ETSETB
Curso 2004-05 Otoño
EXAMEN DE TRANSMISIÓN DE DATOS
20 de enero de 2005

Publicación de notas provisionales: 25/01/04
Fecha límite para las alegaciones: 26/01/05
Publicación de notas definitivas: 27/07/04

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. Indique cuál de las siguientes afirmaciones es FALSA:
   a) Un código binario de repetición Cod(3,1) tiene un subespacio ortogonal de 4 elementos
   b) Existe un código lineal binario 1-perfecto de distancia mínima 3
   c) El código polinómico Cod(7,4) generado por el polinomio $g(D) = D^3 + D^2 + 1$ es un código de Hamming
   d) Alguna de las anteriores es falsa

2. Se dispone de un código (6,3) lineal y sistemático con capacidad correctora de 1 error. Se sabe que las palabras 101011 y 011101 son palabras código. Indíquese la respuesta correcta

   a) Para poder determinar completamente el código es preciso otra palabra código

   b) 111000 es palabra código

   c) 111111 es palabra código

   d) Ninguna de las anteriores

3. Indíquese la respuesta correcta:

   a) La posesión de un certificado emitido por una autoridad de certificación de confianza, garantiza la identidad del poseedor de dicho certificado

   b) La longitud efectiva de clave del algoritmo DES es de 56 bits

   c) El cifrador DES es una red de Feistel de 18 iteraciones

   d) Ninguna de las anteriores

4. Sea un LFSR con un polinomio de conexiones primitivo $C(D) = D^{12} + D^6 + D^4 + D + 1$. El contenido inicial del registro de desplazamiento es $D^2 + D + 1$ ¿Qué afirmación es correcta?

   a) El estado al cabo 502 iteraciones es $D^3 + D^2 + D$

   b) El estado al cabo 4095 iteraciones es $D^2 + D$

   c) $C(D)$ es divisor de $D^{8172} + 1$

   d) Ninguna de las anteriores

5. Para comprimir un mensaje se utiliza un sistema con buffers limitados, de modo que se divide el mensaje en bloques de 2000 símbolos, y se comprime cada uno de los bloques. El mensaje contiene cuatro símbolos independientes A, B, C, D con probabilidades 0.6, 0.2, 0.1, 0.1 respectivamente. ¿Cual será la longitud media mínima de un bloque comprimido?

   a) 3142 bits

   b) 5000 bits

   c) 500 bits

   d) Ninguna de los anteriores

6. Sea un código lineal sistemático (6,3), del que se conocen Y1=011101, Y2=101110, Y3=001011. Si se recibe Z=110101, el decodificador decidirá que el mensaje de usuario transmitido es:

   a) X=110

   b) X=100

   c) X=010

   d) Ninguno de los anteriores

7. Sea un código sistemático (5,2), del que se conocen Y1=01101, Y2=10011, Y3=11111. Puede asegurarse que:

   a) El código es lineal

   b) La distancia mínima es 2

   c) La distancia mínima es 3

   d) Nada de lo anterior puede asegurarse

8. Se construye un canal de transmisión colocando en paralelo 3 canales binarios simétricos de tasas de error 0.1, 0.2 y 0.3 respectivamente. La salida del canal en paralelo se decide por el valor mayoritario a la salida de los canales elementales (ver figura C). La capacidad del canal conjunto es:
NOTA.- La capacidad de una canal binario simétrico con probabilidad de error de bit p, es $C = 1 - [p\,log_2(\frac{1}{p}) + (1-p)log_2(\frac{1}{1-p})]$ *bits/símbolo*

