ETSETB
Curso 2003-04 Otoño
EXAMEN DE TRANSMISIÓN DE DATOS
13 de enero de 2004

Publicación de notas provisionales: 19/01/04
Fecha límite para las alegaciones: 22/01/04
Publicación de notas definitivas: 29/01/04

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 un LFSR caracterizado por $c(D) = D^4 + D^3 + D^2 + D + 1$ y estado inicial $S(D) = D^2 + D$. El estado al cabo de 17 iteraciones vale:

   a) $D^2 + D + 1$
   b) $D^3 + D^2$
   c) $D + 1$
   d) Niguna de las anteriores

2. Se define el radio de recubrimiento de un código como el mínimo radio que han de tener las bolas centradas en palabras código para que se recubra todo el espacio de las n-plas. ¿Cuál es el radio de recubrimiento para un código binario perfecto con distancia 7?

   a) 7

   b) 5

   c) 3

   d) Ninguna de las anteriores

3. El número medio de mensajes aleatorios que son necesarios para que, con una probabilidad de 0.5, al menos dos de ellos generen el mismo hash de 160 bits es, aproximadamente:

   a) 2^{160}

   b) 2^{159}

   c) 2^{80}

   d) Ninguno de los anteriores

4. Para un código binario lineal NO se puede afirmar que:

   a) Si el producto escalar de dos palabras código es cero, entonces son ortogonales

   b) Si el producto escalar de dos palabras código es cero, entonces son linealmente independientes

   c) Una palabra código NO NULA puede ser ortogonal a ella misma.

   d) Alguna de las anteriores es falsa

5. Indique la respuesta FALSA:

   a) Si la memoria de un codificador convolucional se dobla, la complejidad computacional de la decodificación se eleva al cuadrado.

   b) Si la longitud de la secuencia codificada mediante un código convolucional se dobla, la complejidad computacional de la decodificación también se dobla.

   c) El número de estados de un codificador convolucional crece exponencialmente con la tasa de codificación.

   d) Alguna de las anteriores es falsa.

6. Dado un código convolucional de tasa 1/3, memoria L=2 y conexiones según la Figura A, indicar cuál es la respuesta correcta:

   a) La distancia libre del código es 6

   b) Es una codificación sistemática

   c) La secuencia de salida del codificador para la entrada (1101) es 111100100000

   d) Ninguna de las anteriores

7. Sea el polinomio $D^5 + D^4 + D^2 + 1$, ¿qué afirmación es correcta?

   a) Genera un código polinómico (15,10)

   b) Es apropiado para un LFSR de máximo período (MLSR)

   c) El código polinómico que genera es capaz de corregir 2 errores

   d) Ninguna de las anteriores

8. Lamentablemente en un sistema RSA se ha filtrado cierta información, los números $x1 = 11710301 = pq$ y $x2 = 11700000$ primos entre sí. Con respecto estos números:

   a) Si el módulo es $x1$ entonces $\phi(x1) = x2$

   b) $x2$ podría utilizarse como el módulo del RSA

   c) Se puede comprobar que la inversa de $x2$ mod $x1$ es -320299

   d) Ninguna de las anteriores

9. Indique cuál de las siguientes afirmaciones es FALSA:

   a) La entropía de una fuente sin memoria sólo depende de la estadística de sus símbolos

   b) La entropía de una fuente es siempre menor o igual a la de otra fuente sin memoria con el mismo alfabeto y con símbolos equiprobables

   c) La entropía de una fuente es siempre menor o igual que la longitud media de la codificación, sin pérdidas, de la fuente

   d) Alguna de las anteriores es falsa

10. Un codificador aritmético de una fuente cuyo alfabeto es $\{A, B, C\}$ envía el valor 0.34 correspondiente a la codificación de un mensaje de 4 caracteres. Sabiendo que la codificación aritmética emplea valores crecientes según el orden $\{A, B, C\}$ y que las probabilidades de estos símbolos son respectivamente 0.5, 0.3 y 0.2, indique el valor del mensaje descodificado:

    a) ABBB

    b) ACBA

    c) CBBA

    d) Ninguno de los anteriores

11. En un sistema de Transmisión de Datos, la sucesión usual de bloques que actúan sobre los datos que emite la fuente de información en el emisor, es:

