ETSETB
Curso 2002-03 Primavera
EXAMEN DE TRANSMISIÓN DE DATOS
13 de junio de 2003

PUBLICACIÓN DE NOTAS PROVISIONALES: 17/06/03
FECHA LÍMITE PARA LAS ALEGACIONES: 19/06/03
PUBLICACIÓN DE NOTAS DEFINITIVAS: 20/06/03

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. Un bibliotecario está introduciendo los códigos ISBN de varios libros en una aplicación. Al introducir el ISBN del libro "Digital Communications" de E. Lee y D. Messerschmitt, observa que hay un dígito rasgado imposible de leer: 0792*93910. ¿Qué afirmación es cierta?
   (a) El código ISBN correcto es 0792893910.
   (b) El valor correcto del borrón es 4
   (c) No es posible corregir ese borrón
   (d) Ninguna de las anteriores

2. Una fuente cuyo alfabeto es { A, B, C, D } emplea el método de codificación LZW. El diccionario dispone de 8 posiciones de almacenamiento que se codifican con 3 bits, donde la primera posición está referenciada por el valor 000. Si al receptor llega la secuencia: {000,011,100,101,110} , el mensaje decodificado es:*(NOTA.- La codificación es la posición en el diccionario)*
   (a) ADADDAADD
   (b) ADDAADDDAA
   (c) ADADDADADDAD
   (d) Ninguno de los anteriores

3. Para una clave pública del algoritmo RSA de valor $n = pq = 23 * 59 = 1357$ y $e = 17$, es verdadero que:
   (a) El cifrado del mensaje $m = 59$ tiene por criptograma $c = 354$
   (b) Para un mensaje M cuyo hash o resumen es $h(M) = 236$ la firma será $(M|118)$
   (c) La clave secreta tiene por valor $d = 1200$
   (d) Ninguna de las anteriores

4. Sea una fuente sin memoria que genera 3 símbolos A, B, C con probabilidades P(A)=0.3, P(B)=0.4, P(C)=0.3. La fuente emite 3000 símbolos por segundo y transmite por un canal que presenta una relación señal a ruido de 15 (escala lineal). ¿Cuál es el mínimo ancho de banda que se necesita para una transmisión fiable?
   (a) 1.18 KHz
   (b) 2.59 KHz
   (c) 11.2 KHz
   (d) Ninguna de las anteriores

5. Un código es $\delta - perfecto$ en detección de errores si detecta un número de errores $\leq \delta$ y si nunca detecta *exactamente* $\delta + 1$. Indíquese la respuesta correcta:
   (a) El código de paridad par (3,2) es 2 perfecto en detección
   (b) El código de paridad par (4,3) es 1 perfecto en detección
   (c) El código de repetición (3,1) es 1 perfecto en detección
   (d) Ninguna de las anteriores

6. Sea un código (n, k) que se caracteriza porque la distancia entre dos palabras cualesquiera es cuatro. Se puede afirmar que:
   (a) El código es 2-perfecto
   (b) El código es 4-perfecto
   (c) El código es 1-perfecto
   (d) Nada de lo anterior puede afirmarse

7. 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) 225
   (b) 256
   (c) 196
   (d) Ninguno de los anteriores

8. Indique cuál de los siguientes polinomios es primitivo:
   (a) $D^6 + D^3 + D + 1$
   (b) $D^6 + D + 1$
   (c) $D^6 + D^2 + 1$
   (d) $D^6 + D^5 + D^4 + D^3 + D^2 + D + 1$

9. Una fuente que emite dos símbolos queda completamente definida con las siguientes probabilidades de emisión condicionadas $p(A|A) = 0.8$ y $p(B|B) = 0.8$. Si atraviesa un canal binario simétrico sin memoria con tasa de error 0.2, la entropía a la SALIDA DEL CANAL es:

   (a) 0.720 bits información/símbolo

   (b) 0.904 bits información/símbolo

   (c) 1 bit información/símbolo

   (d) Ninguna de los anteriores

10. Sea un código de Hamming sistemático con la siguiente matriz de comprobación:

$$H = \begin{pmatrix} 1 & 1 & 0 & * & * & * & * \\ 0 & 1 & 1 & * & * & * & * \\ 1 & 0 & 1 & * & * & * & * \end{pmatrix}$$

    Se transmite $Y = 0000000$ y durante la transmisión se producen errores en las posiciones 2, 3, 4 y 5. ¿Qué mensaje de usuario decodificaríamos?

