1-16 SF

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 alegacion que considere oportunas por escrito en la secretaría de la ETSETB a partir de la publicación de las calificaciones provisionales 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 est norma supondrá la expulsión del examen.

CÓDIGO DE LA PRUEBA: 230 11510 00 0

F 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

a) Código $n=3$: 000, 111 ($k=1$, $r=2$)

$G_{k\times n} = (I_k \mid P_{k\times r}) = (1 \mid 1\ 1)$

$H_{r\times n} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} = (-P^T \mid I_r)$ → Genera subespacio ortogonal $C^\perp$:

$2^r = 4$ elementos: 000, 110, 101, 011 (dimensión $r=2$)

CIERTA

b) P.ej. Código(3,1) de Hamming, 1-perfecto. $d_{min} = 3$. CIERTO

c) Visto en clase. Código cíclico (7,4) sistemático tiene $g(D) = D^3+D^2+1$. Es de Hamming.

D++

n k

2. Se dispone de un código (6,3) lineal y sistemático con capacidad correctora de 1 error. Se sabe que las palabras 101011 y 01110 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

Como es 1 corrector (t=1) $\Rightarrow d_{min} = 3 \Rightarrow$ peso mínimo = 3

$101011 \rightarrow \alpha$

$011101 \rightarrow \beta$

3ª palabra $\rightarrow 100abc \rightarrow \gamma$ (Pongo ésta p. ej.)

Base canónica:

				a=0 ⇒ b=1, c=1	a=1 ⇒ b=0, c=1
$\gamma \rightarrow$	1 0 0	a	b c	0 1 1	1 0 1
$\alpha+\beta+\gamma \rightarrow$	0 1 0	1+a	1+b c	1 0 1	0 1 1
$\alpha+\gamma \rightarrow$	0 0 1	a	1+b 1+c	1 !! 0 0	1 1 0
		almenos 2 unos ($d_{min}=3$)		⇒ 2 (*)	OK

a) Falsa; el código está completamente determinado

b) 111 000 es palabra código ⇒ CORRECTA

c) 111 111 no es palabra código ⇒ FALSA

⇒ (b)

(*) ya que si hay más de 3 unos en total, seguro que la ⊕ de dos palabras códigos (α, β, γ) tiene menos de 3 unos.

F

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 d 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

$p^{(0)}(D) = D^2 + D + 1$
$p^{(1)}(D) = D^3 + D^2 + D$

a) $D^3 + D^2 + D = (D^2 + D + 1) \cdot D \Rightarrow$ Es el estado en la primera iteración $\Rightarrow$ FALSO y $502 < L = 4095$ (no he dado vueltas aún)

b) $L = 2^{12} - 1 = 4095 \Rightarrow$ periodo del LFSR $\Rightarrow$ estado $D^2 + D + 1$

$\Rightarrow$ FALSO

c) $8172 = 4095 + 4077 \Rightarrow$ no es múltiplo del periodo $\Rightarrow$ FALSO

$\Rightarrow$ (d)

$$\underbrace{p^{(0)}(D)}_{1} \cdot D^L \bmod \overset{C(D)}{\uparrow} g(D) = \underbrace{p^{(0)}(D)}_{1}$$

$$D^L \bmod g(D) = 1$$

$$D^{4095} \bmod g(D) = 1$$

$$D^{4095} = g(D) \cdot m(D) + 1 \qquad \begin{array}{cc} D^{4095} & \underline{g(D)} \\ 1 & m(D) \end{array}$$

$$D^{4095} + 1 = g(D) \cdot m(D)$$

$$(D^{4095} + 1)^2 = D^{8190} + 1 = g^2(D) \cdot m^2(D)$$

NO...

F

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. ¿Cuál será la longitud media mínima de un bloque comprimido?