    a) Código fuente, código de canal, código de cifrado y modulador

    b) Código de cifrado, código fuente, código de canal y modulador

    c) Código fuente, código de cifrado, código de canal y modulador

    d) Ninguna de los anteriores

12. Un código polinómico emplea el polinomio generador $g(D) = D^2 + D + 1$. Es FALSO que:

   a) La palabra $D^3 + D^2 + D$ es palabra código

   b) Si los mensajes de usuario son de 1 bit, la capacidad correctora del código es 1

   c) Si los mensajes de usuario son de 2 bits, se detectan todos los errores dobles

   d) Alguna de las anteriores es falsa

13. Calcule la probabilidad de detección de error (p_d) para el código codificador de canal ternario 2-perfecto de menor redundancia posible cuando la probabilidad de error en el bit que introduce un canal binario simétrico es $p = 10^{-4}$.

   a) $p_d \leq 10^{-5}$

   b) $10^{-5} < p_d \leq 10^{-2}$

   c) $10^{-2} < p_d \leq 10^{-1}$

   d) $10^{-1} < p_d \leq 1$

14. Sea un código codificador de canal de Hamming sistemático caracterizado por la matriz generadora G. Si se recibe la palabra 1011101, ¿qué afirmación es correcta?*Nota: Las posiciones de la palabra recibida se empiezan a numerar desde la izquierda, empezando por la posición 1.*

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

a) Si el código se usa como corrector, se estima el mensaje de usuario 1001.

b) Si el código se usa como detector, no se detecta error en la palabra recibida.

c) Si el código se usa como corrector, suponiendo que hubo error en las posiciones 1 y 4 se confunde con un error simple en la posición 5.

d) Ninguna de las anteriores

15. Se dispone de dos fuentes A y B cada una con un alfabeto de 4 símbolos. ¿Qué afirmación es correcta?

   a) Es imposible un valor de $H(A, B) = 2,4$ bits/símbolo

   b) Si $H(A|B) = 2$ bits/símbolo, entonces $H(B) \leq H(A)$

   c) Se puede afirmar que $H(A, B) = 4$ bits/símbolo

   d) Ninguna de las anteriores

16. Una fuente F que emite dos símbolos según el diagrama de estados de la Figura B (bit más antiguo a la izquierda) atraviesa un canal binario simétrico caracterizado por una probabilidad de error en el bit $p = 0{,}3$. Sea F' la fuente resultante a la salida del canal. ¿Qué afirmación es FALSA?

    a) La fuente F tiene memoria 1

    b) $0{,}90 \leq H(F) \leq 0{,}96$ bits/símbolo

    c) $0{,}990 \leq H(F) \leq 0{,}993$ bits/símbolo

    d) Alguna de las anteriores es falsa

17. Sean a, k, p números naturales, con p primo y sea $mcd(a, p) = 1, a < p$. El valor de $C = (a^{kp})modp$ es:

   a) 1
   b) $a^k modp$
   c) $a^{(p-k)} modp$
   d) Ninguna de las anteriores

18. Sea un código polinómico caracterizado por $g(D) = (D+1)p(D)$, con $p(D)$ un polinomio primitivo de grado 17. NO puede asegurarse la detección de:

   a) $e(D) = D^{25} + D^{17} + D^{15} + D^8$

   b) $e(D) = D^{127} + D^{23} + D^2 + D + 1$

   c) $e(D) = D^{1024} + 1$

   d) Ninguna de las anteriores

19. Sea una fuente sin memoria con 3 símbolos $\{A, B, C\}$. Se sabe que $p(A) = 0{,}5$. La entropía máxima de una fuente extendida de orden 2 es:

    a) 2 bits

    b) 2.5 bits

    c) 3 bits

    d) Ninguna de las anteriores

20. Sea un usuario A de un sistema RSA con los siguientes parámetros: $e = 723; \phi(N) = 1012$. Decodifique $C = 45$, enviado por un usuario B de forma confidencial al usuario A.

   a) $M = 436$

   b) $M = 234$

   c) $M = 45$

   d) Ninguna de las anteriores