Ejercicio 1

David García Curbelo

Consideremos el cifrado por bloques miniAES descrito en el ejercicio 2.1.
Apartado I. ***Calcula*** $\boldsymbol{E_{dni}}(0x01234567)$ ***usando el modo*** CBC ***e*** $IV = 0x0001$**.**

Tenemos por dni el número 45352581, luego obtenemos la siguiente clave:

$$dni \equiv 1669 \pmod{65536} \quad \Rightarrow \quad clave = 1669$$

y el mensaje que queremos cifrar es el número $0x01234567 = [1001000110100010101100111]$.

Vamos a calcular el criptograma usando el modo CBC y el cifrado de bloques miniAES. Vamos a dividir nuestro mensaje en dos bloques de 16 bits y así calcular c_1 y c_2 para cada uno de los bloques.

$$\overbrace{0,0,0,0,0,0,0,1,0,0,1,0,0,0,1,1}^{m_1},\overbrace{0,1,0,0,0,1,0,1,0,1,1,0,0,1,1,1}^{m_2}$$

Además, por el enunciado tenemos que $c_0 = 0x0001$, y tenemos por tanto que $E_{\text{dni}}(0x01234567) = c_0c_1c_2$. Tomemos por tanto nuestra clave $k = 1669 = 0x0685 = 0b11010000101$, donde podemos ver que $k_0 = 0$, $k_1 = 6$, $k_2 = 8$ y $k_3 = 5$.

Aquí tenemos nuestra función de sustitución γ calculada de manera explícita:
$\gamma(0000) = 0011$
$\gamma(0001) = 1000$
$\gamma(0010) = 1111$
$\gamma(0011) = 0111$
$\gamma(0100) = 0001$
$\gamma(0101) = 0010$
$\gamma(0110) = 1011$
$\gamma(0111) = 0000$
$\gamma(1000) = 1100$
$\gamma(1001) = 1110$
$\gamma(1010) = 1010$
$\gamma(1011) = 0110$
$\gamma(1100) = 1001$
$\gamma(1101) = 1101$
$\gamma(1110) = 0101$
$\gamma(1111) = 0100$

Y obtenemos así las claves de ronda:

- $w_0 = k_0 = 0 = 0000$
- $w_1 = k_1 = 6 = 0110$
- $w_2 = k_2 = 8 = 1000$
- $w_3 = k_3 = 5 = 0101$
- $w_4 = w_0 \oplus \gamma(w_3) \oplus 0001 = 0000 \oplus 0010 \oplus 0001 = \alpha + 1 = 0011$
- $w_5 = w_1 \oplus w_4 = \alpha^2 + \alpha + \alpha + 1 = \alpha^2 + 1 = 0110$

- $w_6 = w_2 \oplus w_5 = \alpha^3 + \alpha^2 + \alpha = 1110$
- $w_7 = w_3 \oplus w_6 = \alpha^2 + 1 + \alpha^3 + \alpha^2 + \alpha = \alpha^3 + \alpha + 1 = 1011$
- $w_8 = w_4 \oplus \gamma(w_7) \oplus 0010 = \alpha + 1 + \alpha^2 + \alpha + \alpha = \alpha^2 + \alpha + 1 = 0111$
- $w_9 = w_5 \oplus w_8 = \alpha^2 + \alpha + \alpha^2 + \alpha + 1 = 1 = 0001$
- $w_{10} = w_6 \oplus w_9 = \alpha^3 + \alpha^2 + \alpha + 1 = 1111$
- $w_{11} = w_7 \oplus w_{10} = \alpha^3 + \alpha + 1 + \alpha^3 + \alpha^2 + \alpha + 1 = \alpha^2 = 0100$