(a) 3142 bits

b) 5000 bits

c) 500 bits

d) Ninguna de los anteriores

$$\bar{\ell}_{\text{SÍMBOLO}} = H = 0'6 \log_2 \frac{1}{0'6} + 0'2 \log_2 \frac{1}{0'2} + 2 \cdot 0'1 \log_2 \frac{1}{0'1} =$$

$$= 0'6 \cdot 0'7369 + 0'2 \cdot 2'3219 + 0'2 \cdot 3'3219 =$$

$$= 1'57 \text{ bits/símbolo}$$

$$\bar{\ell}_{\text{MENSAJE}} = 2000 \text{ [símbolos]} \cdot \bar{\ell}_{\text{SÍMBOLO}} \left[\frac{\text{bits}}{\text{símbolo}}\right] = 3141'9 \text{ bits}$$

$$\bar{\ell}_{\text{mensaje}} = 3142 \text{ bits}$$

$$\bar{\ell} \geq H$$

$$\bar{\ell}_{\min} = H$$

F

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

   a) X=110
   b) X=100
   c) X=010
   d) Ninguno de los anteriores

$Z = 1\,1\,0\,1\,0\,1$

a) $x \Rightarrow 1\,1\,0$

$Y_1 = 0\,1\,1\,1\,0\,1$
$Y_2 = 1\,0\,1\,1\,1\,0$
$\oplus = 1\,1\,0 \;|\; 0\,1\,1 = Y_4 \Rightarrow d(Y_4, Z) = 3$
(1 1 0 = X)

b) $x = 1\,0\,0$

$Y_2 = 1\,0\,1\,1\,1\,0$
$Y_3 = 0\,0\,1\,0\,1\,1$
$\oplus = 1\,0\,0 \;|\; 1\,0\,1 = Y_5 \Rightarrow d(Y_5, Z) = 1 \Rightarrow b$
(1 0 0 = X)

c) $x = 0\,1\,0$

$Y_1 = 0\,1\,1\,1\,0\,1$
$\oplus\; Y_3 = 0\,0\,1\,0\,1\,1$

$Y_6 = 0\,1\,0 \;|\; 1\,1\,0 \qquad d(Y_6, Z) = 3$
(0 1 0 = X)

$Y_7 = 0\,0\,0\;0\,0\,0 \qquad d(Y_7, Z) = 4$

$Y_8 = 1\,1\,1\;0\,0\,0 \qquad d(Y_8, Z) = 3$

$0\,0\,1\,0\,1\,1$
$\oplus\; 1\,0\,0\,1\,0\,1$
$0\,1\,0\,1\,1\,0$
$1\,1\,1\,0\,0\,0$

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

$Y_1 \oplus Y_2 = 01101 \oplus 10011 = 11110 \neq Y_3$

No es un código lineal.

No está determinado!

X	Y
00	00000
01	01101
10	10011
11	11110

3. Indíquese la respuesta correcta:

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

a) Falso, la posesión de un certificado no significa nada por sí misma

b) Cierta

c) No, es de 16 vueltas. Falso

⇒ (b)

D

8. Se construye un canal de transmisión colocando en paralelo 3 canales binarios simétricos de tasas de error 0.1, 0.2 y 0 respectivamente. La salida del canal en paralelo se decide por el valor mayoritario a la salida de los canales elementales (v 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

Hay que hallar la probabilidad de error de bit del nuevo canal.

Prob(error) = prob(2 errores) + prob(3 errores) =

$= 0'1 \cdot 0'2 \cdot (1-0'3) + 0'1 \cdot (1-0'2) \cdot 0'3 +$

$+ (1-0'1) \cdot 0'2 \cdot 0'3 + 0'1 \cdot 0'2 \cdot 0'3 =$

$= 0'098 = p$

$$C = 1 - \left[p \cdot \log_2 \frac{1}{p} + (1-p) \cdot \log_2 \frac{1}{1-p} \right] =$$

