ETSETB
Curso 2003-04 Primavera
EXAMEN DE TRANSMISIÓN DE DATOS
18 de junio de 2004

PUBLICACIÓN DE NOTAS PROVISIONALES: 28/06/04
FECHA LÍMITE PARA LAS ALEGACIONES: 30/06/04
PUBLICACIÓN DE NOTAS DEFINITIVAS: 02/07/04

NOTAS IMPORTANTES:
Toda hoja de respuestas que no esté completamente identificada será anulada.
La numeración en la hoja de respuestas es la de la *izquierda* (*correlativas*)
No se responderá a ninguna pregunta sobre el enunciado. El alumno responderá según su criterio pudiendo realizar las alegaciones que considere oportunas por escrito en la secretaría de la ETSETB a partir de la publicación de las calificaciones provisionales y hasta el plazo arriba indicado. En ellas debe consignarse OBLIGATORIAMENTE el DNI y el código de la prueba.

Queda expresamente prohibido el uso de cualquier dispositivo de comunicación. El incumplimiento de esta norma supondrá la expulsión del examen.

CÓDIGO DE LA PRUEBA: 230 11510 00 0

1. Sea una fuente con alfabeto de 9 símbolos y probabilidades de emisión de los símbolos $\{0.3, 0.2, 0.1, 0.1, 0.1, 0.075, 0.075, 0.025, 0.025\}$ respectivamente. La entropía de la fuente es de 2.8087 bits/símbolo-fuente. El alfabeto del código que se utiliza tiene 5 símbolos. Las longitudes de las palabras código son $\{1, 1, 1, 2, 2, 2, 2, 3, 3\}$ respectivamente. ¿Qué afirmación es correcta?

   (a) Es posible encontrar un código más eficiente
   (b) La longitud media del código es de 2.45 símbolos-código/símbolos-fuente
   (c) El código no puede ser instantáneo
   (d) Ninguna de las anteriores

b) $\overline{L} = \sum_{i=1}^{9} p_i \cdot L_i = 0'3 \cdot 1 + 0'2 \cdot 1 + 0'1 \cdot 1 + 0'1 \cdot 2 + 0'1 \cdot 2 + 0'075 \cdot 2 + 0'075 \cdot 2 + 0'025 \cdot 3 + 0'025 \cdot 3 = 1'45 \ \frac{\text{símbolo\_código}}{\text{símbolo\_fuente}}$

No

a) Quiero expresar H en $\left[\frac{\text{símbolo\_código}}{\text{símbolo\_fuente}}\right]$

$$H = \sum_{i=1}^{9} p_i \cdot \log_S \frac{1}{p_i} \left[\frac{\text{símb\_cód.}}{\text{símb\_fuent}}\right] = \left(\sum_{i=1}^{9} p_i \cdot \underbrace{\log_2\left(\frac{1}{p_i}\right)}_{\frac{\log 1/p_i}{\log 2}} \left[\frac{\text{bits}}{\text{símb\_fuent}}\right]\right) \cdot \frac{\log 2}{\log S}$$

$$= 2'8087 \cdot \frac{\log 2}{\log 5} = 1'2096 \left[\frac{\text{símb\_cód.}}{\text{símb\_fuent}}\right]$$

$$E = \frac{H}{\overline{L}} = \frac{1'2096}{1'45} = 0'8342 < 1 \rightarrow \text{Sí se existen algún código más eficiente.}$$

c) Para $\exists$ cód. inst., debe cumplirse desigualdad KRAFT:

$$\sum_{i=1}^{9} S^{-L_i} \leq 1 \rightarrow 3 \cdot \frac{1}{5} + 4 \cdot \frac{1}{5^2} + 2 \cdot \frac{1}{5^3} = 0'7765 \leq 1$$

Sí se puede ser instantáneo.

2. Referente a los códigos polinómicos, ¿qué afirmación es correcta?

(a) Hay palabras código no nulas de grado menor que $g(D)$

(b) Todo código detecta siempre todos los errores cuyo polinomio $e(D)$ tenga grado menor o igual que el grado del polinomio generador

(c) El polinomio generador es siempre la palabra código de menor peso

(d) Ninguna de las anteriores

a) No, el grado mínimo de las palabras código es el grado de $g(D)$, es decir r. $Y(D) = g(D) \cdot X(D)$

b) Falso. Si $e(D)$ tiene igual grado que $g(D)$, para el caso $e(D) = g(D)$ no se detectaría ese error. Si dijera solo "grado menor", sería correcta.

c) Falso. No tiene por qué!