Procedemos a continuación con el encriptado del mensaje m_1. Para c_1 calculamos ahora $E_k(m_1 \oplus c_0) = E_k(0000000100100010)$. Para ello apliquemos cada una de las funciones de su descomposición $E_k = \sigma_{K_2} \circ \pi \circ \gamma \circ \sigma_{K_1} \circ \theta \circ \pi \circ \gamma \circ \sigma_{K_0}$.

$$
\begin{aligned}
&\sigma_{K_0}\begin{pmatrix} 0000 & 0010 \\ 0001 & 0010 \end{pmatrix} = \begin{pmatrix} 0000 & 0010 \\ 0001 & 0010 \end{pmatrix} + \begin{pmatrix} 0000 & 1000 \\ 0110 & 0101 \end{pmatrix} = \begin{pmatrix} 0000 & 1010 \\ 0111 & 0111 \end{pmatrix} \\
&\gamma\begin{pmatrix} 0000 & 1010 \\ 0111 & 0111 \end{pmatrix} = \begin{pmatrix} 0011 & 1010 \\ 0000 & 0000 \end{pmatrix} \\
&\pi\begin{pmatrix} 0011 & 1010 \\ 0000 & 0000 \end{pmatrix} = \begin{pmatrix} 0011 & 1010 \\ 0000 & 0000 \end{pmatrix} \\
&\theta\begin{pmatrix} 0011 & 1010 \\ 0000 & 0000 \end{pmatrix} = \begin{pmatrix} 0011 & 0010 \\ 0010 & 0011 \end{pmatrix} \cdot \begin{pmatrix} 0011 & 1010 \\ 0000 & 0000 \end{pmatrix} \\
&\qquad\qquad\qquad = \begin{pmatrix} \alpha+1 & \alpha \\ \alpha & \alpha+1 \end{pmatrix} \cdot \begin{pmatrix} \alpha+1 & \alpha^3+\alpha \\ 0 & 0 \end{pmatrix} \\
&\qquad\qquad\qquad = \begin{pmatrix} \alpha^2+1 & \alpha^3+\alpha^2+1 \\ \alpha^2+\alpha & \alpha^2+\alpha+1 \end{pmatrix} = \begin{pmatrix} 0101 & 1101 \\ 0110 & 0111 \end{pmatrix} \\
&\sigma_{K_1}\begin{pmatrix} 0101 & 1101 \\ 0110 & 0111 \end{pmatrix} = \begin{pmatrix} 0101 & 1101 \\ 0110 & 0111 \end{pmatrix} + \begin{pmatrix} 0011 & 1110 \\ 0110 & 1011 \end{pmatrix} = \begin{pmatrix} 0110 & 0011 \\ 0000 & 1100 \end{pmatrix} \\
&\gamma\begin{pmatrix} 0110 & 0011 \\ 0000 & 1100 \end{pmatrix} = \begin{pmatrix} 1011 & 0101 \\ 0011 & 0001 \end{pmatrix} \\
&\pi\begin{pmatrix} 1011 & 0101 \\ 0011 & 0001 \end{pmatrix} = \begin{pmatrix} 1011 & 0101 \\ 0001 & 0011 \end{pmatrix} \\
&\sigma_{K_2}\begin{pmatrix} 1011 & 0101 \\ 0001 & 0011 \end{pmatrix} = \begin{pmatrix} 1011 & 0101 \\ 0001 & 0011 \end{pmatrix} + \begin{pmatrix} 0111 & 1111 \\ 0001 & 0100 \end{pmatrix} = \begin{pmatrix} 1100 & 1010 \\ 0000 & 0111 \end{pmatrix}
\end{aligned}
$$

