Soluciones

4. Semana 4

4.1. Anillos de polinomios. Cuerpo de Galois. Operaciones en el algoritmo AES

1. *a*)

$$\mathcal{P}_f(\mathbb{Z}_2) = \{0,\, 1,\, x,\, x+1\} = \{00, 01, 10, 11\}.$$
$$\mathcal{P}_g(\mathbb{Z}_2) = \{0,\, 1,\, x,\, x+1\} = \{00, 01, 10, 11\}.$$

   b) En $\mathcal{P}_f(\mathbb{Z}_2)$, $11^2 = 11$. En $\mathcal{P}_g(\mathbb{Z}_2)$, $11^2 = 10$.

   c) En $\mathcal{P}_f(\mathbb{Z}_2)$:

·	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10	10	00
11	00	11	00	11

   En $\mathcal{P}_g(\mathbb{Z}_2)$:

·	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01
11	00	11	01	10

   d) $\mathcal{P}_f(\mathbb{Z}_2)$ no es un cuerpo ($x^2 + x$ no es irreducible). En $\mathcal{P}_f(\mathbb{Z}_2)$, 10 y 11 no tienen inverso.

   e) $\mathcal{P}_g(\mathbb{Z}_2)$ es un cuerpo (x^2+x+1 es irreducible). En $\mathcal{P}_g(\mathbb{Z}_2)$, $10^{-1} = 11$ y $11^{-1} = 10$.

2. $11010011 \cdot 00010010 = 00100010$.

3. *a*) $a1 \cdot 03 = f8$.

   b) $(00, 00, a1, 00) \cdot (00, 03, 00, 03) = (f8, 00, f8, 00)$.

4. En GF(2^8), $8d \cdot 02 = 10001101 \cdot 00000010 = 00000001 = 01$, de donde se deduce que $8d^{-1} = 02$.

4.2. El algoritmo AES

1. Transparencia 7 de “4_2AES”.

2. Transparencia 8 de “4_2AES”.

3. *a*) En la fila 8 y columna d se encuentra “5d”. Por tanto, “8d” se transforma en “5d”.

b) Por el problema 4 de la Sección 4.1, sabemos que $8d^{-1} = 02$ (= 00000010).

$$\begin{bmatrix} 1&0&0&0&1&1&1&1\\ 1&1&0&0&0&1&1&1\\ 1&1&1&0&0&0&1&1\\ 1&1&1&1&0&0&0&1\\ 1&1&1&1&1&0&0&0\\ 0&1&1&1&1&1&0&0\\ 0&0&1&1&1&1&1&0\\ 0&0&0&1&1&1&1&1 \end{bmatrix} \begin{bmatrix}0\\1\\0\\0\\0\\0\\0\\0\end{bmatrix} + \begin{bmatrix}1\\1\\0\\0\\0\\1\\1\\0\end{bmatrix} = \begin{bmatrix}0\\1\\1\\1\\1\\1\\0\\0\end{bmatrix} + \begin{bmatrix}1\\1\\0\\0\\0\\1\\1\\0\end{bmatrix} = \begin{bmatrix}1\\0\\1\\1\\1\\0\\1\\0\end{bmatrix}.$$

01011101 en hexadecimal es "5d". Por tanto, "8d" se transforma en "5d".

4. $Rcon(13) = (ab, 00, 00, 00)$.

5.
$$\begin{aligned} &InvMixColumn(AddRoundKey(S, K_r)) \\ &= InvMixColumn(\begin{bmatrix} s_1 \oplus k_{r1} & s_2 \oplus k_{r2} & s_3 \oplus k_{r3} & s_4 \oplus k_{r4}\end{bmatrix}) \\ &= \begin{bmatrix} d\cdot(s_1 \oplus k_{r1}) & d\cdot(s_2 \oplus k_{r2}) & d\cdot(s_3 \oplus k_{r3}) & d\cdot(s_4 \oplus k_{r4})\end{bmatrix}. \end{aligned}$$

$$\begin{aligned} &AddRoundKey(InvMixColumn(S), InvK_r) \\ &= AddRoundKey(InvMixColumn(S), InvMixColumn(K_r)) \\ &= AddRoundKey(\begin{bmatrix} d\cdot s_1 & d\cdot s_2 & d\cdot s_3 & d\cdot s_4\end{bmatrix}, \begin{bmatrix} d\cdot k_{r1} & d\cdot k_{r2} & d\cdot k_{r3} & d\cdot k_{r4}\end{bmatrix}) \\ &= \begin{bmatrix} (d\cdot s_1)\oplus(d\cdot k_{r1}) & (d\cdot s_1)\oplus(d\cdot k_{r2}) & (d\cdot s_1)\oplus(d\cdot k_{r3}) & (d\cdot s_1)\oplus(d\cdot k_{r4})\end{bmatrix}. \end{aligned}$$

Por la propiedad distributiva de $(\cdot)$ con respecto a $\oplus$, se tiene que, para $i = 1, \ldots, 4$,

$$d\cdot(s_i \oplus k_{ri}) = (d\cdot s_i) \oplus (d\cdot k_{ri})$$

y por tanto,

$$InvMixColumn(AddRoundKey(S, K_r)) = AddRoundKey(InvMixColumn(S), InvK_r).$$

6. En primer lugar debemos expandir la clave K_0 hasta obtener las 3 subclaves de ronda K_1, K_2 y K_3.

A continuación, copiamos C sobre la matriz de estado y realizamos sobre ella las siguientes operaciones:

$$AK \mid ISR \quad IBS \quad AK \quad IMC \mid ISR \quad IBS \quad AK \quad IMC \mid ISR \quad IBS \quad AK \tag{1}$$

donde

$$AK = AddRoundKey, \quad IBS = InvByteSub,$$

$$ISR = InvShiftRow, \quad IMC = InvMixColumn$$

y cada aplicación de la función AK en el esquema anterior utiliza una de las claves K_3, K_2, K_1, K_0 por este orden.

