

ETSETB
Curso 2005-06 Primavera
EXAMEN DE TRANSMISIÓN DE DATOS
6 de junio de 2006

PUBLICACIÓN DE NOTAS PROVISIONALES: 9/06/2006

FECHA LÍMITE PARA LAS ALEGACIONES: 13/06/2006

PUBLICACIÓN DE NOTAS DEFINITIVAS: 16/06/2006

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. En un sistema de transmisión de datos se emplea un código binario lineal y sistemático Cod(5,2) generado por el polinomio $D^3 + D^2 + 1$. El sistema de decisión entrega al decodificador de canal el bloque con borrones (1 a b c 0). Los valores más verosímiles de a, b y c son respectivamente:
 - a) a=0, b=1, c=1
 - b) a=1, b=0, c=1
 - c) a=1, b=1, c=0
 - d) a=0, b=0, c=1

2. Sean A y B dos fuentes binarias independientes sin memoria donde $H(A)$ tiene entropía máxima. Se puede afirmar que:

a) $H(B/A) < H(A)$

b) $H(A \text{ XOR } B) = H(A)$

c) $I(A;B) > 0$

d) Ninguna de las anteriores

3. Para un receptor con $S/N=10$ y una fuente ternaria sin memoria con probabilidad de emisión de los símbolos $1/2$, $1/8$ y $3/8$ respectivamente, el ancho de banda mínimo necesario para poder transmitir 1000 símbolos por segundo de dicha fuente sin pérdidas es:
- a) 406 Hz
 - b) 526 Hz
 - c) 1748 Hz
 - d) Ninguna de las anteriores

4. En Z_{35} , la inversa de 25 es:

a) 30

b) 1

c) 3

d) Ninguna de las anteriores

5. Sea una fuente $F = \{A, B, C\}$, con las siguientes probabilidades condicionadas

$$P(A/A) = P(C/C) = 0,5;$$

$$P(A/C) = P(C/A) = 0;$$

$$P(A/B) = P(C/B) = 0,5.$$

La eficiencia de una codificación de Huffman de F vale:

a) 1

b) 0.75

c) 0.6

d) Ninguna de las anteriores

6. Para un código con capacidad correctora 5, puede asegurarse que:

- a) La distancia mínima es al menos 12
- b) La razón (k/n) es mayor que 0.1
- c) La redundancia es mayor o igual que 10
- d) Ninguna de las anteriores

7. El número de códigos binarios de Hamming sistemáticos distintos para $n=255$ vale:

- a) $8!$
- b) 256
- c) $247!$
- d) Ninguna de las anteriores

8. Dos usuarios A y B ofrecen confidencialidad a sus comunicaciones mediante un cifrado en flujo (Vernan). La clave de cifrado k es generada por A y enviada a B utilizando un cifrado RSA (la clave pública de B vale $N_B=187=11*17$; $e_B=7$), generándose el criptograma C1. Posteriormente B obtiene k y cifra el mensaje M2, obteniendo el criptograma C2. Conocidos C1=00000011 y C2=11110000 (mayor peso a la izquierda), calcule el valor de M2.

- a) 00110011
- b) 01000101
- c) 11100011
- d) Ninguna de las anteriores

9. Alicia envía un mensaje m a Bob con la clave $e_1=4807$ y $n = pq=360671$ y también a Berta con la clave $e_2=9889$ y $n=360671$. Se consigue descifrar:

- a) con la inversa de $(e_1 + e_2) \bmod \Phi(n)$
- b) con la inversa del $\text{mcd}(e_1, e_2) \bmod \Phi(n)$
- c) únicamente con las inversas de $e_1 \bmod \Phi(n)$ y de $e_2 \bmod \Phi(n)$
- d) Ninguna de las anteriores

10. Dados a, p, q coprimos, entonces $((a * b) \bmod p) * q * (a^{-1} \bmod p)$ es:

- a) $q * (b \bmod p)$ si se calcula el $\bmod(p * q)$
- b) 1 si se calcula el $(\bmod q)$
- c) $b * (q \bmod p)$ si se calcula el $(\bmod p)$ y $b < p$
- d) Ninguna de las anteriores