Conseguimos finalmente que $c_1 = E_k(m_1 \oplus c_0) = 1100000010100111$. Procedemos al encriptado de c_2, que sabemos que tiene la forma $c_2 = E_k(m_2 \oplus c_1) = E_k(0100010101100111 \oplus 1100000010100111) = E_k(1000010111000000)$. Procedemos por tanto aplicando la descomposición de E_k como en el apartado anterior:

$$\sigma_{K_0}\begin{pmatrix}1000 & 1100\\0101 & 0000\end{pmatrix}=\begin{pmatrix}1000 & 1100\\0101 & 0000\end{pmatrix}+\begin{pmatrix}0000 & 1000\\0110 & 0101\end{pmatrix}=\begin{pmatrix}1000 & 0100\\0011 & 0101\end{pmatrix}$$

$$\gamma\begin{pmatrix}1000 & 0100\\0011 & 0101\end{pmatrix}=\begin{pmatrix}1100 & 0001\\0111 & 0010\end{pmatrix}$$

$$\pi\begin{pmatrix}1100 & 0001\\0111 & 0010\end{pmatrix}=\begin{pmatrix}1100 & 0001\\0010 & 0111\end{pmatrix}$$

$$\begin{aligned}\theta\begin{pmatrix}1100 & 0001\\0010 & 0111\end{pmatrix}&=\begin{pmatrix}0011 & 0010\\0010 & 0011\end{pmatrix}\cdot\begin{pmatrix}1100 & 0001\\0010 & 0111\end{pmatrix}\\&=\begin{pmatrix}\alpha+1 & \alpha\\\alpha & \alpha+1\end{pmatrix}\cdot\begin{pmatrix}\alpha^3+\alpha^2 & 1\\\alpha & \alpha^2+\alpha+1\end{pmatrix}\\&=\begin{pmatrix}\alpha+1 & \alpha^3+\alpha^2+1\\\alpha^3+\alpha^2+1 & \alpha^3+\alpha+1\end{pmatrix}=\begin{pmatrix}0011 & 1101\\1101 & 1011\end{pmatrix}\end{aligned}$$

$$\sigma_{K_1}\begin{pmatrix}0011 & 1101\\1101 & 1011\end{pmatrix}=\begin{pmatrix}0011 & 1101\\1101 & 1011\end{pmatrix}+\begin{pmatrix}0011 & 1110\\0110 & 1011\end{pmatrix}=\begin{pmatrix}0000 & 0011\\1011 & 0000\end{pmatrix}$$

$$\gamma\begin{pmatrix}0000 & 0011\\1011 & 0000\end{pmatrix}=\begin{pmatrix}0011 & 0111\\0110 & 0011\end{pmatrix}$$

$$\pi\begin{pmatrix}0011 & 0111\\0110 & 0011\end{pmatrix}=\begin{pmatrix}0011 & 0111\\0011 & 0110\end{pmatrix}$$

$$\sigma_{K_2}\begin{pmatrix}0011 & 0111\\0011 & 0110\end{pmatrix}=\begin{pmatrix}0011 & 0111\\0011 & 0110\end{pmatrix}+\begin{pmatrix}0111 & 1111\\0001 & 0100\end{pmatrix}=\begin{pmatrix}0100 & 1000\\0010 & 0010\end{pmatrix}$$

Con lo que conseguimos finalmente que $c_2 = E_k(m_2 \oplus c_1) = 0100100000100010$. Así, el mensaje encriptado queda como sigue:

$$E_k(0x01234567) = c = c_0 * c_1 * c_2 = 000000000000000111000000101001110100100000100010$$

Apartado I. ***Calcula*** $\boldsymbol{E_{dni}}(0x01234567)$ ***usando el modo*** CFB**,** $r = 11$**,** ***y vector de inicialización*** $IV = 0x0001$**.**

Tomamos nuestro mensaje $m = 0x01234567 = 1001000110100010101100111$ que tiene 25 cifras, que añadiendo ceros a la izquierda, obtenemos un mensaje para dividir en bloques de 11 bits, obteniendo

$$\overbrace{0,0,0,0,0,0,0,0,1,0,0}^{m_1},\overbrace{1,0,0,0,1,1,0,1,0,0,0}^{m_2},\overbrace{1,0,1,0,1,1,0,0,1,1,1}^{m_3}$$