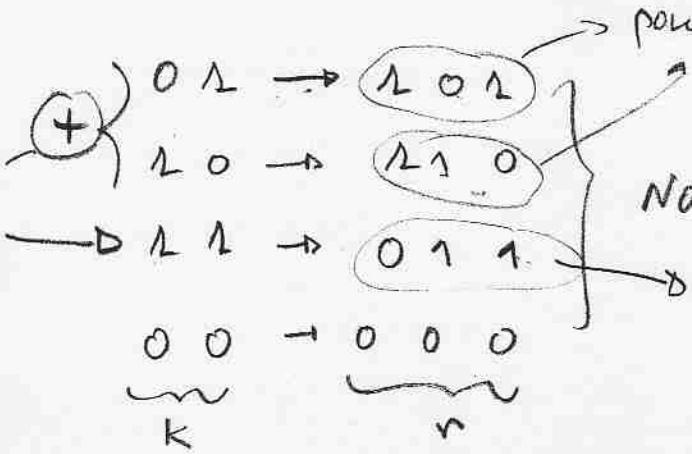
$= 0'5374$ bits/símbol

$= 1 - (0'3284 + 0'1342)$

D+

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



→ pone 2 unos, en cualquier sitio

No existen 2 palabras a distancia 5

si tiene 2 unos ⇒ OK!

Este código sirve.

$e=1 \rightarrow d_{min}=3$

N

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

a) Falso $a^{\phi(N)} \bmod N = 1$

b) $a^{p(q-1)} = a^{(p-1+1)(q-1)} = a^{(p-1)(q-1)+(q-1)} = a^{(p-1)(q-1)} \cdot a^{(q-1)} = a^{(q-1)}$

$\underbrace{a^{(p-1)(q-1)}}_{1}$

OK

$a^{\phi(N)} \bmod N = 1$

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, 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

a) Falso $\text{Card}(C) = 2^k$ $\text{Card}(C^{\perp}) = 2^{n-k}$ $\text{card}(N) = 2^n$

$\Rightarrow$ En la unión de C y $C^{\perp}$ no hay 2^n elementos sino $2^k + 2^{n-k} << 2^n$

b) Falso, pueden existir palabras no nulas ortogonales a sí mismas

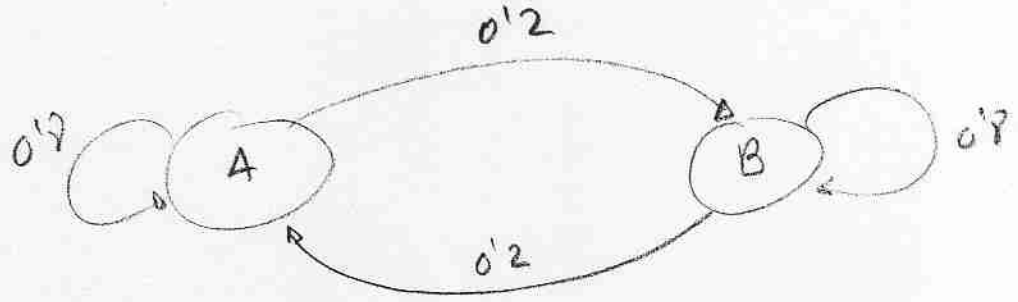
c) Cierto $\dim C = k$; $\dim C^{\perp} = n-k$ $\dim N = n$

$\Rightarrow$ $k + n - k = n$ (OK)!

7

12. Una fuente binaria markoviana de dos estados y memoria 1, cuyas probabilidades de transición entre estados son de valor 0 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) $H \leq 0.7$



Por SIMETRIA entre A y B

$$\left.\begin{array}{l} H(X|A) = H(X|B) \\ p(A) = p(B) \end{array}\right\} H(X) = H(X|A) = H(X|B)$$

$$= p(A|A) \log_2 \frac{1}{p(A|A)} + p(A|B) \log_2 \frac{1}{p(A|B)} =$$

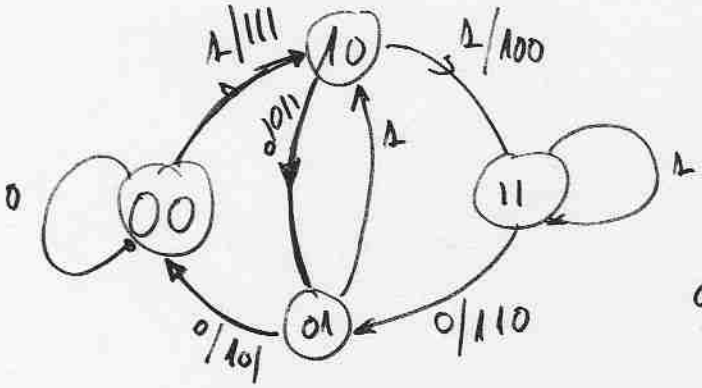
$$= 0'8 \log_2 \frac{1}{0'8} + 0'2 \log_2 \frac{1}{0'2} = 0'722 \text{ bit/simb.}$$

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 respectivament se puede afirmar que:

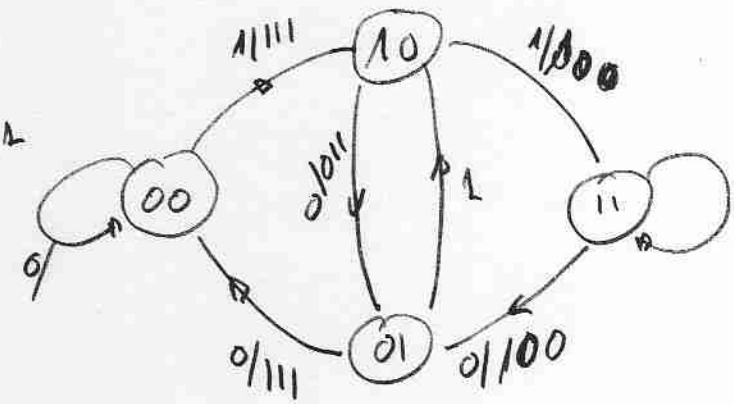
   a) Es recomendable utilizar el A frente al B en decodificación
   b) A y B son codificadores sistemáticos
   c) Es recomendable utilizar el B frente al A en decodificación
   d) Es indiferente utilizar el A o el B en decodificación

Al tener la misma tasa, ~~elegiremos~~ y la misma memoria elegiremos el que tenga mayor distancia libre

A



$d_f = 7$



$d_f = 8$.

B mejor que A

D+

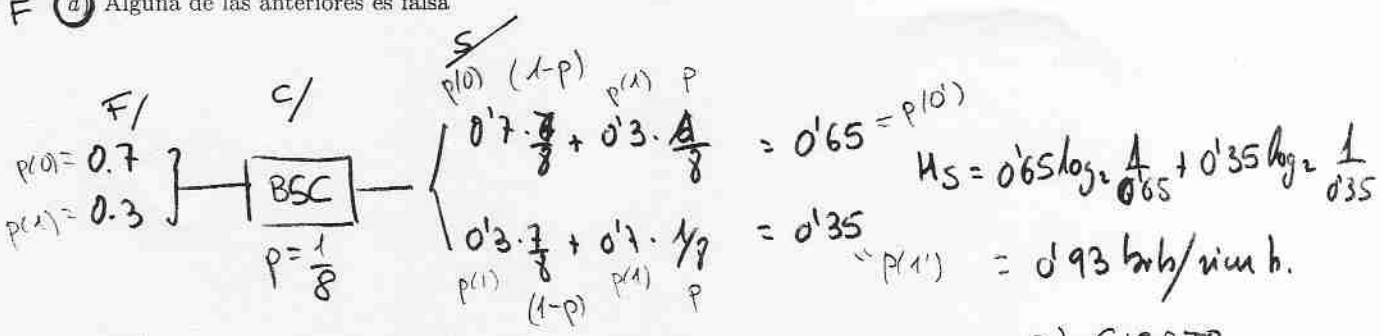
14. Una fuente emite símbolos del alfabeto {0, 1} con probabilidades 0.7 y 0.3 respectivamente sobre un canal simétrico cuya probabilidad de error de bit es 1/8. Respecto a la entropía a la salida del canal, es FALSO que :

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

OK b) Depende de la entropía de la fuente

OK c) Es superior a 0.9

F (d) Alguna de las anteriores es falsa



$H_S = 0'65 \log_2 \frac{1}{0'65} + 0'35 \log_2 \frac{1}{0'35}$

$\approx 0'93$ bits/sim b.

c) CIERTO

a) b)

Gnral:

$H_S \geq \text{Max}(H_F, H_C) = H_C$

0'7, 0'3 → H_F

0,2 → $H_C = 0'54$ bits/sim b.

$H_S \geq H_C$ en este caso.

7/8 1/8 = 1'125

$\approx 0'875$

$\frac{7}{8}\log_2\frac{8}{7} + \frac{1}{8}\log_2 8$ (3)

$H_F = 0'88$ bits/sim b. $= 0'7 \cdot \log_2 \frac{1}{0'7} + 0'3 \cdot \log_2 \frac{1}{0'3}$

17. Se sabe que un cifrador que trabaja con bloques de 64 bits realiza una permutación fija de los mismos. El número mínimo 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

Como test 13/06/2003, pregunta 9 ⇒ $\log_2 64 = 6$

F

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

$$P(x_i) = \sum_{j=1}^{4} P(x_i, y_j)$$

$$P(X_1) = P(X_1, Y_1) + P(X_1, Y_2) + P(X_1, Y_3) + P(X_1, Y_4) =$$
$$= 1/8 + 1/16 + 1/16 + 1/4 = 1/2$$

$$P(X_2) = 1/16 + 1/8 + 1/16 + \phi = 1/4$$

$$P(X_3) = \frac{1}{32} + \frac{1}{32} + \frac{1}{16} + \phi = \frac{1}{8}$$

$$P(X_4) = 1/8$$

$$H(X) = \sum_{i=1}^{4} p(x_i) \cdot \log_2 \frac{1}{p(x_i)} = \frac{1}{2} \cdot \log_2 2 + \frac{1}{4} \cdot \log_2 2^2 + 2 \cdot \frac{1}{8} \cdot \log_2 2^3 =$$

$$= \frac{1}{2} + \frac{1}{2} + \frac{3}{4} = 1'75 \text{ bits/símbolo}$$

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

$$I(X;Y) = H(Y) - H(Y|X)$$

$$H(X,Y) = H(X) + H(Y|X) = H(Y) + H(X|Y)$$

$$I(X;Y) = H(X) + \underbrace{H(Y) - H(X,Y)}_{-H(X|Y)}$$

a) $I(X;Y) = H(Y) - H(Y|X) = 2 - \frac{13}{8} = \frac{3}{8} =$

$= 0'375$ bits/símbolo

b) $H(X,Y) = H(X) + H(Y|X) = 2'5 + \frac{13}{8} =$

$= 4'125$ bits/símbolo

c) $H(X|Y) = \underbrace{H(X) + H(Y|X)}_{H(X,Y)} - H(Y) =$

$= 2'5 + \frac{13}{8} - 2 = 2'125$ bits/símbolo

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

Como test 13/01/04, pregunta 3:

$\sqrt{2^{128}} = 2^{64}$

19. Un cifrador bloque binario perfectamente aleatorio puede implementar todas las biyecciones posibles entre su entrada y su salic ¿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.

Como test 07/01/2003, pregunta 3 ⇒ 6

Longitud clave $\geq \log_2(2^4!) = 296$ bits

18. Es cierto que

a) En un cifrado incondicionalmente seguro (Vernam) la entropía del espacio de criptogramas, $H(C)$, puede ser mayor que l 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)) c inferior a 2^{127}
d) Ninguna de las anteriores

Como test 18/06/2004, pregunta 12