpha^3 + \alpha^2$$

$$w_1 = k_1 = 9 = 1001 = \alpha^3 + 1$$

$$w_2 = k_2 = B = 11 = 1011 = \alpha^3 + \alpha + 1$$

$$w_3 = k_3 = C = 12 = 1100 = \alpha^3 + \alpha^2$$

$$w_4 = w_0 + \gamma(w_3) + 0001 = (\alpha^3 + \alpha^2) + (\alpha^3 + 1) + 1 = \alpha^2 = 0100$$

$$w_5 = w_1 + w_4 = \alpha^3 + \alpha^2 + 1 = 1101$$

$$w_6 = w_5 + w_1 = \alpha^3 + \alpha^2 + 1\alpha^3 + 1 = \alpha^2 = 0100$$

$$w_7 = w_6 + w_3 = \alpha^2 + \alpha^3 + \alpha^2 = \alpha^3 = 1000$$

$$w_8 = w_4 + \gamma(w_7) + 0010 = \alpha^2 + \alpha^3 + \alpha^2 + \alpha = \alpha^3 + \alpha = 1010$$

$$w_9 = w_5 + w_8 = \alpha^3 + \alpha^2 + 1\alpha^3 + \alpha = \alpha^2 + \alpha + 1 = 0111$$

$$w_{10} = w_6 + w_9 = \alpha^2 + \alpha^2 + \alpha + 1 = \alpha + 1 = 0011$$

$$w_{11} = w_7 + w_{10} = \alpha^3 + \alpha + 1 = 1011$$
Aplicamos σ_{k_0}

$$0000 \quad 0000$$

$$\sigma_{k_0} \left(\begin{array}{c} 0000 \quad 0000 \\ 0000 \quad 0001 \end{array} \right) = \left(\begin{array}{c} 0000 \quad 0000 \\ 1110 \quad 1101 \end{array} \right) + \left(\begin{array}{c} 1100 \quad 1011 \\ 1001 \quad 1100 \end{array} \right) = \left(\begin{array}{c} 1100 \quad 1011 \\ 1001 \quad 1101 \end{array} \right)$$
Aplicamos π .
$$\pi \left(\begin{array}{c} 1001 \quad 0110 \\ 1101 \quad 1101 \end{array} \right) = \left(\begin{array}{c} 1001 \quad 0110 \\ 1101 \quad 1110 \end{array} \right)$$
Aplicamos π .
$$\pi \left(\begin{array}{c} 0010 \quad 0110 \\ 1110 \quad 1011 \\ 1001 \quad 1101 \end{array} \right) = \left(\begin{array}{c} 1001 \quad 0110 \\ 1101 \quad 1110 \right)$$
Aplicamos θ .
$$\theta \left(\begin{array}{c} \alpha^3 + 1 \quad \alpha^2 + \alpha \\ \alpha^3 + \alpha^2 + 1 \quad \alpha^3 + \alpha^2 + \alpha \end{array} \right) = \left(\begin{array}{c} \alpha + 1 \quad \alpha \\ \alpha \quad \alpha + 1 \end{array} \right) * \left(\begin{array}{c} \alpha^3 + 1 \quad \alpha^2 + \alpha \\ \alpha^3 + \alpha^2 + 1 \quad \alpha^3 + \alpha^2 + \alpha \end{array} \right) = \left(\begin{array}{c} \alpha^4 + \alpha + \alpha^3 + 1 + \alpha^4 + \alpha^3 + \alpha \quad \alpha^3 + \alpha^2 + \alpha^2 + \alpha^3 + \alpha^2 + \alpha^3 + \alpha^2 + \alpha \end{array} \right) = \left(\begin{array}{c} 1 \quad \alpha^2 + 1 \\ \alpha^4 + \alpha + \alpha^4 + \alpha^3 + \alpha + \alpha^3 + \alpha^2 + 1 \quad \alpha^3 + \alpha^2 + \alpha^3 + \alpha^2 + \alpha^3 + \alpha^2 + \alpha \right) = \left(\begin{array}{c} 1 \quad \alpha^2 + 1 \\ \alpha^4 + \alpha + \alpha^4 + \alpha^3 + \alpha + \alpha^3 + \alpha^2 + 1 \quad \alpha^3 + \alpha^2 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha^3 + \alpha^2 + \alpha \right) = \left(\begin{array}{c} 1 \quad \alpha^2 + 1 \\ \alpha^2 + 1 \quad \alpha^3 + \alpha^2 + 1 \end{array} \right) = \left(\begin{array}{c} 0001 \quad 0101 \\ 0101 \quad 1101 \end{array} \right)$$
Aplicamos σ_{k_1} .

$$\sigma_{k_1} \left(\begin{array}{c} 0001 \quad 0101 \\ 0101 \quad 1101 \end{array} \right) + \left(\begin{array}{c} 0100 \quad 0100 \\ 0101 \quad 1100 \end{array} \right) = \left(\begin{array}{c} 0101 \quad 0001 \\ 1000 \quad 0101 \end{array} \right)$$



```
\begin{pmatrix} 0101 & 0001 \\ 1000 & 0101 \end{pmatrix} = \begin{pmatrix} 0010 & 1000 \\ 1100 & 0010 \end{pmatrix}
Aplicamos \pi.
      \begin{pmatrix} 0010 & 1000 \\ 1100 & 0010 \end{pmatrix} = \begin{pmatrix} 0010 & 1000 \\ 0010 & 1100 \end{pmatrix}
\sigma_{k_2} \left( \begin{array}{ccc} 0010 & 1000 \\ 0010 & 1100 \end{array} \right) = \left( \begin{array}{ccc} 0010 & 1000 \\ 0010 & 1100 \end{array} \right) + \left( \begin{array}{ccc} 1010 & 0011 \\ 0111 & 1011 \end{array} \right) = \left( \begin{array}{ccc} 1000 & 1011 \\ 0101 & 0111 \end{array} \right)
Entonces tenemos que:
E_k(x_{[1]}) = 1000010110110111
msb_{11}(E_k(x_{[1]})) = 10000101101
c_{[1]} = m_{[1]} + \dot{1}0000101101 = 00000001001 + 10000101101 = 10000100100
Por otro lado también tenemos:
lsb_{N-r}(x_{[1]}) = lsb_{16-11}(x_{[1]}) = lsb_5(x_{[1]}) = 00001
Entonces tenemos que x_{[2]} = 0000110000100100, volvemos a hacer la iteración
para x_{[2]}
Aplicamos \sigma_{k_0}
\sigma_0 \left( \begin{array}{cc} 0000 & 0010 \\ 1100 & 0100 \end{array} \right) = \left( \begin{array}{cc} 0000 & 0010 \\ 1100 & 0100 \end{array} \right) + \left( \begin{array}{cc} 1100 & 1011 \\ 1001 & 1100 \end{array} \right) = \left( \begin{array}{cc} 1100 & 1001 \\ 0101 & 1000 \end{array} \right)
Aplicamos \gamma.

\gamma \begin{pmatrix} 1100 & 1001 \\ 0101 & 1000 \end{pmatrix} = \begin{pmatrix} 1001 & 1110 \\ 0010 & 1100 \end{pmatrix}

Aplicamos \pi.
     \left(\begin{array}{cc} 1001 & 1110 \\ 0010 & 1100 \end{array}\right) = \left(\begin{array}{cc} 1001 & 1110 \\ 1100 & 0010 \end{array}\right)
Aplicamos \theta.
0110 0101
    0000 1001
Aplicamos ahora \sigma_1
\sigma_{k_1} \left( \begin{array}{ccc} 0110 & 0101 \\ 0000 & 1001 \end{array} \right) = \left( \begin{array}{ccc} 0110 & 0101 \\ 0000 & 1001 \end{array} \right) + \left( \begin{array}{ccc} 0100 & 0100 \\ 1101 & 1000 \end{array} \right) = \left( \begin{array}{ccc} 0010 & 0001 \\ 1101 & 0001 \end{array} \right)
Aplicamos \gamma
     \left(\begin{array}{cc} 0010 & 0001 \\ 1101 & 0001 \end{array}\right) = \left(\begin{array}{cc} 1111 & 1000 \\ 1101 & 1000 \end{array}\right)
Aplicamos \pi.
\pi \left( \begin{array}{cc} 1111 & 1000 \\ 1101 & 1000 \end{array} \right) = \left( \begin{array}{cc} 1111 & 1000 \\ 1000 & 1101 \end{array} \right)
Aplicamos \sigma_{k_2}
\sigma_{k_2} \left( \begin{array}{ccc} 1111 & 1000 \\ 1000 & 1101 \end{array} \right) = \left( \begin{array}{ccc} 1111 & 1000 \\ 1000 & 1101 \end{array} \right) + \left( \begin{array}{ccc} 1010 & 0011 \\ 0111 & 1011 \end{array} \right) = \left( \begin{array}{ccc} 0101 & 1011 \\ 1111 & 0110 \end{array} \right)
Entonces tenemos que:
E_k(x_{[2]}) = 01011111110110110
msb_{11}(E_k(x_{[2]})) = 010111111101
c_{[2]} = m_{[2]} + 010111111101 = 00011010001 + 010111111101 = 01000101100
Por otro lado también tenemos:
lsb_{N-r}(x_{[2]}) = lsb_{16-11}(x_{[2]}) = lsb_5(x_{[2]}) = 00100
Entonces tenemos que x_{[3]} = 0010001000101100, y volvemos a hacer la iteración.
```



Aplicamos σ_{k_0}

```
\sigma_0 \left( \begin{array}{cc} 0010 & 0010 \\ 0010 & 1100 \end{array} \right) = \left( \begin{array}{cc} 0010 & 0010 \\ 0010 & 1100 \end{array} \right) + \left( \begin{array}{cc} 1100 & 1011 \\ 1001 & 1100 \end{array} \right) = \left( \begin{array}{cc} 1101 & 1001 \\ 1011 & 0000 \end{array} \right)
Aplicamos \gamma.
\gamma \left( \begin{array}{cc} 1101 & 1001 \\ 1011 & 0000 \end{array} \right) = \left( \begin{array}{cc} 1101 & 1110 \\ 0110 & 0011 \end{array} \right)
Aplicamos \pi.
      \left(\begin{array}{cc} 1101 & 1110 \\ 0110 & 0011 \end{array}\right) = \left(\begin{array}{cc} 1101 & 1110 \\ 0011 & 0110 \end{array}\right)
Aplicamos \theta.
     \begin{pmatrix} 1101 & 1110 \\ 0011 & 0110 \end{pmatrix} = \begin{pmatrix} \alpha+1 & \alpha \\ \alpha & \alpha+1 \end{pmatrix} * \begin{pmatrix} \alpha^3+\alpha^2+1 & \alpha^3+\alpha^2+\alpha \\ \alpha+1 & \alpha^2+\alpha \end{pmatrix} = \begin{pmatrix} \alpha & \alpha^3+\alpha^2+1 \\ \alpha^3+\alpha^2 & \alpha^2+1 \end{pmatrix} = \begin{pmatrix} 0010 & 1101 \\ 1100 & 0101 \end{pmatrix}
Aplicamos ahora \sigma_1
\sigma_{k_1} \left( \begin{array}{ccc} 0010 & 1101 \\ 1100 & 0101 \end{array} \right) = \left( \begin{array}{ccc} 0010 & 1101 \\ 1100 & 0101 \end{array} \right) + \left( \begin{array}{ccc} 0100 & 0100 \\ 1101 & 1000 \end{array} \right) = \left( \begin{array}{ccc} 0110 & 1001 \\ 0001 & 1101 \end{array} \right)
Aplicamos \gamma
      \left(\begin{array}{cc} 0110 & 1001 \\ 0001 & 1101 \end{array}\right) = \left(\begin{array}{cc} 1011 & 1110 \\ 1000 & 1101 \end{array}\right)
       \begin{pmatrix} 1011 & 1110 \\ 1000 & 1101 \end{pmatrix} = \begin{pmatrix} 1011 & 1110 \\ 1101 & 1000 \end{pmatrix} 
Aplicamos \sigma_{k_2}
\sigma_{k_2} \left( \begin{array}{ccc} 1011 & 1110 \\ 1101 & 1000 \end{array} \right) = \left( \begin{array}{ccc} 1011 & 1110 \\ 1101 & 1000 \end{array} \right) + \left( \begin{array}{ccc} 1010 & 0011 \\ 0111 & 1011 \end{array} \right) = \left( \begin{array}{ccc} 0001 & 1101 \\ 1010 & 0011 \end{array} \right)
         Entonces tenemos que:
E_k(x_{[3]}) = 0001101011010011
msb_{[3]}(E_k(x_{[3]})) = 00011010110
c_{[3]} = m_{[3]} + 00011010110 = 01011001111 + 00011010110 = 01000011001
Por tanto obtenemos finalmente que:
E_{dni}(0x01234567) = c = c_{[1]} \cdot c_{[2]} \cdot c_{[3]} = 100001001000100110001100011001
```