   (a) X = 0100

   (b) X = 0111

   (c) X = 0011

   (d) X = Ninguno de los anteriores

11. Sea un LFSR con polinomio de conexiones primitivo $C(D) = D^4 + D + 1$. El contenido inicial de los registros de desplazamiento es D ¿Qué afirmación es cierta?

   (a) $C(D)$ es divisor de $D^{48} + 1$

   (b) El estado al cabo de 6 iteraciones $D^2 + 1$

   (c) El estado al cabo de 58 iteraciones es $D^2 + D^3$

   (d) Ninguna de las anteriores.

12. Se tiene un código cíclico con $g(D) = D^4 + D + 1$ (primitivo) y se tienen mensajes de longitud de datos (sin redundancia) de 27 bits. Sabiendo que se han producido 2 errores en la transmisión y que el canal es binario simétrico sin memoria, indíquese la probabilidad de que NO sea detectado

   (a) 16/465

   (b) 13/465

   (c) 17/465

   (d) Ninguna de las anteriores

13. Para verificar un certificado digital necesitamos:

   (a) La clave privada de la Autoridad de Certificación

   (b) La clave pública del posesor del certificado

   (c) La clave pública de la Autoridad de Certificación

   (d) Ninguna de las anteriores

14. Una fuente emite símbolos según este algoritmo:
    -Se lanza un dado, sea X el resultado
    -Se lanza una moneda
    -Si cara, se emite $Xmod4$
    -Si cruz, se emite $(Xmod3) + 4$
    La entropía de la fuente es:

   (a) $1/3 + 2log_2(3)$ bits inf/simb

   (b) $7/6 + log_2(3)$ bits inf/simb

   (c) $log_2(6)$ bits inf/simb

   (d) Ninguna de las anteriores

15. Un código polinómico binario Cod(5,1) tiene por polinomio generador el polinomio $D^4 + D^3 + 1$. Se puede afirmar que:

   (a) Es un código 2-perfecto

   (b) No detecta una ráfaga de errores de longitud 5 con una probabilidad 0.125

   (c) El código es capaz de detectar cualquier número impar de errores

   (d) Nada de lo anterior puede afirmarse

16. Para un código ternario de repetición Cod(3,1) es falso que:

   (a) Si se emplea entrelazado con una profundidad $D = 2$ y se producen únicamente dos errores consecutivos en la transmisión, se asegura la corrección de los mismos

   (b) Es un código 1-perfecto

   (c) La distancia mínima del código es 3

   (d) Alguna de las anteriores es falsa

17. Se sabe que un cifrador que trabaja con bloques de 8 bits realiza una permutación fija de los mismos. El número mínimo de parejas texto-claro texto-cifrado (escogidas) que se necesitan para determinar unívocamente la permutación es:

   (a) 5

   (b) 7

   (c) 3

   (d) Ninguno de los anteriores

18. Una fuente emite dos símbolos A y B con probabilidades: $P(B|A) = P(B|B) = 0.4$. Para una extensión de fuente de orden 1 (agrupaciones de 2 símbolos), ¿cuánto vale la entropía de dicha fuente extendida?

   (a) 1.94 bits inf/simb

   (b) 1.90 bits inf/simb

   (c) 0.95 bits inf/simb

   (d) Ninguna de las anteriores

19. Sea un código polinómico con polinomio generador $g(D) = (D + 1)p(D)$, con $p(D)$ un polinomio primitivo de grado 4. ¿Cuál de los siguientes errores puede NO ser detectado?

   (a) $e(D) = D^{13} + D^2$

   (b) $e(D) = D^{45} + D^{37} + D^{12} + D^8 + D^3$

   (c) $e(D) = D^{14} + D^{13} + D^{12} + D^{11}$

   (d) Todos los patrones de error anteriores pueden ser detectados

20. Sea una fuente de 2 símbolos A y B con las siguientes probabilidades: $P(A) = 1/3, P(A/A) = 2/3$. Calcule la entropía de la fuente.

   (a) 0.739 bits inf/simb

   (b) 0.918 bits inf/simb

   (c) 0.637 bits inf/simb

   (d) Ninguna de las anteriores