Para $g(D) = g_{n-k} \cdot D^{n-k} + \cdots + g_1 \cdot D + g_0$

$$G_{k \times n} = \begin{bmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & 0 \cdots & 0 \\ \vdots & & & & & & \\ 0 & \cdots & 0 & g_0 & \cdots & \cdots & g_{n-k} \end{bmatrix}$$

Sería un código no sistemático.

Puede que haya otra palabra código (a parte de las que conforman G) con menor peso que $g(D)$:

$g(D) = D^3 + D^2 + D + 1$, $n = 7$

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \Rightarrow 1000100$$

$w = 2$

3. Sea un código polinómico sistemático (6, 3) al que pertenecen las palabras código 101101, 011011, 010010. ¿Qué afirmación es correcta?

(a) El polinomio generador es $g(D) = D^3 + D^2 + 1$

(b) El polinomio generador es $g(D) = D^4 + D + 1$

(c) 000101 es palabra código

(d) Ninguna de las anteriores

b) $n=6$, $k=3$ $\Big\}$ $r=3$ $\rightarrow$ $g(D)$ tiene grado $r=3$

c) Código:

000	000
001	001
010	010
011	011
100	100
101	101
110	110
111	111

(+)

No. Los códigos cíclicos son lineales, deben incluir al elemento neutro.

a) $X = 101 \rightarrow X(D) = D^2 + 1$

$Y(D) = R(D) + D^r \cdot X(D)$

$D^r \cdot X(D) = D^3 \cdot (D^2 + 1) = D^5 + D^3$

$D^r \cdot X(D) \bmod g(D) =$

$$\begin{array}{r|l} D^5 + D^3 & D^3 + D^2 + 1 \\ \hline D^5 + D^4 + D^2 & D^2 + D \\ \hline D^4 + D^3 + D^2 & \\ D^4 + D^3 + D & \\ \hline D^2 + D = R(D) & \end{array}$$

$Y(D) = D^2 + D + D^5 + D^3 = D^5 + D^3 + D^2 + D \equiv 101110$

— NO.

4. Sea un código bloque lineal (6, 3) con matriz generadora G. Se recibe Z=011100. Se puede afirmar que:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

(a) La palabra código 001101 es más verosímil que la palabra código 011010

(b) La palabra código 001101 es menos verosímil que la palabra código 011010

(c) La palabra código 110100 es más verosímil que la palabra código 101110

(d) Ninguna de las anteriores

Código:

X	Y	$z = 011100$
000	000 →	$d(Y,z) = 3$
001	101 →	2
010	111 →	3
011	010 →	2
100	011 →	6
101	110 →	3
110	100 →	2
111	001 →	3

a) $d(001101, z) = d(011010, z) = 2$: Igual de verosímil

b) $d(001101, z) = 2$
$d(011010, z) = 2$
} son = de verosímil

c) $d(110100, z) = 2$ → es más verosímil (está más cerca)
$d(101110, z) = 3$

5. Sea un LFSR con un polinomio de conexiones primitivo $C(D) = D^5+D^2+1$. El contenido inicial de los registros de desplazamiento es $D^2 + D + 1$. ¿Qué afirmación es correcta?

(a) El estado al cabo de 1857 iteraciones es 11110

(b) $C(D)$ es divisor de $D^{186} + 1$

(c) El estado al cabo de 5 iteraciones es 11001

(d) Ninguna de las anteriores

a) Al ser primitivo, $L = 2^5 - 1 = 31$;; $1857 \bmod 31 = 28$

$P^{1857}(D) = P^{28}(D) = P^{(-3)}(D)$ → Hay que retroceder 3 estados.

$D \cdot P^{(-1)}(D) = C(D) \cdot \begin{Bmatrix} 1 \\ 0 \end{Bmatrix} + P^{(0)}(D) = (D^5+D^2+1) \cdot \begin{Bmatrix} 1 \\ 0 \end{Bmatrix} + D^2+D+1 = D^5 + D$

$P^{(-1)}(D) = D^4 + 1$

$D \cdot P^{(-2)}(D) = C(D) \cdot \begin{Bmatrix} 1 \\ 0 \end{Bmatrix} + P^{(-1)}(D) = (D^5+D^2+1) \cdot \begin{Bmatrix} 1 \\ 0 \end{Bmatrix} + D^4 + 1 = D^5 + D^4 + D^2$

$P^{(-2)}(D) = D^4 + D^3 + D$

$D \cdot P^{(-3)}(D) = C(D) \cdot \begin{Bmatrix} 1 \\ 0 \end{Bmatrix} + P^{(-2)}(D) = (D^5+D^2+1) \cdot \begin{Bmatrix} 0 \end{Bmatrix} + D^4 + D^3 + D = D^4 + D^3 + D$

$P^{(-3)}(D) = D^3 + D^2 + 1 \equiv \underset{1}{1}\ \underset{D}{0}\ \underset{D^2}{1}\ \underset{D^3}{1}\ \underset{D^4}{0}$

b) $D^L \bmod C(D) = P^{(0)}(D) = D^2 + D + 1$

$D^{31} \bmod C(D) = D^2 + D + 1 \Rightarrow D^{31} = C(D) \cdot Q(D) + D^2 + D + 1$

$D^{31} + D^2 + D + 1 = C(D) \cdot Q(D)$;; $186 \overline{)\,31}\ 6$

$(D^{31} + D^2 + D + 1)^6 = D^{186} + D^{12} + D^6 + 1 = C^6(D) \cdot Q^6(D)$

$C(D)$ es divisor de $D^{186} + D^{12} + D^6 + 1$.

c)

# iteración	$P^{(m)}(D)$
0	$D^2 + D + 1$
1	$D^3 + D^2 + D$
2	$D^4 + D^3 + D^2$
3	$D^5 + D^4 + D^3 \bmod D^5 + D^2 + 1 = D^4 + D^3 + D^2 + 1$
4	$D^5 + D^4 + D^3 + D \bmod D^5 + D^2 + 1 = D^4 + D^3 + D^2 + D$
5	$D^5 + D^4 + D^3 + D^2 \bmod D^5 + D^2 + 1 = D^4 + D^3 + 1 \equiv \underset{1}{1}\ \underset{D}{0}\ \underset{D^2}{0}\ \underset{D^3}{1}\ \underset{D^4}{1}$

8. Para un sistema RSA con los siguientes parámetros: $e = 723$, $n = 1081$, indique cuál de las siguientes afirmaciones es cierta:

(a) La decodificación del criptograma $c = 47$ no es $m = 47$

(b) La decodificación del criptograma $c = 1035$ no es $m = 1035$

(c) La elección de e no es correcta para que funcione el sistema

(d) todas las anteriores son falsas

$n = 1081 = 23 \cdot 47 = p \cdot q$

$\Phi(n) = (p-1)(q-1) = 1012 = 2^2 \cdot 11 \cdot 23$

$e = 723 = 3 \cdot 241.$

$d \cdot e = 1 + k\,\Phi(n) \Rightarrow d = 7$

a) $m = c^d \bmod n = 47^7 \bmod 1081 = (47^2 \cdot 47)^2 47 \bmod 1081 = 47$

b) $m = c^d \bmod n = 1035^7 \bmod 1081 = (1035^2 \cdot 1035)^2 \cdot 1035 \bmod 1081 = 1035$

c) $m.c.d\,(e, \Phi(n)) = 1$

d) todas las anteriores son falsas

7. ¿Qué afirmación es correcta?

(a) El algoritmo de cifrado DES utiliza redes de Feistel de 18 rondas

(b) El modo de operación del algoritmo de cifrado DES más seguro, es el modo ECB

(c) Un certificado se verifica con la clave privada de su emisor

(d) Ninguno de los anteriores

a) No, son de 16 rondas

b) No, es el menos recomendado. Un atacante tiene facilidades y se si hay patrones en claro, también los hay en cifrado.

c) No, se verifica con la clave pública de quien ha emitido dicho certificado.

9. Dado un código convolucional de tasa 1/3, memoria L=2 y conexiones según la Figura A, indique cuál es la afirmación incorrecta:

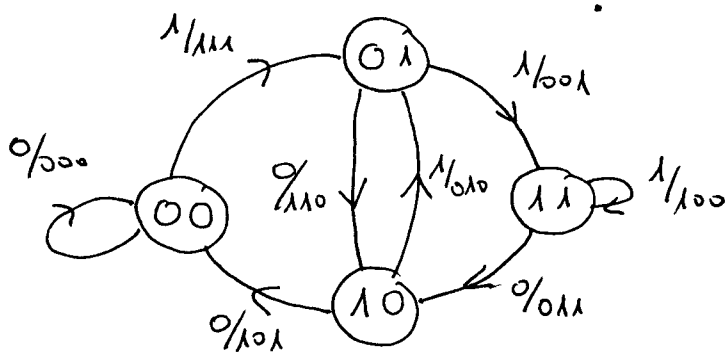
(a) La distancia libre del código es 7

(b) No es un código sistemático

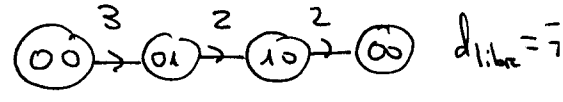
(c) El mensaje decodificado para una secuencia recibida 111 000 111 es 110

(d) Alguna de las otras afirmaciones es incorrecta

S_n u_2	u_1	u_0	S_{n+1} $V_2 = u_2+u_1+u_0$	$V_1 = u_1+u_0$	$V_0 = u_2+u_0$
0	0	0	0	0	0
0	0	1	1	1	1
0	1	0	1	1	0
0	1	1	0	0	1
1	0	0	1	0	1
1	0	1	0	1	0
1	1	0	0	1	1
1	1	1	1	0	0



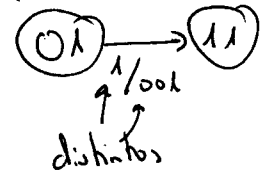
a)



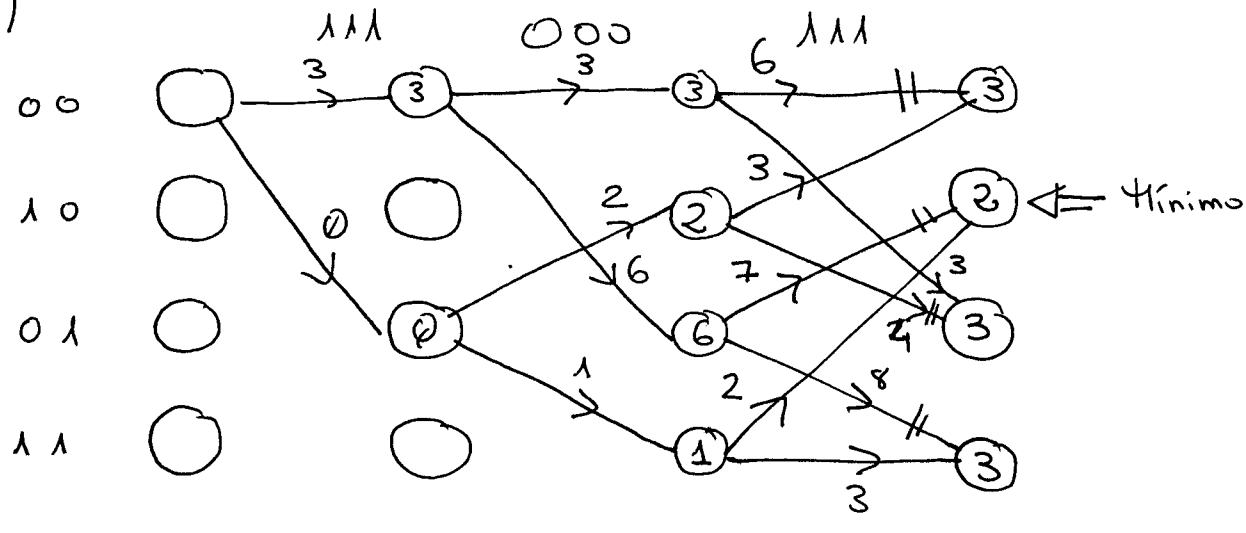
$d_{libre} = 7$

b) No es sistemático.

Por inspección



c)



1 1 ∅ => decodificación

d) Todos los demás son correctos, esta afirmación es falsa.

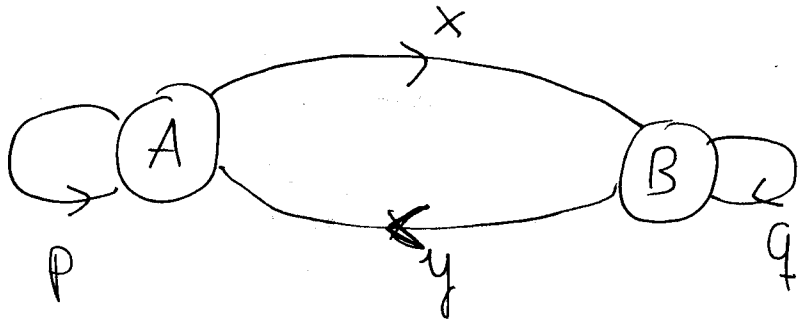
10. Sea una fuente binaria caracterizada por las siguientes probabilidades condicionadas: $P(A|A) = p$, $P(B|A) = x$, $P(A|B) = y$, $P(B|B) = q$. Puede afirmarse que:

(a) Se trata de una fuente sin memoria para cualquier valor de p y q

(b) Se trata de una fuente sin memoria para $p = q$

(c) Se trata de una fuente sin memoria para $x = y = 1/2$

(d) Ninguna de las anteriores



FUENTE SIN MEMORIA

$$\left.\begin{array}{l} p = y \\ q = x \end{array}\right\}.$$

Si $x = y = \frac{1}{2} \Rightarrow p = \frac{1}{2}$ $q = \frac{1}{2}$

SE CUMPLE

---

6. Se codifica el mensaje AABBABBCBBCDA generado por una fuente cuyo alfabeto es $\{A, B, C, D\}$ utilizando la técnica LZ-77. La codificación aplicada es binaria con una capacidad en el búfer de almacenamiento de 3 posiciones. Para referenciar cadenas de símbolos se emplean 2 bits para la longitud y 2 bits para la posición relativa. Teniendo en cuenta que los símbolos de la fuente se codifican con dos bits según la asignación: A=00, B=01, C=10, D=11, indique cuál es el valor hexadecimal de la secuencia binaria enviada (mayor peso a la izquierda):

(a) 0025246AC6F0

(b) 015536FC0

(c) 515D5697B

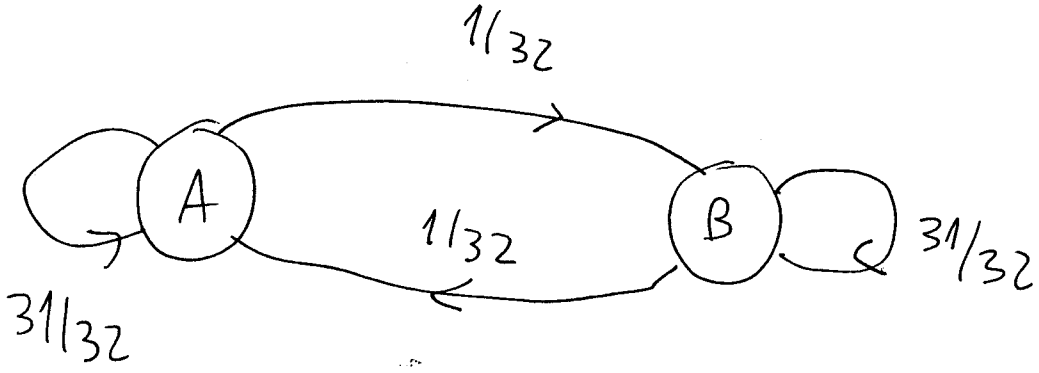
(d) Ninguno de los anteriores

A	AB	BA	BBC	BBCD	A
(0,0)A	(1,1)B	(1,1)A	(3,2)C	(3,3)D	(0,0)A
000000	010101	010100	111010	111111	000000
0	1	5	5	3	A	F	C	0

11. Sea una fuente binaria caracterizada por las siguentes probabilidades condicionadas: $P(A|A) = p, P(B|A) = x, P(A|B) = y, P(B|B) = q$. Sea $p = q = 31/32$, ¿cuál es la SNR mínima a la entrada del receptor si se pueden transmitir de forma fiable 10.000 símbolos de fuente en 2 segundos por un canal con W=1KHz?

(a) 1
(b) 5
(c) 10
(d) Ninguna de las anteriores

¿cual es, aproximadamente, la SNR mínima (en escala lineal) a...



POR SIMETRIA $P(A) = P(B)$; $H(F|A) = H(F|B) = H(t$

$$H(F) = H(F|A) = \frac{31}{32}\log_2\left(\frac{32}{31}\right) + \frac{1}{32}\log_2 32 \simeq 0'2006$$

NOTA: PODEMOS TOMAR (APROXIMANDO) $H(F) \simeq 0'2$ CON UN MARGEN DE ERROR MENOR DE 1%

$$\frac{10.000 \text{ símbolos}}{2 \text{ s}} = 5.000 \frac{\text{símbolos FUENTE}}{\text{s}}$$ / que podemos tx con

$$\underbrace{H(F)}_{5000 \cdot 0'2} = 1.000 \text{ bps}$$

Shannon $V_t < W\log_2\left(1 + \frac{S}{N}\right)$

$10^3 < 10^3 \log_2\left(1 + \frac{S}{N}\right) \Rightarrow \frac{S}{N} = 1$

13. Sea un código polinómico caracterizado por $g(D) = D^3 + 1$. Si se transmite $M = 1011011001$, ¿cuál de los siguientes mensajes recibidos no será detectado como erróneo?

(a) 1111001110 → "cambia último bit a 0"

(b) 1110111001

(c) 1111011101

(d) Ninguna de las anteriores

$g(D) = (D+1)(D^2+D+1)$

a) $1\,0\,1\,1\,0\,1\,1\,0\,0\,1 = M_{tx}$

$\oplus\ 1\,1\,1\,1\,0\,0\,1\,1\,1\,0 = M_{rx}$

$0\,1\,0\,0\,0\,1\,0\,1\,1\,1$ error | 5 errores ⇒ se detecta

b) $1\,0\,1\,1\,0\,1\,1\,0\,0\,1$

$1\,1\,1\,0\,1\,1\,1\,0\,0\,1$

$0\,1\,0\,1\,1\,0\,0\,0\,0\,0$ $\quad e'(D) = D^3 + D + 1$

NO MULTIPLO DE D^3+1

⇒ se detecta

c) $1\,0\,1\,1\,0\,1\,1\,0\,0\,1$

$1\,1\,1\,1\,0\,1\,1\,1\,0\,1$

$0\,1\,0\,0\,0\,0\,0\,0\,1\,0\,0$ $\quad e'(D) = (D^6+1) = (D^3+1)^2$

⇒ NO SE DETECTA

MULTIPLO DE $g(D)$

→ CORREGIR a)

12. Es cierto que

(a) En el cifrado de Vernam la entropía del espacio de mensajes, $H(M)$, puede ser mayor que la entropía del espacion de claves, $H(K)$

(b) Para el cifrado DES, la suma XOR de 2 criptogramas es siempre otro criptograma

(c) Para una función de Hash de 160 bits, el número de mensajes que colisionan (es decir, que dan un mismo Hash(M)) es inferior a $2^{160}+1$

(d) Ninguna de las anteriores

b) → CUALQUIER BLOQUE DE 64 bits puede ser descifrado con una clave, POR LO TANTO, "dé lo que dé" la suma, será un CRIPTOGRAMA

---

14. Se dispone de un cifrador bloque (E) que convierte un grupo de 4 bits en otro, de acuerdo con la expresión $C_i = E(M_i) = (M_i * 15) mod 16$. Dicho cifrador se usa como función de hash mediante la recurrencia $h_i = E(M_i \oplus h_{i-1})$, donde $h_0 = 7$ y el hash es el último bloque de 4 bits obtenido. El número de mensajes de la forma $X_1X_2X_3F$ (incluido el mensaje $FFFF$) que dan el mismo hash que $FFFF$ es:
NOTA: $M_i, h_i, X_i \in \{0, 1, 2, ...F\}$ *y están expresados en hexadecimal*

(a) 196

(b) 225

(c) 256

(d) Ninguno de los anteriores

Ver pregunta 7 del Test del 13 de junio de 2003.