Como IBS opera en bytes mientras que ISR sólo los cambia de lugar, las dos operaciones pueden intercambiarse.

Además, la secuencia $AK \quad IMC$ puede cambiarse por $IMC \quad AK^I$ donde, si en AK se utiliza la clave K_r, en AK^I se utiliza $IMC(K_r)$ (ver Problema 5).

Por tanto, el descifrado puede llevarse a cabo también de la siguiente manera:

$$AK \mid IBS \quad ISR \quad IMC \quad AK^I \mid IBS \quad ISR \quad IMC \quad AK^I \mid IBS \quad ISR \quad AK \tag{2}$$

donde las claves que se utlzan son K_3, $IMC(K_2)$, $IMC(K_1)$, K_0, en ese orden.

Veamos el descifrado completo sobre el bloque C:

Siguiendo el procedimiento (1):

$$\begin{array}{lll}
C = S_3'' \oplus K_3 & = S & \\
AK(S, K_3) & = S \oplus K_3 = S_3'' \oplus K_3 \oplus K_3 & = S_3'' \\
 & & \\
ISR(S_3'') & = ISR(SR(S_3')) & = S_3' \\
IBS(S_3') & = IBS(BS(S_2)) & = S_2 \\
AK(S_2, K_2) & = S_2''' \oplus K_2 \oplus K_2 & = S_2''' \\
IMC(S_2''') & = IMC(MC(S_2'')) & = S_2'' \\
 & & \\
ISR(S_2'') & = ISR(SR(S_2')) & = S_2' \\
IBS(S_2') & = IBS(BS(S_1)) & = S_1 \\
AK(S_1, K_2) & = S_1''' \oplus K_1 \oplus K_1 & = S_1''' \\
IMC(S_1''') & = IMC(MC(S_1'')) & = S_1'' \\
 & & \\
ISR(S_1'') & = ISR(SR(S_1')) & = S_1' \\
IBS(S_1') & = IBS(BS(S_0)) & = S_0 \\
AK(S_0, K_0) & = S \oplus K_0 \oplus K_0 & = S = B.
\end{array}$$

Siguiendo el procedimiento (2) y teniendo en cuenta que

$$IBS(ISR(S)) = ISR(IBS(S)),$$

$$IMC(AK(S, K_r)) = AK(IMC(S), IMC(K_r)) :$$

$$
\begin{array}{lll}
C = S_3'' \oplus K_3 & = S & \\
AK(S, K_3) & = S \oplus K_3 = S_3'' \oplus K_3 \oplus K_3 & = S_3'' \\
 & & \\
IBS(S_3'') & = \hat{S}_3'' & \\
ISR(\hat{S}_3'') & = ISR(IBS(S_3'')) = IBS(ISR(S_3'')) & \\
 & = IBS(ISR(SR(S_3'))) = IBS(S_3') & \\
 & = IBS(BS(S_2)) & = S_2 \\
IMC(S_2) & = \hat{S}_2 & \\
AK(\hat{S}_2, IMC(K_2)) & = AK(IMC(S_2), IMC(K_2)) = IMC(AK(S_2, K_2)) & \\
 & = IMC(S_2 \oplus K_2) = IMC(S_2''' \oplus K_2 \oplus K_2) & \\
 & = IMC(S_2''') = IMC(MC(S_2'')) & = S_2'' \\
 & & \\
IBS(S_2'') & = \hat{S}_2'' & \\
ISR(\hat{S}_2'') & = ISR(IBS(S_2'')) = IBS(ISR(S_2'')) & \\
 & = IBS(ISR(SR(S_2'))) = IBS(S_2') & \\
 & = IBS(BS(S_1)) & = S_1 \\
IMC(S_1) & = \hat{S}_1 & \\
AK(\hat{S}_1, IMC(K_1)) & = AK(IMC(S_1), IMC(K_1)) = IMC(AK(S_1, K_1)) & \\
 & = IMC(S_1 \oplus K_1) = IMC(S_1''' \oplus K_1 \oplus K_1) & \\
 & = IMC(S_1''') = IMC(MC(S_1'')) & = S_1'' \\
 & & \\
IBS(S_1'') & = \hat{S}_1'' & \\
ISR(\hat{S}_1'') & = ISR(IBS(S_1'')) = IBS(ISR(S_1'')) & \\
 & = IBS(ISR(SR(S_1'))) = IBS(S_1') & \\
 & = IBS(BS(S_0)) & = S_0 \\
AK(S_0, K_0) & = S \oplus K_0 \oplus K_0 & = S = B.
\end{array}
$$

4.3. Primalidad. Factorización

1. *a*) $s = 3, \quad t = 111.$

   b) $2^{222} \equiv 540 \mod 889, \quad 2^{444} \equiv 8 \mod 889.$

   c) Podemos asegurar que $n = 889$ es compuesto.

2. $221 = 13 \cdot 17$. Ha sido necesario calcular 4 elementos de la sucesión.

3. $2701 = 73 \cdot 37; \quad t = 55, \quad s = 18.$