ejer1.pdf

Albadlc

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.

$$m = 0x01234567 = \overbrace{0000000100100011}^{m_1}\overbrace{0100010101100111}^{m_2}$$

Por tanto obtenemos que $l = 3$ $dni \mod 65536 = 51644$ que en binario sería 1100100110111100, que tiene 16 dígitos.
Entonces $k = 1100100110111100$
A continuación realizaremos el método Mini AES. $k = 0xC9BC$
$w_0 = k_0 = C = 12 = 1100 = \alpha^3 + \alpha^2$
$w_1 = k_1 = 9 = 1001 = \alpha^3 + 1$
$w_2 = k_2 = B = 11 = 1011 = \alpha^3 + \alpha + 1$
$w_3 = k_3 = C = 12 = 1100 = \alpha^3 + \alpha^2$
$w_4 = w_0 + \gamma(w_3) + 0001 = (\alpha^3 + \alpha^2) + (\alpha^3 + 1) + 1 = \alpha^2 = 0100$
$w_5 = w_1 + w_4 = \alpha^3 + \alpha^2 + 1 = 1101$
$w_6 = w_5 + w_1 = \alpha^3 + \alpha^2 + 1\alpha^3 + 1 = \alpha^2 = 0100$
$w_7 = w_6 + w_3 = \alpha^2 + \alpha^3 + \alpha^2 = \alpha^3 = 1000$
$w_8 = w_4 + \gamma(w_7) + 0010 = \alpha^2 + \alpha^3 + \alpha^2 + \alpha = \alpha^3 + \alpha = 1010$
$w_9 = w_5 + w_8 = \alpha^3 + \alpha^2 + 1\alpha^3 + \alpha = \alpha^2 + \alpha + 1 = 0111$
$w_{10} = w_6 + w_9 = \alpha^2 + \alpha^2 + \alpha + 1 = \alpha + 1 = 0011$
$w_{11} = w_7 + w_{10} = \alpha^3 + \alpha + 1 = 1011$
Para calcular $c_{[1]}$ haremos $E_k(m_{[1]} \oplus c_{[0]}) = E_k(0000000100100011 \oplus 0000000000000001) = E_k(0000000100100010)$

Aplicamos σ_{k_0}
$\sigma_{k_0}\begin{pmatrix} 0000 & 0010 \\ 0001 & 0010 \end{pmatrix} = \begin{pmatrix} 0000 & 0010 \\ 0001 & 0010 \end{pmatrix} + \begin{pmatrix} 1100 & 1011 \\ 1001 & 1100 \end{pmatrix} = \begin{pmatrix} 1100 & 1001 \\ 1000 & 1110 \end{pmatrix}$
Aplicamos γ.
$\gamma\begin{pmatrix} 1100 & 1001 \\ 1000 & 1110 \end{pmatrix} = \begin{pmatrix} 1001 & 1110 \\ 1100 & 0101 \end{pmatrix}$
Aplicamos π.
$\pi\begin{pmatrix} 1001 & 1110 \\ 1100 & 0101 \end{pmatrix} = \begin{pmatrix} 1001 & 1110 \\ 0101 & 1100 \end{pmatrix}$
Aplicamos θ.
$\theta\begin{pmatrix} \alpha^3+1 & \alpha^3+\alpha^2+\alpha \\ \alpha^2+1 & \alpha^3+\alpha^2 \end{pmatrix} = \begin{pmatrix} \alpha+1 & \alpha \\ \alpha & \alpha+1 \end{pmatrix} * \begin{pmatrix} \alpha^3+1 & \alpha^3+\alpha^2+\alpha \\ \alpha^2+1 & \alpha^3+\alpha^2 \end{pmatrix} =$