11. Si n tiene k factores primos impares f_i con multiplicidad l_i , la función $\lambda(n)$ se define como el $mcm(\Phi(f_1^{l_1}), \Phi(f_2^{l_2}), \dots, \Phi(f_k^{l_k}))$ y se cumple que $m^{\lambda(n)} \bmod n = 1$ si el $mcd(m, n) = 1$. Para $n = 19 * 43 * 43$ se calcula el criptograma 127 como $m^e \bmod n$ con $e = 9851$, entonces:
- a) $m = 18033$ y $d = 11$
 - b) $e = 9851$ no es un valor válido
 - c) El número de e distintas tal que $mcd(e, \Phi(n)) = 1$ reducidas $\bmod \lambda(n)$ no coincide con las e tal que $mcd(e, \lambda(n)) = 1$
 - d) Ninguna de las anteriores

12. La secuencia de punteros (4,6)D (2,3)A (3,3)C en dígitos decimales ha sido generada por un compresor LZ77 con un buffer inicializado con BCBCBDC (más antiguo a la izquierda). La posición del buffer más próxima a los datos por codificar es la número 1. La secuencia que se ha comprimido contiene la cadena:

- a) BDCD
- b) DBAD
- c) BADC
- d) Ninguna de las anteriores

13. Un código de Hamming (7,4) se ha extendido con 1 bit de paridad global para utilizarlo en un canal con una probabilidad de error de bit de 10^{-3} y una probabilidad de borrón de 10^{-3} . La probabilidad p de recibir 1 error y 1 borrón es:

a) $p \geq 0,044 \cdot 10^{-3}$

b) $0,044 \cdot 10^{-3} > p \geq 0,033 \cdot 10^{-3}$

c) $0,033 \cdot 10^{-3} > p \geq 0,022 \cdot 10^{-3}$

d) $0,022 \cdot 10^{-3} > p$

14. A partir de un LFSR de 3 registros se ha generado la secuencia 001110100111010011101, entonces el polinomio de conexiones:

- a) tiene el término D^2 no nulo
- b) tiene el término D no nulo
- c) no existe para esta secuencia
- d) Ninguna de las anteriores

15. El polinomio de conexiones de un LFSR es $D^4 + D + 1$. Indica la FALSA:

- a) La secuencia generada es $D^{11} + D^8 + D^7 + D^5 + D^3 + D^2 + D + 1$
- b) La probabilidad de emitir un 0 es de $7/15$
- c) La secuencia generada tiene ráfagas de cuatro 1's y tres 0's
- d) alguna de las anteriores es falsa

16. Una fuente X emite los símbolos 0 y 1 y se sabe que la $P(0/1)=0.3$ y $P(1/0)=0.7$. Una segunda fuente Y independiente de la primera también emite los símbolos 0 y 1 pero la $P(0/1)=0.4$ y la $P(1/0)=0.6$. La entropía conjunta H es:

- a) $H > 1,95$
- b) $1,95 \geq H > 1,9$
- c) $1,9 \geq H > 1,85$
- d) $1,85 \geq H$

17. Un mensaje de 50 bits se envía por un canal BSC (Binary Symmetric Channel) con probabilidad de error en el bit $p = 10^{-3}$. Se utiliza un código corrector de errores 2-perfecto. Comparando la $p_{e_{bit}}$ (mensaje) sin protegerlo con la $p_{e_{bit}}$ (mensaje) residual de usuario, se ha reducido *aproximadamente* en:
- a) 50 veces
 - b) 505 veces
 - c) 2550 veces
 - d) Ninguna de las anteriores

18. El alfabeto de una fuente consta de 4 símbolos con probabilidades $p(A)=0.2$, $p(B)=0.4$, $p(C)=0.3$, $p(D)=0.1$ y se utiliza un código Huffman binario. La fuente emite un mensaje de 10 símbolos. Se desea aleatorizar el mensaje utilizando un LFSR. El grado mínimo del polinomio de conexiones a utilizar es:

- a) 6
- b) 5
- c) 4
- d) Ninguna de las anteriores

19. ¿Qué diagrama de enrejado puede corresponder con un codificador convolucional de tasa $2/3$ y memoria 2?

- a) Figura A
- b) Figura B
- c) Figura C
- d) Ninguna de las anteriores.

20. Una fuente emite 5 símbolos con las siguientes probabilidades: $p(A)=0.3$, $p(B)=0.15$, $p(C)=0.25$, $p(D)=0.1$, $p(E)=0.2$. Descodifique la secuencia de longitud 3 cuya palabra código es 0.20, si se ha utilizado un codificador aritmético.
- a) ACE
 - b) AAE
 - c) ACC
 - d) Ninguna de las anteriores