Ejercicios

3. Semana 3

3.1. Registros de desplazamiento

1. Generar una secuencia producida por un LFSR con polinomio de conexión $C(D)$ y calcular su período. ¿Es el polinomio $C(D)$ primitivo?

   a) $C(D) = D^4 + D^2 + 1$.

   b) $C(D) = D^3 + D + 1$.

2. Consideremos los polinomios

   $$C(D) = D^4 + D + 1, \quad C'(D) = D^4 + D^3 + 1.$$

   Observemos que

   $$C'(D) = D^4 C(\frac{1}{D}).$$

   Obtener las secuencias de longitud 19 generadas por los dos LFSR con polinomios de conexión $C(D)$ y $C(D')$ y estados iniciales $(s_0, s_1, s_2, s_3) = (0, 1, 0, 1)$ y $(s'_0, s'_1, s'_2, s'_3) = (1, 0, 1, 0)$, respectivamente. ¿Se observa alguna relación entre las dos secuencias generadas?

3. Dado el polinomio con coeficientes en $\mathbb{Z}_2$:

   $$C(D) = D^4 + D^3 + D^2 + D + 1.$$

   a) Probar que $C(D)$ es irreducible.

   b) Probar que $C(D)$ divide a $D^5 + 1$.

   c) ¿Es $C(D)$ primitivo?

   d) Obtener los períodos de todas las secuencias posibles generadas por un LFSR de longitud $L = 4$ y polinomio de conexión $C(D)$.

4. Encontrar el LFSR de longitud 4 que genera $(11001000\ldots)$. Generar la secuencia.

3.2. Introducción al cifrado en bloque. Modos de cifrado

1. Explicar en qué consiste la confusión y la difusión.

2. El objetivo de este problema es mostrar que para descifrar un cifrado con una red de Feistel basta aplicar el mismo algoritmo, pero con las claves de ronda en orden inverso.

   Recordemos el algoritmo: en primer lugar se divide el bloque en dos mitades L_0, R_0 (izquierda y derecha). A continuación se realiza un cifrado

iterativo de n rondas, en el que la salida de cada ronda se utiliza como entrada de la siguiente.

$$\left.\begin{array}{l} L_i = R_{i-1} \\ R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \end{array}\right\} \quad i = 1, \ldots, n-1,$$

$$\begin{array}{l} L_n = L_{n-1} \oplus f(R_{n-1}, K_n) \\ R_n = R_{n-1} \end{array}$$

donde f es una función arbitraria, diferente para cada algoritmo, y K_i es la clave de la ronda i.

Es decir, el algoritmo de cifrado es:

- Entrada:
$$\begin{bmatrix} L_0 & R_0 \end{bmatrix}.$$
- Para $i = 1, \ldots, n$:
$$\begin{bmatrix} L_i & R_i \end{bmatrix} = \begin{bmatrix} R_{i-1} & L_{i-1} \oplus f(R_{i-1}, K_i) \end{bmatrix}. \tag{1}$$
- Salida:
$$\begin{bmatrix} R_n & L_n \end{bmatrix}.$$

Y el de descifrado:

- Entrada:
$$\begin{bmatrix} \widehat{L}_0 & \widehat{R}_0 \end{bmatrix}.$$
- Para $i = 1, \ldots, n$:
$$\begin{bmatrix} \widehat{L}_i & \widehat{R}_i \end{bmatrix} = \begin{bmatrix} \widehat{R}_{i-1} & \widehat{L}_{i-1} \oplus f(\widehat{R}_{i-1}, \widehat{K}_i) \end{bmatrix}. \tag{2}$$
- Salida:
$$\begin{bmatrix} \widehat{R}_n & \widehat{L}_n \end{bmatrix}.$$

Las claves de descifrado son $\widehat{K}_1 = K_n$, $\widehat{K}_2 = K_{n-1}$, $\ldots$, $\widehat{K}_n = K_1$.

Es decir,

$$\widehat{K}_i = K_{n-i+1}, \quad 1 = 1, \ldots, n. \tag{3}$$

Lo que debemos probar es que, si la entrada al algoritmo de descifrado es $\begin{bmatrix} R_n & L_n \end{bmatrix}$, la salida es $\begin{bmatrix} L_0 & R_0 \end{bmatrix}$.

Sea entonces

$$\begin{bmatrix} \widehat{L}_0 & \widehat{R}_0 \end{bmatrix} = \begin{bmatrix} R_n & L_n \end{bmatrix}. \tag{4}$$

Debemos probar

$$\begin{bmatrix} \widehat{R}_n & \widehat{L}_n \end{bmatrix} = \begin{bmatrix} L_0 & R_0 \end{bmatrix}. \tag{5}$$

Para ello, demostraremos por inducción sobre i que, para $i = 1, \ldots, n$,

$$\left[\widehat{R}_i \quad \widehat{L}_i\right] = \left[L_{n-i} \quad R_{n-i}\right] \tag{6}$$

ya que entonces para $i = n$ se tiene (5).

- Para $i = 1$:

$$\widehat{R}_1 \overset{(2)}{=} \widehat{L}_0 \oplus f(\widehat{R}_0, \widehat{K}_1) \overset{(4),(3)}{=} R_n \oplus f(L_n, K_n)$$

$$\overset{(1)}{=} L_{n-1} \oplus f(R_{n-1}, K_n) \oplus f(R_{n-1}, K_n) = L_{n-1} \oplus 0 = L_{n-1}.$$

  De forma análoga se prueba $\widehat{L}_1 = R_{n-1}$.

- Supongamos que (6) se satisface para $i = p$ y veamos que entonces también se satisface para $i = p + 1$. Es decir, suponemos que

$$\left[\widehat{R}_p \quad \widehat{L}_p\right] = \left[L_{n-p} \quad R_{n-p}\right] \tag{7}$$

  y debemos probar

$$\left[\widehat{R}_{p+1} \quad \widehat{L}_{p+1}\right] = \left[L_{n-p-1} \quad R_{n-p-1}\right].$$

$$\widehat{R}_{p+1} \overset{(2)}{=} \widehat{L}_p \oplus f(\widehat{R}_p, \widehat{K}_{p+1}) \overset{(7),(3)}{=} R_{n-p} \oplus f(L_{n-p}, K_{n-p})$$

$$\overset{(1)}{=} L_{n-p-1} \oplus f(R_{n-p-1}, K_{n-p}) \oplus f(R_{n-p-1}, K_{n-p}) = L_{n-p-1} \oplus 0 = L_{n-p-1}.$$

  De forma análoga se prueba $\widehat{L}_{p+1} = R_{n-p-1}$.

a) Probar $\widehat{L}_1 = R_{n-1}$.

b) Suponiendo (7), probar $\widehat{L}_{p+1} = R_{n-p-1}$.

3. En el modo de funcionamiento CBC:

$$C_0 = IV$$
$$C_i = \mathrm{E}(M_i \oplus C_{i-1}, K)$$

   donde IV es un vector inicial, E es la función de cifrado, M_i es el bloque i y C_i es su cifrado con la clave K.

   Justificar que:

$$M_i = \mathrm{D}(C_i, K) \oplus C_{i-1}$$

   donde D es la función de descifrado.

4. En el modo de funcionamiento CFB:

$$C_0 = IV$$
$$C_i = M_i \oplus \mathrm{E}(C_{i-1}, K)$$

   donde IV es un vector inicial, E es la función de cifrado, M_i es el bloque i y C_i es su cifrado con la clave K.

   Justificar que:

$$M_i = C_i \oplus \mathrm{E}(C_{i-1}, K).$$

3.3. El algoritmo DES

1. Describir la estructura general del algoritmo DES.

2. Describir la estructura de la función f utilizada en el algoritmo DES.

3. S_5 es una S-caja 6×4 utilizada en el algoritmo DES:

S_5	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

   Obtener la salida $S_5(B)$ para los bloques siguientes:

   a) $B = 010101$.

   b) $B = 111100$.

4. Explicar la estructura general del algoritmo de generación de subclaves en DES.

5. PC1 es una tabla de permutación es utilizada en la generación de subclaves en el algoritmo DES. Transforma una clave de 64 bits en una cadena de 56 bits, ya que descarta los colocados en las posiciones $8, 16, 24, 32, 40, 48, 56, 64$, que son bits de control de paridad.

   Permutación PC1

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

   La siguiente clave está expresada en hexadecimal.

   $$e0e0e0e0f1f1f1f1$$

   a) Expresarla en bits.

   b) Obtener la salida después de aplicarle PC1 y expresarla en hexadecimal.

6. Explicar lo que son claves débiles y semidébiles.