$\begin{pmatrix} \alpha & \alpha^3+\alpha \\ \alpha^3+\alpha^2+\alpha & \alpha^3 \end{pmatrix} = \begin{pmatrix} 0010 & 1010 \\ 1110 & 1000 \end{pmatrix}$
Aplicamos σ_{k_1}.
$\sigma_{k_1}\begin{pmatrix} 0010 & 1010 \\ 1110 & 1000 \end{pmatrix} = \begin{pmatrix} 0010 & 1010 \\ 1110 & 1000 \end{pmatrix} + \begin{pmatrix} 0100 & 0100 \\ 1101 & 1000 \end{pmatrix} = \begin{pmatrix} 0110 & 1110 \\ 0011 & 0000 \end{pmatrix}$
Aplicamos γ.
$\gamma\begin{pmatrix} 0110 & 1110 \\ 0011 & 0000 \end{pmatrix} = \begin{pmatrix} 1011 & 0101 \\ 0111 & 0011 \end{pmatrix}$
Aplicamos π.
$\pi\begin{pmatrix} 1011 & 0101 \\ 0111 & 0011 \end{pmatrix} = \begin{pmatrix} 1011 & 0101 \\ 0011 & 0111 \end{pmatrix}$
Aplicamos σ_{k_2}.
$\sigma_{k_2}\begin{pmatrix} 1011 & 0101 \\ 0011 & 0111 \end{pmatrix} = \begin{pmatrix} 1011 & 0101 \\ 0011 & 0111 \end{pmatrix} + \begin{pmatrix} 1010 & 0011 \\ 0111 & 1011 \end{pmatrix} = \begin{pmatrix} 0001 & 0110 \\ 0100 & 1100 \end{pmatrix}$
Por tanto $c_{[1]} = E_k(0000000100100010) = 0001010001101100$. Calculemos ahora
$c_{[2]} = E_k(m_{[2]} \oplus c_{[1]}) = E_k(0100010101100111 \oplus 0001010001101100) = E_k(0101000100001011)$
Aplicamos σ_{k_0}
$\sigma_{k_0}\begin{pmatrix} 0101 & 0000 \\ 0001 & 1011 \end{pmatrix} = \begin{pmatrix} 0101 & 0000 \\ 0001 & 1011 \end{pmatrix} + \begin{pmatrix} 1100 & 1011 \\ 1001 & 1100 \end{pmatrix} = \begin{pmatrix} 1001 & 1011 \\ 1000 & 0111 \end{pmatrix}$
Aplicamos γ.
$\gamma\begin{pmatrix} 1001 & 1011 \\ 1000 & 0111 \end{pmatrix} = \begin{pmatrix} 1110 & 0110 \\ 1100 & 0000 \end{pmatrix}$
Aplicamos π.
$\pi\begin{pmatrix} 1110 & 0110 \\ 1100 & 0000 \end{pmatrix} = \begin{pmatrix} 1110 & 0110 \\ 0000 & 1100 \end{pmatrix}$
Aplicamos θ.
$\theta\begin{pmatrix} \alpha^3+\alpha^2+\alpha & \alpha^2+\alpha \\ 0 & \alpha^3+\alpha^2 \end{pmatrix} = \begin{pmatrix} \alpha+1 & \alpha \\ \alpha & \alpha+1 \end{pmatrix} * \begin{pmatrix} \alpha^3+\alpha^2+\alpha & \alpha^2+\alpha \\ 0 & \alpha^3+\alpha^2 \end{pmatrix} =$
$\begin{pmatrix} 1 & 1 \\ \alpha^3+\alpha^2+\alpha+1 & \alpha^3+\alpha^3+\alpha+1 \end{pmatrix} = \begin{pmatrix} 0001 & 0001 \\ 1111 & 1111 \end{pmatrix}$
Aplicamos σ_{k_1}.
$\sigma_{k_1}\begin{pmatrix} 0001 & 0001 \\ 1111 & 1111 \end{pmatrix} = \begin{pmatrix} 0001 & 0001 \\ 1111 & 1111 \end{pmatrix} + \begin{pmatrix} 0100 & 0100 \\ 1101 & 1000 \end{pmatrix} = \begin{pmatrix} 0101 & 0101 \\ 0010 & 0111 \end{pmatrix}$
Aplicamos γ.
$\gamma\begin{pmatrix} 0101 & 0101 \\ 0010 & 0111 \end{pmatrix} = \begin{pmatrix} 0010 & 0010 \\ 1111 & 0000 \end{pmatrix}$
Aplicamos π.
$\pi\begin{pmatrix} 0010 & 0010 \\ 1111 & 0000 \end{pmatrix} = \begin{pmatrix} 0010 & 0010 \\ 0000 & 1111 \end{pmatrix}$
Aplicamos σ_{k_2}.
$\sigma_{k_2}\begin{pmatrix} 0010 & 0010 \\ 0000 & 1111 \end{pmatrix} = \begin{pmatrix} 0010 & 0010 \\ 0000 & 1111 \end{pmatrix} + \begin{pmatrix} 1010 & 0011 \\ 0111 & 1011 \end{pmatrix} = \begin{pmatrix} 1000 & 0001 \\ 0111 & 0100 \end{pmatrix}$
Por tanto $c_{[2]} = E_k(0101000100001011) = 1000011100010100$.
Obtenemos por tanto que:

$$E_{dni}(0x01234567) = c = c_{[0]} \cdot c_{[1]} \cdot c_{[2]} = 000000000000000100010100011011001000011100010100$$

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

Como $x_{[1]} = IV = 0x0001 = 0000\,0000\,0000\,0001 \in \mathbb{B}^{16} \implies N = 16 \implies N - r = 16 - 11 = 5$
Vemos que $0x01234567$ tiene 32 dígitos, por tanto añadimos al final un 1 para que sean 33 y sea divisible por 11. Entonces:

$$m = 0x01234567 = \overbrace{0000\,0001\,001}^{m1}\overbrace{00011010001}^{m2}\overbrace{01011001111}^{m3}$$

Por tanto obtenemos que $l = 3$ $dni \mod 65536 = 51644$ que en binario sería 1100100110111100, que tiene 16 dígitos.
Entonces $k = 1100100110111100$
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}
$\sigma_{k_0}\begin{pmatrix} 0000 & 0000 \\ 0000 & 0001 \end{pmatrix} = \begin{pmatrix} 0000 & 0000 \\ 0000 & 0001 \end{pmatrix} + \begin{pmatrix} 1100 & 1011 \\ 1001 & 1100 \end{pmatrix} = \begin{pmatrix} 1100 & 1011 \\ 1001 & 1101 \end{pmatrix}$
Aplicamos γ.
$\gamma\begin{pmatrix} 1100 & 1011 \\ 1001 & 1101 \end{pmatrix} = \begin{pmatrix} 1001 & 0110 \\ 1110 & 1101 \end{pmatrix}$
Aplicamos π.
$\pi\begin{pmatrix} 1001 & 0110 \\ 1110 & 1101 \end{pmatrix} = \begin{pmatrix} 1001 & 0110 \\ 1101 & 1110 \end{pmatrix}$
Aplicamos θ.
$\theta\begin{pmatrix} \alpha^3 + 1 & \alpha^2 + \alpha \\ \alpha^3 + \alpha^2 + 1 & \alpha^3 + \alpha^2 + \alpha \end{pmatrix} = \begin{pmatrix} \alpha + 1 & \alpha \\ \alpha & \alpha + 1 \end{pmatrix} * \begin{pmatrix} \alpha^3 + 1 & \alpha^2 + \alpha \\ \alpha^3 + \alpha^2 + 1 & \alpha^3 + \alpha^2 + \alpha \end{pmatrix} =$
$\begin{pmatrix} \alpha^4 + \alpha + \alpha^3 + 1 + \alpha^4 + \alpha^3 + \alpha & \alpha^3 + \alpha^2 + \alpha^2 + \alpha + \alpha^4 + \alpha^3 + \alpha^2 \\ \alpha^4 + \alpha + \alpha^4 + \alpha^3 + \alpha + \alpha^3 + \alpha^2 + 1 & \alpha^3 + \alpha^2 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha^3 + \alpha^2 + \alpha \end{pmatrix} =$
$\begin{pmatrix} 1 & \alpha^2 + 1 \\ \alpha^2 + 1 & \alpha^3 + \alpha^2 + 1 \end{pmatrix} = \begin{pmatrix} 0001 & 0101 \\ 0101 & 1101 \end{pmatrix}$
Aplicamos σ_{k_1}.
$\sigma_{k_1}\begin{pmatrix} 0001 & 0101 \\ 0101 & 1101 \end{pmatrix} = \begin{pmatrix} 0001 & 0101 \\ 0101 & 1101 \end{pmatrix} + \begin{pmatrix} 0100 & 0100 \\ 1101 & 1000 \end{pmatrix} = \begin{pmatrix} 0101 & 0001 \\ 1000 & 0101 \end{pmatrix}$
Aplicamos γ.

