Ejercicio Tema 2

Ana Buendía Ruiz-Azuaga

April 23, 2022

1 Ejercicio Tema 2

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

1.1 Apartado 1

Calcula $\mathbf{E}_{dni}$(0x01234567) usando el modo CBC e IV = 0x0001.

Trabajamos en $\mathbb{F}_{16} = \mathbb{F}_2(\xi)_{\xi^4+\xi+1}$.

Del ejercicio 2.1, vamos a usar la definición explícita de γ que calculamos en clase, y además consideramos las funciones que, dado

$$\begin{pmatrix} a_0 & a_2 \\ a_1 & a_3 \end{pmatrix} \in \mathbb{F}_{16}^{2\times 2}$$

se definen:

$$\gamma \begin{pmatrix} a_0 & a_2 \\ a_1 & a_3 \end{pmatrix} = \begin{pmatrix} \gamma(a_0) & \gamma(a_2) \\ \gamma(a_1) & \gamma(a_3) \end{pmatrix}$$

$$\pi \begin{pmatrix} a_0 & a_2 \\ a_1 & a_3 \end{pmatrix} = \begin{pmatrix} a_0 & a_2 \\ a_3 & a_1 \end{pmatrix}$$

$$\theta \begin{pmatrix} a_0 & a_2 \\ a_1 & a_3 \end{pmatrix} = \begin{pmatrix} 0011 & 0010 \\ 0010 & 0011 \end{pmatrix} \begin{pmatrix} a_0 & a_2 \\ a_1 & a_3 \end{pmatrix}$$

$$\sigma_{K_i} \begin{pmatrix} a_0 & a_2 \\ a_1 & a_3 \end{pmatrix} = \begin{pmatrix} a_0 & a_2 \\ a_1 & a_3 \end{pmatrix} + \begin{pmatrix} k_{i,0} & k_{i,2} \\ k_{i,1} & k_{i,3} \end{pmatrix}$$

Tenemos que $k = k_0k_1k_2k_3$ y se define $E_K = \sigma_{K_2} \circ \pi \circ \gamma \circ \sigma_{K_1} \circ \theta \circ \pi \circ \gamma \circ \sigma_{K_0}$.

Ahora calculamos nuestro dni módulo 65536, resultando $77770080 \mod 65536 \equiv 44384$.

Y, pasanod 44384 a binario y hexadecimal tenemos que:

$$k = 1010110101100000 = 0xAD60.$$

Además, sabemos que:

$$c_{[0]} = 0x0001 = 0000000000000001$$

que tiene 16 dígitos.

Ahora, dividimos el mensaje en bloques de esta longitud:

$$m = 0x01234567 = 00000001001000110100010101100111$$

Resultando así dos bloques, $m_1 = 0000000100100011$ y $m_2 = 0100010101100111$, luego tenemos que l=2.

A continuación calculamos:

Calculamos K_0:

$$w_0 = k_0 = A = 1010$$
$$w_1 = k_1 = D = 1101$$
$$w_2 = k_2 = 6 = 0110$$
$$w_3 = k_3 = 0 = 0000$$

Calculamos K_1:

$$w_4 = w_0 \oplus \gamma(w_3) \oplus 0001 = 1010 \oplus \gamma(0000) \oplus 0001 = 1000$$
$$w_5 = w_1 \oplus w_4 = 1101 \oplus 1000 = 0101$$
$$w_6 = w_2 \oplus w_5 = 0110 \oplus 0101 = 0011$$
$$w_7 = w3_{\oplus} w_6 = 0000 \oplus 0011 = 0011$$

Calculamos K_2:

$$w_8 = w_4 \oplus \gamma(w_7) \oplus 0010 = 1000 \oplus \gamma(0011) \oplus 0010 = 1101$$
$$w_9 = w_5 \oplus w_8 = 0101 \oplus 1101 = 1000$$
$$w_{10} = w_6 \oplus w_9 = 0011 \oplus 1000 = 1011$$
$$w_{11} = w_7 \oplus w_{10} = 0011 \oplus 1011 = 1000$$

Comenzamos calculando $E_K(m_1 \oplus c_{[0]}) = E_K(0000000100100011 \oplus 0000000000000001) = E_K(0000000100100010)$.