   a) 0.673 bits/simb

   b) 0.482 bits/simb

   c) 0.373 bits/simb

   d) Ninguna de las anteriores

9. Sea $N = pq$, con p y q primos y sea un número a tal que $mcd(a, N) = 1$. Pueda afirmarse que:

   a) $a^N mod N = 1$

   b) $a^{p(q-1)} mod N = a^{(q-1)} mod N$

   c) $a^{p(q-1)} mod N = a \; mod N$

   d) Nada de lo anterior puede afirmarse

10. Para un código binario lineal (5,2) que corrige un error es FALSO que:

   a) Existen al menos dos palabras a distancia 4

   b) Existen al menos dos palabras a distancia 3

   c) Existen al menos dos palabras a distancia 5

   d) Alguna de las anteriores es falsa

11. Para un código lineal binario C (n,k) arbitrario y su correspondiente ortogonal $C^{\perp}$, definido sobre el espacio de las n-plas, E, se puede afirmar que:

   a) $C \cup C^{\perp} = E$

   b) $C \cap C^{\perp} = \{\vec{0}\}$

   c) $dim(C) + dim(C^{\perp}) = n$

   d) Nada de lo anterior puede afirmarse

12. Una fuente binaria markoviana de dos estados y memoria 1, cuyas probabilidades de transición entre estados son de valor 0.2, tiene por entropía un valor H que cumple:

    a) $0.9 < H \leq 1$

    b) $0.8 < H \leq 0.9$

    c) $0.7 < H \leq 0.8$

    d) $H \leq 0.7$

13. De los codificadores continuos convolucionales A y B de tasa 1/3 y memoria 2 que se muestran en las figuras A y B respectivamente, se puede afirmar que:

   a) Es recomendable utilizar el A frente al B en decodificación

   b) A y B son codificadores sistemáticos

   c) Es recomendable utilizar el B frente al A en decodificación

   d) Es indiferente utilizar el A o el B en decodificación

14. Una fuente emite símbolos del alfabeto $\{0, 1\}$ con probabilidades 0.7 y 0.3 respectivamente sobre un canal simétrico cuya probabilidad de error de bit es 1/8. Respecto a la entropía a la salida del canal, es FALSO que :

    a) Está acotada inferiormente por la entropía del error introducido por el canal

    b) Depende de la entropía de la fuente

    c) Es superior a 0.9

    d) Alguna de las anteriores es falsa

15. Sean X e Y dos variables aleatorias discretas con la siguiente función de distribución (probabilidades conjuntas):

$p(X_i, Y_i)$	X_1	X_2	X_3	X_4
Y_1	1/8	1/16	1/32	1/32
Y_2	1/16	1/8	1/32	1/32
Y_3	1/16	1/16	1/16	1/16
Y_4	1/4	0	0	0

La entropía H(X)vale:

a) 1.95 bits/símbolo

b) 1.75 bits/símbolo

c) 1.55 bits/símbolo

d) Ninguna de las anteriores

16. Si $H(Y) = 2$ bits/símbolo, $H(Y|X) = \frac{13}{8}$ bits/símbolo, $H(X)$ =2.5 bits/símbolo, ¿qué afirmación es correcta?

   a) $I(X;Y)$ =3.625 bits/símbolo

   b) $H(X,Y)$ =0.875 bits/símbolo

   c) $H(X|Y)$ =2.875 bits/símbolo

   d) Ninguna de las anteriores

17. Se sabe que un cifrador que trabaja con bloques de 64 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) 6

    c) 7

    d) Ninguno de los anteriores

18. Es cierto que

a) En un cifrado incondicionalmente seguro (Vernam) la entropía del espacio de criptogramas, $H(C)$, puede ser mayor que la entropía del espacio de claves, $H(K)$

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

c) Para una función de Hash de 128 bits, el número de mensajes que colisionan (es decir, que dan un mismo Hash(M)) es inferior a 2^{127}

d) Ninguna de las anteriores

19. Un cifrador bloque binario perfectamente aleatorio puede implementar todas las biyecciones posibles entre su entrada y su salida ¿Cuál es la longitud mínima de clave para que un cifrador bloque binario de 6 bits pueda ser perfectamente aleatorio?

    a) 77 bits

    b) 128 bits

    c) 296 bits

    d) Ninguna de los anteriores.

20. 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 128 bits es, aproximadamente:

    a) 2^{127}

    b) 2^{80}

    c) 2^{64}

    d) Ninguno de los anteriores