Ejercicios

4. Semana 4

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

1. En $\mathbb{Z}_2[x]$ consideramos los polinomios

$$f(x) = x^2 + x \ (= 110), \quad g(x) = x^2 + x + 1 \ (= 111).$$

   a) Describir los elementos de $\mathcal{P}_f(\mathbb{Z}_2)$ y de $\mathcal{P}_g(\mathbb{Z}_2)$.

   b) Calcular 11^2 en $\mathcal{P}_f(\mathbb{Z}_2)$ y en $\mathcal{P}_g(\mathbb{Z}_2)$.

   c) Construir las tablas del producto de $\mathcal{P}_f(\mathbb{Z}_2)$ y de $\mathcal{P}_g(\mathbb{Z}_2)$.

   d) ¿Es $\mathcal{P}_f(\mathbb{Z}_2)$ un cuerpo?

   e) ¿Es $\mathcal{P}_g(\mathbb{Z}_2)$ un cuerpo?

2. Calcular el producto $11010011 \cdot 00010010$ en el cuerpo de Galois $\mathrm{GF}(2^8)$ generado por el polinomio $m(x) = x^8 + x^4 + x^3 + x + 1$, usado en AES.

3. Realizando las operaciones utilizadas en el algoritmo AES:

   a) Calcular el producto de los bytes (expresados en hexadecimal)

$$a1 \cdot 03.$$

   b) Calcular el producto de las palabras (expresadas en hexadecimal)

$$(00, 00, a1, 00) \cdot (00, 03, 00, 03).$$

4. Dados los bytes expresados en hexadecimal $8d$ y 02, comprobar que

$$8d^{-1} = 02$$

   en el cuerpo de Galois $\mathrm{GF}(2^8)$ generado por el polinomio $m(x) = x^8 + x^4 + x^3 + x + 1$, usado en AES.

4.2. El algoritmo AES

1. Describir el algoritmo AES con n rondas.

2. Describir una ronda del algoritmo AES.

3. La transformación *ByteSub* utilizada en el algoritmo AES realiza una sustitución no lineal de cada byte de la matriz de estado, mediante una S-Caja:

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Los bytes están expresados en hexadecimal.

ByteSub transforma un byte "*xy*" en el byte situado en la fila x y la columna y de la S-caja. Por ejemplo, transforma "01" en ""7c" y "a3" en "0a".

La S-caja se obtiene componiendo dos transformaciones:

- Sustitución de cada byte por su inverso en GF(2^8):

$$a = a_7a_6a_5a_4a_3a_2a_1a_0 \longrightarrow a^{-1} = x_7x_6x_5x_4x_3x_2x_1x_0$$

  El valor cero queda inalterado.

- Transformación afín:

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}.$$

Se pide calcular en qué byte se transforma "8d"

a) utilizando la S-caja,

b) utilizando las transformaciones.

Sugerencia: utilizar el problema 4 de la Sección 4.1.

4. Expresar en hexadecimal la constante $Rcon(13)$ utilizada en la función de expansión del cálculo de subclaves en el algoritmo AES.

5. Recordemos que, si $S = \begin{bmatrix} s_1 & s_2 & s_3 & s_4 \end{bmatrix}$ es una cierta matriz de estado, en donde s_1, s_2, s_3, s_4 representan las palabras del estado, y $K_r = \begin{bmatrix} k_{r1} & k_{r2} & k_{r3} & k_{r4} \end{bmatrix}$ es la clave de la ronda r, entonces

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

   e

   $$InvMixColumn(S) = \begin{bmatrix} d \cdot s_1 & d \cdot s_2 & d \cdot s_3 & d \cdot s_4 \end{bmatrix}$$

   donde $d = (0b, 0d, 09, 0e)$ y cada palabra se interpreta como un elemento en el anillo $\mathcal{P}_M(\mathrm{GF}(2^8))$ de polinomios de grado menor que 4 con coeficientes en $\mathrm{GF}(2^8)$ generado por el polinomio no irreducible $M(x) = x^4 + 1$.

   Comprobar que la secuencia

   $$\begin{array}{l} AddRoundKey(S, K_r) \\ InvMixColumn(S) \end{array}$$

   puede cambiarse por

   $$\begin{array}{l} InvMixColumn(S) \\ AddRoundKey(S, InvK_r) \end{array}$$

   donde $InvK_r$ se obtiene aplicando $InvMixColumn$ a K_r.

   Es decir, probar que

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

6. Describimos el procedimiento de un cifrado AES de 3 rondas:

   Supongamos dado un bloque de mensaje B y una clave inicial K_0 de tamaño adecuado.

   En primer lugar debemos expandir la clave K_0 hasta obtener suficientes palabras para completar las subclaves de ronda. En este caso se necesitan 3 subclaves de ronda K_1, K_2 y K_3.

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

   AK | BS SR MC AK | BS SR MC AK | BS SR AK

   donde

   $$AK = AddRoundKey, \quad BS = ByteSub,$$
   $$SR = ShiftRow, \quad MC = MixColumn$$

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

   Veamos el proceso completo de cifrado:

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

Se pide describir el proceso de descifrado y comprobar que el descifrado de C es B.

4.3. Primalidad. Factorización

1. Sea $n = 889$.

   a) Calcular números enteros s y t, con t impar, tales que $n - 1 = 2^s t$.

   b) Sabiendo que
   $$2^{111} \equiv 64 \mod 889,$$
   calcular
   $$2^{222} \mod 889, \quad 2^{444} \mod 889.$$

   c) ¿Podemos asegurar que n es compuesto?

2. Utilizando el polinomio $p(x) = x^2+1$ y la semilla $x_0 = 2$, aplicar el método rho de Pollard para factorizar $n = 221$. ¿Cuántos elementos de la sucesión ha sido necesario calcular?

3. Utilizar el método de Fermat para factorizar $n = 2701$ y especificar los valores obtenidos para t y s.