Aplicamos en orden por tanto:

$$\sigma_{K_0}\begin{pmatrix}0000 & 0010\\ 0001 & 0010\end{pmatrix} = \begin{pmatrix}0000 & 0010\\ 0001 & 0010\end{pmatrix} + \begin{pmatrix}1010 & 0110\\ 1101 & 0000\end{pmatrix} = \begin{pmatrix}1010 & 0100\\ 1100 & 0010\end{pmatrix}$$

$$\gamma\begin{pmatrix}1010 & 0100\\ 1100 & 0010\end{pmatrix} = \begin{pmatrix}1010 & 0001\\ 1001 & 1111\end{pmatrix}$$

$$\pi\begin{pmatrix}1010 & 0001\\ 1001 & 1111\end{pmatrix} = \begin{pmatrix}1010 & 0001\\ 1111 & 1001\end{pmatrix}$$

$$\theta\begin{pmatrix}1010 & 0001\\ 1111 & 1001\end{pmatrix} = \begin{pmatrix}0011 & 0010\\ 0010 & 0011\end{pmatrix}\begin{pmatrix}1010 & 0001\\ 1111 & 1001\end{pmatrix} = \begin{pmatrix}0000 & 0010\\ 0101 & 1010\end{pmatrix}$$

$$\sigma_{K_1}\begin{pmatrix}0000 & 0010\\ 0101 & 1010\end{pmatrix} = \begin{pmatrix}0000 & 0010\\ 0101 & 1010\end{pmatrix} + \begin{pmatrix}1000 & 0011\\ 0101 & 0011\end{pmatrix} = \begin{pmatrix}1000 & 0001\\ 0000 & 1001\end{pmatrix}$$

$$\gamma \begin{pmatrix} 1000 & 0001 \\ 0000 & 1001 \end{pmatrix} = \begin{pmatrix} 1100 & 1000 \\ 0011 & 1110 \end{pmatrix}$$

$$\pi \begin{pmatrix} 1100 & 1000 \\ 0011 & 1110 \end{pmatrix} = \begin{pmatrix} 1100 & 1000 \\ 1110 & 0011 \end{pmatrix}$$

$$\sigma_{K_2} \begin{pmatrix} 1100 & 1000 \\ 1110 & 0011 \end{pmatrix} = \begin{pmatrix} 1100 & 1000 \\ 1110 & 0011 \end{pmatrix} + \begin{pmatrix} 1101 & 1011 \\ 1000 & 1000 \end{pmatrix} = \begin{pmatrix} 0001 & 0011 \\ 0110 & 1011 \end{pmatrix}$$

luego $c_{[1]} = 0001011000111011$ y pasamos a calcular $c_{[2]} = E_K(m_2 \oplus c_{[1]}$.

$E_K(m_2 \oplus c_{[1]}) = E_K(0100010101100111 \oplus 0001011000111011) = E_K(0101001101011100)$.

Aplicamos:

$$\sigma_{K_0} \begin{pmatrix} 0101 & 0101 \\ 0011 & 1100 \end{pmatrix} = \begin{pmatrix} 0101 & 0101 \\ 0011 & 1100 \end{pmatrix} + \begin{pmatrix} 1010 & 0110 \\ 1101 & 0000 \end{pmatrix} = \begin{pmatrix} 1111 & 0011 \\ 1110 & 1100 \end{pmatrix}$$

$$\gamma \begin{pmatrix} 1111 & 0011 \\ 1110 & 1100 \end{pmatrix} = \begin{pmatrix} 0100 & 0111 \\ 0101 & 1001 \end{pmatrix}$$

$$\pi \begin{pmatrix} 0100 & 0111 \\ 1110 & 1001 \end{pmatrix} = \begin{pmatrix} 0100 & 0111 \\ 1001 & 0101 \end{pmatrix}$$

$$\theta \begin{pmatrix} 0100 & 0111 \\ 1001 & 0101 \end{pmatrix} = \begin{pmatrix} 0011 & 0010 \\ 0010 & 0011 \end{pmatrix} \begin{pmatrix} 0100 & 0111 \\ 1001 & 0101 \end{pmatrix} = \begin{pmatrix} 1101 & 0011 \\ 0000 & 0001 \end{pmatrix}$$

$$\sigma_{K_1} \begin{pmatrix} 1101 & 0011 \\ 0000 & 0001 \end{pmatrix} = \begin{pmatrix} 1101 & 0011 \\ 0000 & 0001 \end{pmatrix} + \begin{pmatrix} 1000 & 0011 \\ 0101 & 0011 \end{pmatrix} = \begin{pmatrix} 0101 & 0000 \\ 0101 & 0010 \end{pmatrix}$$

$$\gamma \begin{pmatrix} 0101 & 0000 \\ 0101 & 0010 \end{pmatrix} = \begin{pmatrix} 0010 & 0011 \\ 0010 & 1111 \end{pmatrix}$$

$$\pi \begin{pmatrix} 0010 & 0011 \\ 0010 & 1111 \end{pmatrix} = \begin{pmatrix} 0010 & 0011 \\ 1111 & 0010 \end{pmatrix}$$

$$\sigma_{K_2} \begin{pmatrix} 0010 & 0011 \\ 1111 & 0010 \end{pmatrix} = \begin{pmatrix} 0010 & 0011 \\ 1111 & 0010 \end{pmatrix} + \begin{pmatrix} 1101 & 1011 \\ 1000 & 1000 \end{pmatrix} = \begin{pmatrix} 1111 & 1000 \\ 0111 & 1010 \end{pmatrix}$$

Luego $c_{[2]} = 1111011110001010$ y, por tanto:

$E_{dni}(0x1234567) = c = c_{[0]}c_{[1]}c_{[2]} = 00000000000000010001011000111011111110111110001010$

1.2 Apartado 2

Calcula $\mathbf{E}_{dni}$(0x01234567) usando el modo CFB, r=11, y vector de inicialización IV = 0x0001.

Tenemos que $x_{[1]} = 0x0001 = 0000000000000001$, que tiene 16 dígitos, y por tanto N=16.

Por otro lado, como $m = 0x01234567$ tiene 32 dígitos, y 32 no es divisible por r=11, añado un 1 al final del mensaje, de forma que su longitud sea 33, divisible por 11. Ahora, dividimos el mensaje en secciones de 11 dígitos:

$$m = 0x01234567 = 00000001001000110100010101100111 1$$

Y por tanto $m_1 = 00000001001$, $m_2 = 00011010001$ y $m_3 = 01011001111$, por tanto $l = 3$.

La clave es la misma de ante, $k = 0xAD60$, luego no se recalculan los w_i, con $i = 1, \cdots 11$.

Calculamos $E_K(x_{[1]})$:

$$\sigma_{K_0}\begin{pmatrix}0000 & 0000\\ 0000 & 0001\end{pmatrix} = \begin{pmatrix}0000 & 0000\\ 0000 & 0001\end{pmatrix} + \begin{pmatrix}1010 & 0110\\ 1101 & 0000\end{pmatrix} = \begin{pmatrix}1010 & 0110\\ 1101 & 0001\end{pmatrix}$$

$$\gamma\begin{pmatrix}1010 & 0110\\ 1101 & 0001\end{pmatrix} = \begin{pmatrix}1010 & 1011\\ 1101 & 1000\end{pmatrix}$$

$$\pi\begin{pmatrix}1010 & 1011\\ 1101 & 1000\end{pmatrix} = \begin{pmatrix}1010 & 10011\\ 1000 & 1101\end{pmatrix}$$

$$\theta\begin{pmatrix}1010 & 1011\\ 1000 & 1101\end{pmatrix} = \begin{pmatrix}0011 & 0010\\ 0010 & 0011\end{pmatrix}\begin{pmatrix}1010 & 1011\\ 1000 & 1101\end{pmatrix} = \begin{pmatrix}1110 & 0111\\ 1100 & 0001\end{pmatrix}$$

$$\sigma_{K_1}\begin{pmatrix}1110 & 0111\\ 1100 & 0001\end{pmatrix} = \begin{pmatrix}1110 & 0111\\ 1100 & 0001\end{pmatrix} + \begin{pmatrix}1000 & 0011\\ 0101 & 0011\end{pmatrix} = \begin{pmatrix}0110 & 0100\\ 1001 & 0010\end{pmatrix}$$

$$\gamma\begin{pmatrix}0110 & 0100\\ 1001 & 0010\end{pmatrix} = \begin{pmatrix}1011 & 0001\\ 1110 & 1111\end{pmatrix}$$

$$\pi\begin{pmatrix}1011 & 0001\\ 1110 & 1111\end{pmatrix} = \begin{pmatrix}1011 & 0001\\ 1111 & 1110\end{pmatrix}$$

$$\sigma_{K_2}\begin{pmatrix}1011 & 0001\\ 1111 & 1110\end{pmatrix} = \begin{pmatrix}1011 & 0001\\ 1111 & 1110\end{pmatrix} + \begin{pmatrix}1101 & 1011\\ 1000 & 1000\end{pmatrix} = \begin{pmatrix}0110 & 1010\\ 0111 & 0110\end{pmatrix}$$

luego $E_K(x_{[1]}) = 0110011110100110$, y tenemos que:

$$\text{msb}_r(E_K(x_{[1]})) = 011001111101$$

$$\text{lsb}_{N-r}(x_{[1]}) = 00001$$

$$c_{[1]} = m_1 \oplus \text{msb}_r(E_K(x_{[1]})) = 00000001001 \oplus 01100111101 = 01100110100$$

$$x_{[2]} = \text{lsb}_{N-r}(x_{[1]})||c_{[1]} = 0000101100110100$$

Ahora $E_K(x_{[2]})$:

$$\sigma_{K_0}\begin{pmatrix}0000 & 0011\\ 1011 & 0100\end{pmatrix} = \begin{pmatrix}0000 & 0011\\ 1011 & 0100\end{pmatrix} + \begin{pmatrix}1010 & 0110\\ 1101 & 0000\end{pmatrix} = \begin{pmatrix}1010 & 0101\\ 0110 & 0100\end{pmatrix}$$

$$\gamma\begin{pmatrix}1010 & 0101\\ 0110 & 0100\end{pmatrix} = \begin{pmatrix}1010 & 0010\\ 1011 & 0001\end{pmatrix}$$

$$\pi\begin{pmatrix}1010 & 0010\\ 1011 & 0001\end{pmatrix} = \begin{pmatrix}1010 & 0010\\ 0001 & 1011\end{pmatrix}$$

$$\theta\begin{pmatrix}1010 & 0010\\ 0001 & 1011\end{pmatrix} = \begin{pmatrix}0011 & 0010\\ 0010 & 0011\end{pmatrix}\begin{pmatrix}1010 & 0010\\ 0001 & 1011\end{pmatrix} = \begin{pmatrix}1111 & 0011\\ 0100 & 1010\end{pmatrix}$$

$$\sigma_{K_1}\begin{pmatrix}1111 & 0011\\ 0100 & 1010\end{pmatrix} = \begin{pmatrix}1111 & 0011\\ 0100 & 1010\end{pmatrix} + \begin{pmatrix}1000 & 0011\\ 0101 & 0011\end{pmatrix} = \begin{pmatrix}0111 & 0000\\ 0001 & 1001\end{pmatrix}$$

$$\gamma\begin{pmatrix}0111 & 0000\\ 0001 & 1001\end{pmatrix} = \begin{pmatrix}0000 & 0011\\ 1000 & 1110\end{pmatrix}$$

$$\pi\begin{pmatrix}0000 & 0011\\ 1000 & 1110\end{pmatrix} = \begin{pmatrix}0000 & 0011\\ 1110 & 1000\end{pmatrix}$$

$$\sigma_{K_2}\begin{pmatrix}0000 & 0011\\ 1110 & 1000\end{pmatrix} = \begin{pmatrix}0000 & 0011\\ 1110 & 1000\end{pmatrix} + \begin{pmatrix}1101 & 1011\\ 1000 & 1000\end{pmatrix} = \begin{pmatrix}1101 & 1000\\ 0110 & 0000\end{pmatrix}$$

luego $E_K(x_{[2]}) = 1101011010000000$, y tenemos que:

$$\text{msb}_r(E_K(x_{[2]})) = 11010110100$$

$$\text{lsb}_{N-r}(x_{[2]}) = 10100$$

$$c_{[2]} = m_2 \oplus \text{msb}_r(E_K(x_{[2]})) = 00011010001 \oplus 11010110100 = 11001100101$$

$$x_{[3]} = \text{lsb}_{N-r}(x_{[2]})||c_{[2]} = 1010011001100101$$

Ahora calculamos $E_K(x_{[3]})$:

$$\sigma_{K_0}\begin{pmatrix}1010 & 0110\\ 0110 & 0101\end{pmatrix} = \begin{pmatrix}1010 & 0110\\ 0110 & 0101\end{pmatrix} + \begin{pmatrix}1010 & 0110\\ 1101 & 0000\end{pmatrix} = \begin{pmatrix}0000 & 0000\\ 1011 & 0101\end{pmatrix}$$

$$\gamma\begin{pmatrix}0000 & 0000\\ 1011 & 0101\end{pmatrix} = \begin{pmatrix}0011 & 0011\\ 0110 & 0010\end{pmatrix}$$

$$\pi\begin{pmatrix}0011 & 0011\\ 0110 & 0010\end{pmatrix} = \begin{pmatrix}0011 & 0011\\ 0010 & 0110\end{pmatrix}$$

$$\theta \begin{pmatrix} 0011 & 0011 \\ 0010 & 0110 \end{pmatrix} = \begin{pmatrix} 0011 & 0010 \\ 0010 & 0011 \end{pmatrix} \begin{pmatrix} 0011 & 0011 \\ 0010 & 0110 \end{pmatrix} = \begin{pmatrix} 0001 & 1001 \\ 0000 & 1100 \end{pmatrix}$$

$$\sigma_{K_1} \begin{pmatrix} 0001 & 0011 \\ 0000 & 1100 \end{pmatrix} = \begin{pmatrix} 0001 & 0011 \\ 0000 & 1100 \end{pmatrix} + \begin{pmatrix} 1000 & 0011 \\ 0101 & 0011 \end{pmatrix} = \begin{pmatrix} 1001 & 1010 \\ 0101 & 1111 \end{pmatrix}$$

$$\gamma \begin{pmatrix} 1001 & 1010 \\ 0101 & 1111 \end{pmatrix} = \begin{pmatrix} 1110 & 1010 \\ 0010 & 0100 \end{pmatrix}$$

$$\pi \begin{pmatrix} 1110 & 1010 \\ 0010 & 0100 \end{pmatrix} = \begin{pmatrix} 1110 & 1010 \\ 0100 & 0010 \end{pmatrix}$$

$$\sigma_{K_2} \begin{pmatrix} 1110 & 1010 \\ 0100 & 0010 \end{pmatrix} = \begin{pmatrix} 1110 & 1010 \\ 0100 & 0010 \end{pmatrix} + \begin{pmatrix} 1101 & 1011 \\ 1000 & 1000 \end{pmatrix} = \begin{pmatrix} 0011 & 0001 \\ 1100 & 1010 \end{pmatrix}$$

luego $E_K(x_{[3]}) = 0011110000011010$, y tenemos que:

$$\mathrm{msb}_r(E_K(x_{[3]})) = 00111100000$$

$c_{[3]} = m_3 \oplus \mathrm{msb}_r(E_K(x_{[3]})) = 01011001111 \oplus 00111100000 = 01100101111$

Por tanto $E_{dni}(0x01234567) = c = c_{[1]}c_{[2]}c_{[3]} = 011001101001100110010101100101111$.