$\gamma \begin{pmatrix} 0101 & 0001 \\ 1000 & 0101 \end{pmatrix} = \begin{pmatrix} 0010 & 1000 \\ 1100 & 0010 \end{pmatrix}$
Aplicamos π.
$\pi \begin{pmatrix} 0010 & 1000 \\ 1100 & 0010 \end{pmatrix} = \begin{pmatrix} 0010 & 1000 \\ 0010 & 1100 \end{pmatrix}$
Aplicamos σ_{k_2}.
$\sigma_{k_2} \begin{pmatrix} 0010 & 1000 \\ 0010 & 1100 \end{pmatrix} = \begin{pmatrix} 0010 & 1000 \\ 0010 & 1100 \end{pmatrix} + \begin{pmatrix} 1010 & 0011 \\ 0111 & 1011 \end{pmatrix} = \begin{pmatrix} 1000 & 1011 \\ 0101 & 0111 \end{pmatrix}$
Entonces tenemos que:
$E_k(x_{[1]}) = 1000010110110111$
$msb_{11}(E_k(x_{[1]})) = 10000101101$
$c_{[1]} = m_{[1]} + 10000101101 = 00000001001 + 10000101101 = 10000100100$
Por otro lado también tenemos:
$lsb_{N-r}(x_{[1]}) = lsb_{16-11}(x_{[1]}) = lsb_5(x_{[1]}) = 00001$
Entonces tenemos que $x_{[2]} = 0000110000100100$,y volvemos a hacer la iteración para $x_{[2]}$
Aplicamos σ_{k_0}
$\sigma_0 \begin{pmatrix} 0000 & 0010 \\ 1100 & 0100 \end{pmatrix} = \begin{pmatrix} 0000 & 0010 \\ 1100 & 0100 \end{pmatrix} + \begin{pmatrix} 1100 & 1011 \\ 1001 & 1100 \end{pmatrix} = \begin{pmatrix} 1100 & 1001 \\ 0101 & 1000 \end{pmatrix}$
Aplicamos γ.
$\gamma \begin{pmatrix} 1100 & 1001 \\ 0101 & 1000 \end{pmatrix} = \begin{pmatrix} 1001 & 1110 \\ 0010 & 1100 \end{pmatrix}$
Aplicamos π.
$\pi \begin{pmatrix} 1001 & 1110 \\ 0010 & 1100 \end{pmatrix} = \begin{pmatrix} 1001 & 1110 \\ 1100 & 0010 \end{pmatrix}$
Aplicamos θ.
$\theta \begin{pmatrix} 1001 & 1110 \\ 1100 & 0010 \end{pmatrix} = \begin{pmatrix} \alpha+1 & \alpha \\ \alpha & \alpha+1 \end{pmatrix} * \begin{pmatrix} \alpha^3+1 & \alpha^3+\alpha^2+\alpha \\ \alpha^3+\alpha^2 & \alpha \end{pmatrix} = \begin{pmatrix} \alpha^2+\alpha & \alpha^2+1 \\ 0 & \alpha^3+1 \end{pmatrix} =$
$\begin{pmatrix} 0110 & 0101 \\ 0000 & 1001 \end{pmatrix}$
Aplicamos ahora σ_1
$\sigma_{k_1} \begin{pmatrix} 0110 & 0101 \\ 0000 & 1001 \end{pmatrix} = \begin{pmatrix} 0110 & 0101 \\ 0000 & 1001 \end{pmatrix} + \begin{pmatrix} 0100 & 0100 \\ 1101 & 1000 \end{pmatrix} = \begin{pmatrix} 0010 & 0001 \\ 1101 & 0001 \end{pmatrix}$
Aplicamos γ
$\gamma \begin{pmatrix} 0010 & 0001 \\ 1101 & 0001 \end{pmatrix} = \begin{pmatrix} 1111 & 1000 \\ 1101 & 1000 \end{pmatrix}$
Aplicamos π.
$\pi \begin{pmatrix} 1111 & 1000 \\ 1101 & 1000 \end{pmatrix} = \begin{pmatrix} 1111 & 1000 \\ 1000 & 1101 \end{pmatrix}$
Aplicamos σ_{k_2}
$\sigma_{k_2} \begin{pmatrix} 1111 & 1000 \\ 1000 & 1101 \end{pmatrix} = \begin{pmatrix} 1111 & 1000 \\ 1000 & 1101 \end{pmatrix} + \begin{pmatrix} 1010 & 0011 \\ 0111 & 1011 \end{pmatrix} = \begin{pmatrix} 0101 & 1011 \\ 1111 & 0110 \end{pmatrix}$
Entonces tenemos que:
$E_k(x_{[2]}) = 0101111110110110$
$msb_{11}(E_k(x_{[2]})) = 01011111101$
$c_{[2]} = m_{[2]} + 01011111101 = 00011010001 + 01011111101 = 01000101100$
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}

$\sigma_0 \begin{pmatrix} 0010 & 0010 \\ 0010 & 1100 \end{pmatrix} = \begin{pmatrix} 0010 & 0010 \\ 0010 & 1100 \end{pmatrix} + \begin{pmatrix} 1100 & 1011 \\ 1001 & 1100 \end{pmatrix} = \begin{pmatrix} 1101 & 1001 \\ 1011 & 0000 \end{pmatrix}$
Aplicamos γ.
$\gamma \begin{pmatrix} 1101 & 1001 \\ 1011 & 0000 \end{pmatrix} = \begin{pmatrix} 1101 & 1110 \\ 0110 & 0011 \end{pmatrix}$
Aplicamos π.
$\pi \begin{pmatrix} 1101 & 1110 \\ 0110 & 0011 \end{pmatrix} = \begin{pmatrix} 1101 & 1110 \\ 0011 & 0110 \end{pmatrix}$
Aplicamos θ.
$\theta \begin{pmatrix} 1101 & 1110 \\ 0011 & 0110 \end{pmatrix} = \begin{pmatrix} \alpha+1 & \alpha \\ \alpha & \alpha+1 \end{pmatrix} * \begin{pmatrix} \alpha^3+\alpha^2+1 & \alpha^3+\alpha^2+\alpha \\ \alpha+1 & \alpha^2+\alpha \end{pmatrix} =$
$\begin{pmatrix} \alpha & \alpha^3+\alpha^2+1 \\ \alpha^3+\alpha^2 & \alpha^2+1 \end{pmatrix} = \begin{pmatrix} 0010 & 1101 \\ 1100 & 0101 \end{pmatrix}$
Aplicamos ahora σ_1
$\sigma_{k_1} \begin{pmatrix} 0010 & 1101 \\ 1100 & 0101 \end{pmatrix} = \begin{pmatrix} 0010 & 1101 \\ 1100 & 0101 \end{pmatrix} + \begin{pmatrix} 0100 & 0100 \\ 1101 & 1000 \end{pmatrix} = \begin{pmatrix} 0110 & 1001 \\ 0001 & 1101 \end{pmatrix}$
Aplicamos γ
$\gamma \begin{pmatrix} 0110 & 1001 \\ 0001 & 1101 \end{pmatrix} = \begin{pmatrix} 1011 & 1110 \\ 1000 & 1101 \end{pmatrix}$
Aplicamos π.
$\pi \begin{pmatrix} 1011 & 1110 \\ 1000 & 1101 \end{pmatrix} = \begin{pmatrix} 1011 & 1110 \\ 1101 & 1000 \end{pmatrix}$
Aplicamos σ_{k_2}
$\sigma_{k_2} \begin{pmatrix} 1011 & 1110 \\ 1101 & 1000 \end{pmatrix} = \begin{pmatrix} 1011 & 1110 \\ 1101 & 1000 \end{pmatrix} + \begin{pmatrix} 1010 & 0011 \\ 0111 & 1011 \end{pmatrix} = \begin{pmatrix} 0001 & 1101 \\ 1010 & 0011 \end{pmatrix}$

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:
$E_{dni}(0x01234567) = c = c_{[1]} \cdot c_{[2]} \cdot c_{[3]} = 100001001000100010110001000011001$