Soluciones

3. Semana 3

3.1. Registros de desplazamiento

1. *a*) Por ejemplo, con el estado inicial $(s_3, s_2, s_1, s_0) = (1, 0, 1, 0)$ se obtiene $s = (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, \dots)$. El período es 6. El polinomio $D^4 + D^2 + 1$ no es primitivo.

   b) Por ejemplo, con el estado inicial $(s_2, s_1, s_0) = (1, 1, 1)$ se obtiene $s = (1, 1, 1, 0, 1, 0, 0, 1, \dots)$. El período es 7. El polinomio $D^3 + D + 1$ es primitivo.

2. $s = 01011001000111101 01, \quad s' = 10101111000100110 10$

   $s_j = s'_{19-j}, \quad 0 \le j \le 19$. Es decir, la secuencia s' es la secuencia s recorrida en sentido inverso.

3. *a*) Si $C(D)$ es producto de dos polinomios de grado menor que 4, hay dos posibilidades:
   - Uno de los dos polinomios tiene grado 3 y el otro grado 1.
   - Los dos polinomios tienen grado 2.

   En los dos casos se llega a una contradicción.

   b) Para que $(D^5+1) = (D^4+D^3+D^2+D+1)C_1(D)$, debe ser $C_1(D) = D + 1$.

$$(D^4 + D^3 + D^2 + D + 1)(D + 1)$$
$$= D^5+D^4+D^3+D^3+D^2+D+D^4+D^3+D^3+D^2+D+1 = D^5+1.$$

   c) Los divisores propios de $2^4 - 1 = 15$ son $3, 5$. Como $C(D)$ divide a $D^5 + 1$, $C(D)$ no es primitivo.

   d) Los posibles estados iniciales (s_3, s_2, s_1, s_0) son

   (1)0001, (2)0010, (3)0011, (4)0100, (5)0101, (6)0110, (7)0111, (8)1000,

   (9)1001, (10)1010, (11)1011, (12)1100, (13)1101, (14)1110 (15)1111.

$$s_j = s_{j-4} + s_{j-3} + s_{j-2} + s_{j-1}$$

S_3	S_2	S_1	S_0		S_3	S_2	S_1	S_0		S_3	S_2	S_1	S_0	
0	0	0	1	(1)	0	0	1	0	(2)	0	1	1	1	(7)
1	0	0	0	(8)	1	0	0	1	(9)	1	0	1	1	(11)
1	1	0	0	(12)	0	1	0	0	(4)	1	1	0	1	(13)
0	1	1	0	(6)	1	0	1	0	(10)	1	1	1	0	(14)
0	0	1	1	(3)	0	1	0	1	(5)	1	1	1	1	(15)
0	0	0	1	(1)	0	0	1	0	(2)	0	1	1	1	(7)

   Observemos que se han obtenido todos los posibles estados. Con cualquiera de ellos como estado inicial se obtiene un período igual a 5.

4. $L = 4, \quad C(D) = 1 + D + D^4, \quad s = (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0 \dots)$.

3.2. Introducción al cifrado en bloque. Modos de cifrado

1. Transparencia 3 de "3_2bloque".
2. *a)* $\widehat{L}_1 = \widehat{R}_0 = L_n = R_{n-1}$.
   b) $\widehat{L}_{p+1} = \widehat{R}_p = L_{n-p} = R_{n-p-1}$.
3. $$\mathrm{D}(C_i, K) = \mathrm{D}(\mathrm{E}(M_i \oplus C_{i-1}, K), K) = M_i \oplus C_{i-1}.$$
   $$\mathrm{D}(C_i, K) \oplus C_{i-1} = (M_i \oplus C_{i-1}) \oplus C_{i-1}$$
   $$= M_i \oplus (C_{i-1} \oplus C_{i-1}) = M_i \oplus 0 = M_i.$$
4. $$C_i \oplus \mathrm{E}(C_{i-1}, K) = (M_i \oplus \mathrm{E}(C_{i-1}, K)) \oplus \mathrm{E}(C_{i-1}, K)$$
   $$= M_i \oplus (\mathrm{E}(C_{i-1}, K) \oplus \mathrm{E}(C_{i-1}, K)) = M_i \oplus 0 = M_i.$$

3.3. El algoritmo DES

1. Tansparencias 2, 3 de "3_3DES".
2. Tansparencias 5, 6 de "3_3DES".
3. *a)* $S_5(010101) = 1111$.
   b) $S_5(111100) = 0000$.
4. Transparencias 11, 12 de "3_3DES".
5. *a)* 1110 0000 1110 0000 1110 0000 1110 00001111 0001 1111 0001 1111 0001 1111 0001
   b) $ffffffff0000000$
6. Tansparencias 17, 18 de "3_3DES".