---

15. Se tiene un cifrador en flujo constituido por un LFSR y una función no lineal SIN memoria. Indique la respuesta FALSA

(a) El periodo de la secuencia cifrante no puede ser mayor que el del LFSR

(b) El periodo de la secuencia cifrante puede ser menor que el del LFSR

(c) Si la longitud de la secuencia generada por el LFSR es un número primo, la longitud de la secuencia cifrante es 1 o coincide con la del LFSR

(d) Alguna de las anteriores es correcta

Si la función no tiene memoria, la longitud de la secuencia cifrante debe ser divisor de la long del LFSR

17. Se tiene un código lineal y sistemático, usado como detector, que utiliza como polinomio generador $D^4 + D + 1$, y trabaja con bloques de 11 bits de información. Indique la respuesta correcta

(a) Se detectan siempre todas las ráfagas de longitud 5

(b) No se puede asegurar la detección de ráfagas de errores de longitud menor o igual a 4

(c) No se detectan todos los errores dobles

(d) Ninguna de las anteriores

$n = k + r = 15$

$11 \quad 4$

c) ~~si $e(D) = D^{14} +$~~ Para que $e(D)$ sea múltiplo de $r(D)$ con $W_H(e(D)) = 2$, ~~solo~~ $e(D) = D^{15} + 1$, $D^{30} + 1$, ... pero no puede ser $D^k + 1$, $k < 15$. Por lo tanto todos los errores dobles se detectan

a) Si la ráfaga coincide con $g(D)$ es de 5 errores y no se detecta

b) Si $e(D) = D^m \cdot p(D)$, siendo grado $p(D) \leq 3$, $e(D)$ no puede ser múltiplo de $r(D)$, y por lo tanto se puede asegurar su detección

---

16. De entre los siguientes polinomios sólo hay uno primitivo. Indique cuál es:

(a) $D^{10} + D^7 + 1$

(b) $D^{10} + D^8 + D^7 + D^6 + 1$

(c) $D^{10} + D^4 + D^3 + D^2 + 1$

(d) $D^{10} + D^9 + D^8 + D^7 + D^6 + D^5 + D^4 + D^3 + D^2 + D + 1$

b) y c) son recíprocos, por lo cual si uno lo fuese el otro también.

d) es completo, por lo tanto no puede ser primitivo.

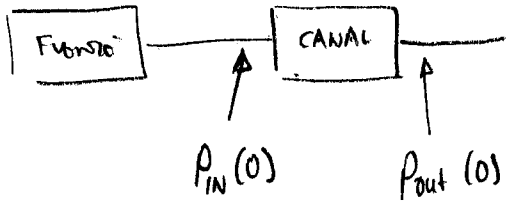
18. Una fuente emite cuatro símbolos independientes $\{A, B, C, D\}$ con probabilidades $\{0.6, 0.2, 0.1, 0.1\}$ respectivamente. Si el codificador de fuente realiza la codificación: $\{A : 00, B : 01, C : 10, D : 11\}$ a la salida del canal binario simétrico se tiene un 60% de ceros ¿Cuánto vale la probabilidad de error de dicho canal? Indique el resultado con dos cifras significativas.

(a) 0.15

(b) 0.22

(c) 0.30

(d) Ninguna de las anteriores



$$P_{IN}(0) = \frac{2 \cdot 0'6 + 1 \cdot 0'2 + 1 \cdot 0'1 + 1 \cdot 0'1}{2} = 0'75$$

$$P_{out}(0) = 0'6 = 0'25 \cdot p_e + 0'75 \cdot (1 - p_e) \Rightarrow$$

$$p_e = \frac{0'15}{0'5} = 0'3$$

---

19. Un procesador permite realizar una exponenciación modular módulo N en $(log_2(N)/16)^2$ operaciones máquina. Se tienen dos sistemas RSA. El sistema A emplea loa valores $e_A = 65537$ y N_A de 1024 bits. El sistema B emplea los valores $e_B = 65537$ y N_B de 512 bits. ¿Cuántas veces resulta más rápido realizar un CIFRADO con el sistema B que con el sistema A?

(a) 2

(b) 4

(c) 8

(d) Ninguna de las anteriores

$$\frac{Op_A}{Op_B} = \left(\frac{1024/16}{512/16}\right)^2 = 4$$