Procedemos a continuación a encriptar el mensaje $x_1 = 0000000000000001$ mediante la función E_k descrita en el apartado anterior:

$$\begin{aligned}
&\sigma_{K_0}\begin{pmatrix} 0000 & 0000 \\ 0000 & 0001 \end{pmatrix} = \begin{pmatrix} 0000 & 0000 \\ 0000 & 0001 \end{pmatrix} + \begin{pmatrix} 0000 & 1000 \\ 0110 & 0101 \end{pmatrix} = \begin{pmatrix} 0000 & 1000 \\ 0110 & 0100 \end{pmatrix} \\
&\gamma\begin{pmatrix} 0000 & 1000 \\ 0110 & 0100 \end{pmatrix} = \begin{pmatrix} 0011 & 1100 \\ 1011 & 0001 \end{pmatrix} \\
&\pi\begin{pmatrix} 0011 & 1100 \\ 1011 & 0001 \end{pmatrix} = \begin{pmatrix} 0011 & 1100 \\ 0001 & 1011 \end{pmatrix} \\
&\theta\begin{pmatrix} 0011 & 1100 \\ 0001 & 1011 \end{pmatrix} = \begin{pmatrix} 0011 & 0010 \\ 0010 & 0011 \end{pmatrix} \cdot \begin{pmatrix} 0011 & 1100 \\ 0001 & 1011 \end{pmatrix} \\
&\qquad = \begin{pmatrix} \alpha+1 & \alpha \\ \alpha & \alpha+1 \end{pmatrix} \cdot \begin{pmatrix} \alpha+1 & \alpha^3+\alpha^2 \\ 1 & \alpha^3+\alpha+1 \end{pmatrix} \\
&\qquad = \begin{pmatrix} \alpha^2+\alpha+1 & \alpha \\ \alpha^2+1 & \alpha^2+1 \end{pmatrix} = \begin{pmatrix} 0111 & 0010 \\ 0101 & 0101 \end{pmatrix} \\
&\sigma_{K_1}\begin{pmatrix} 0111 & 0010 \\ 0101 & 0101 \end{pmatrix} = \begin{pmatrix} 0111 & 0010 \\ 0101 & 0101 \end{pmatrix} + \begin{pmatrix} 0011 & 1110 \\ 0110 & 1011 \end{pmatrix} = \begin{pmatrix} 0100 & 1100 \\ 0011 & 1110 \end{pmatrix} \\
&\gamma\begin{pmatrix} 0100 & 1100 \\ 0011 & 1110 \end{pmatrix} = \begin{pmatrix} 0001 & 1001 \\ 0111 & 0101 \end{pmatrix} \\
&\pi\begin{pmatrix} 0001 & 1001 \\ 0111 & 0101 \end{pmatrix} = \begin{pmatrix} 0001 & 1001 \\ 0101 & 0111 \end{pmatrix} \\
&\sigma_{K_2}\begin{pmatrix} 0001 & 1001 \\ 0101 & 0111 \end{pmatrix} = \begin{pmatrix} 0001 & 1001 \\ 0101 & 0111 \end{pmatrix} + \begin{pmatrix} 0111 & 1111 \\ 0001 & 0100 \end{pmatrix} = \begin{pmatrix} 0110 & 0110 \\ 0100 & 0011 \end{pmatrix}
\end{aligned}$$

Tenemos por tanto que $E_k(x_1) = 0110011001000011$, y así obtenemos que $msb_{11}(E_k(x_1)) = 01100110010$. Por tanto, $c_1 = m_1 \oplus msb_{11}(E_k(x_1)) = 00000000100 \oplus 01100110010 = 01100110110$.

Por otro lado, $lsb_{16-11}(x_1) = lsb_5(x_1) = 00001$, y por tanto obtenemos $x_2 = 0000101100110110$, a la que aplicamos de nuevo la función E_k: