EXAMEN DE TRANSMISIÓN DE DATOS
7 de enero de 2003

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 en la forma y plazo que se anunciará una vez se hagan públicas las calificaciones provisionales.

CÓDIGO DE LA PRUEBA: 230 11510 00 0

Una fuente que emite dos símbolos independientes con probabilidades 0.23 y 0.77 atraviesa un canal binario simétrico. A la salida del canal se observa una entropía de 1 bit/símbolo. ¿Cuánto vale la probabilidad de error del canal?

(a) 0.5
(b) 0.25
(c) 0.125
(d) Ninguna de las anteriores

fuente → A, B $P(A) = 0'23$ $P(B) = 0'77$ → BSC → $H = 1$ bit/símbolo

p

$\emptyset \xrightarrow{1-p} \emptyset$
$1 \xrightarrow{p} 1$

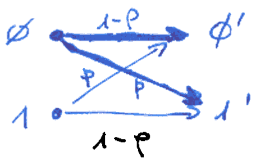
$\Rightarrow P(1) = P(0) = 0'5$

$H\{0,1\} = \log_2 2 = 1$ bit/símbolo

Los 2 símbolos se codifican con algún código fuente:

$A \to \emptyset$ $P(\emptyset) = 0'23$
$B \to 1$ $P(1) = 0'77$

La única manera de conseguir $p(0) = p(1) = 0'5$, es se la p haya sido del 50%

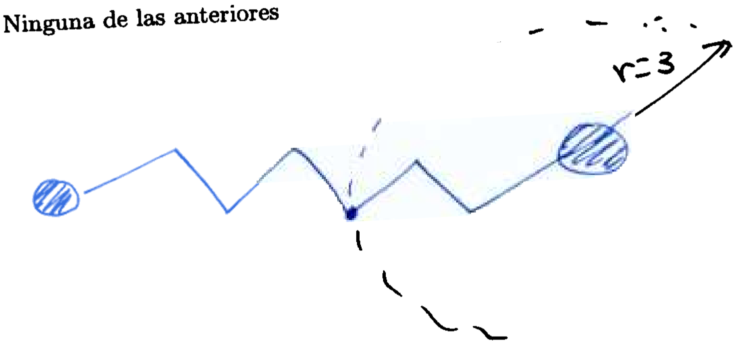


$P(\emptyset') = P(\emptyset)\cdot(1-p) + P(1)\cdot p = 0'23(1-p) + 0'77p$
$\shortparallel$
$0'5$
$\shortparallel$
$P(1') = p(\emptyset)\, p + p(1)\cdot(1-p) = 0'23 \cdot p + 0'77(1-p)$

$\Rightarrow p = 0'5$

2. En un juego de azar se lanzan 23 monedas y la apuesta es hacer un pronóstico sobre los resultados de dichos lanzamientos (ordenados). Un jugador realiza el número mínimo de apuestas que le garantizan tener, al menos, 20 aciertos. ¿Cuál es la probabilidad de que consiga al menos 22 aciertos? *NOTA: Existe un código binario (23,12) que es perfecto y tiene una distancia mínima de 7*

(a) 1/256
(b) 2/256
(c) 3/256
(d) Ninguna de las anteriores



$n=23$
$k=12$
$d_{min}=7 \rightarrow e = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor = 3$

Apostando a todas las palabras código, se consigue que cualquier resultado esté como mucho a distancia 3 de alguna apuesta ($\equiv$ 20 aciertos al menos)

$$\# \text{ apuestas mínimo} = 2^k = 2^{12}$$

- Para acertar 22 o 23 resultados, ha de salir una n-tupla que diste 1 de una palabra código (⇒ 22 aciertos) o una palabra código (⇒ 23 aciertos)

Por tanto, la probabilidad es

$$\frac{2^{12}\cdot 23 + 2^{12}}{2^{23}} = \frac{24\cdot 2^{12}}{2^{23}} = \frac{3\cdot 2^{15}}{2^{23}} = \frac{3}{2^8} = \frac{3}{256}$$

(casos favorables) → numerador
(casos posibles) → denominador

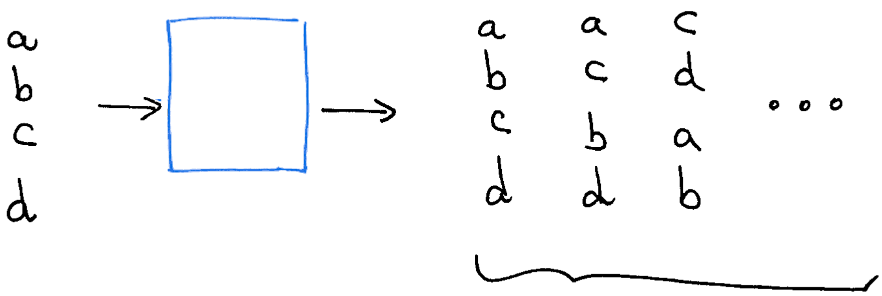
3. Un cifrador bloque binario perfectamente aleatorio puede implementar todas las biyecciones posibles entre su entrada y su salida ¿Cuál es la longitud mínima de clave para que un cifrador bloque binario de 4 bits pueda ser perfectamente aleatorio?

(a) 5 bits

(b) 27 bits

(c) 45 bits

(d) Ninguna de los anteriores.



Hay $(2^4)!$ biyecciones diferentes

La clave debe tener un nº de dígitos suficiente para poderlas diferenciar:

$$2^{\text{long. clave}} \geq 2^4!$$

longitud clave $\geq \log_2(2^4!)$ 44'

45 bits

9. 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

4. Para un código cuya matriz de comprobación es

$$H = \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right) = \left(-P^T \mid I_r\right)$$

puede afirmarse que:

(a) Hay menos de 6 vectores de error distintos no detectables

(b) La capacidad detectora de errores es 1

(c) El codigo es de Hamming

(d) Ninguna de las anteriores

$H(r \times n)$ $\quad r=3$, $n=6$ $\quad k = n - r = 3$

a) $\vec{z} = y + \vec{e}$ Hay tantos errores no detectables como palabras código (excepto $\vec{e} = \vec{\emptyset}$), pues la suma de 2 palabras código otra palabra código.

$2^k - 1 = 8 - 1 = 7$

b) $G(k \times n) = (I_k \mid P) = \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right)$

El Código es:

000 000
001 101
010 011
011 110
100 110
101 011
110 101
111 000

$d_{min} = 3 \Rightarrow e = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor = 1$

$\delta = 2 \cdot e = 2$

c) $e = 1$. Para ser e-perfecto, se ha de cumplir

$2^r = 1 + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{e}$

$e = 1 \Rightarrow 2^r = 1 + n \Rightarrow 2^3 = 8$
$1 + n = 7$

No lo es!

5. Sean n=pq=101*173 y e=(a mod Φ(n)) los parámetros de un sistema RSA bien diseñado. Indicar cuál de las siguientes afirmaciones es cierta:

(a) El criptograma de 3 es 10920 cuando e es igual a 41
(b) e puede valer 43
(c) El mcd(a,Φ(n)) es 1
(d) Ninguna de las anteriores

$e=41$

$C = M^e \bmod N = 3^{41} \bmod 17473$

$41 \equiv 101001 \Rightarrow 3^{41} = ((((3^2)^2 \cdot 3)^2)^2)^2 \cdot 3$

$243^2 = 59049 \bmod 17473 = 6630$

$6630^2 = 43956900$ 〃 $= 12305$

$12305^2 = 151413025$ 〃 $= 9480$

$9480 \cdot 3 = 28440$ 〃 $= \boxed{10967} = C$

Se ha de cumplir que $\text{mcd}(\phi(N), e) = 1$.

$\phi(N) = (p-1)\cdot(q-1) = 100 \cdot 172 = 17200$

$17200 = 43 \cdot 400$!!

$\text{mcd}(\underset{43\cdot 400}{\underset{\shortparallel}{17200}}, 43) = 43 = e \neq 1$

Como $e = a \bmod \phi(N) \Rightarrow a = e + k\cdot\phi(N)$

Los factores en común que tengan a y $\phi(N)$, también los ha de tener e

Como $\text{mcd}(e, \phi(N)) = 1 \Rightarrow \text{mcd}(a, \phi(N)) = 1$

6. En un sistema RSA se tiene $n = pq$ con p y q primos. Se sabe que $33347^2 \equiv 55717^2 \ mod \ n$ ¿Cuál de los siguientes números primos puede ser un valor posible para p?

(a) 1231

(b) 5237

(c) 6761

(d) Ninguno de los anteriores

$$55717^2 - 33347^2 = k \cdot n = k \cdot p \cdot q$$

$$(55717 + 33347) \cdot (55717 - 33347) = k \cdot p \cdot q$$

$$89064 \cdot 22370 = k \cdot p \cdot q$$

$$\left.\begin{array}{l} 89064 = 2^3 \cdot 3^2 \cdot 1237 \\ 22370 = 2 \cdot 5 \cdot 2237 \end{array}\right\} \quad \begin{array}{l} p = 1237 \\ q = 2237 \\ k = 2^4 \cdot 3^2 \ 5 \end{array}$$

También se pueden probar las soluciones, ninguna va:

$p = 1231 \longrightarrow 89064 \cdot 22370 = k \cdot 1231 \cdot q$

$1628'95 = k \cdot q$ //

$p = 5237 \longrightarrow 89064 \cdot 22370 = k \cdot 5237 \cdot q$

$380439'5 = k \cdot q$ //

$p = 6761 \longrightarrow 89064 \cdot 22370 = k \cdot 6761 \cdot q$

$296'59 = k \cdot q$ //

7. Sea un código de comprobación de redundancia cíclica (CRC) definido por el polinomio generador $g(D) = D^{16} + D^{15} + D^2 + 1$ ¿Qué afirmación es cierta?

$\rightarrow r = 16.$

(a) Podría corresponder a un código bloque polinómico Cod(16, 15).

(b) La palabra código asociada al mensaje $1 + D$ es $D^{17} + D^{16} + D^3 + D$

(c) El decodificador resuelve que la palabra recibida $D^{17} + D^{16} + D^3 + D + 1$ no tiene errores

(d) Ninguna de los anteriores

a) En ese caso $r = n - K = 1$

La matriz $g(D)$ tiene grado r !! Por lo que no puede ser

b) $X(D) = 1 + D$

$R(D) = D^r X(D) \bmod g(D) = D^{16} \cdot (1 + D) \bmod g(D)$

$$\begin{array}{l|l} D^{17} + D^{16} & D^{16} + D^{15} + D^2 + 1 \\ \cline{2-2} D^{17} + D^{16} + D^3 + D & D \\ \hline D^3 + D = R(D) & \end{array}$$

$Y(D) = R(D) + D^r \cdot X(D) = D^3 + D + D^{16} \cdot (1 + D) =$

$D^3 + D + D^{16} + D^{17}$ ok!!

c) $Z(D) = D^{17} + D^{16} + D^3 + D + 1$

$S(D) = Z(D) \bmod g(D)$

$$\begin{array}{l|l} + D^{16} + D^3 + D + 1 & D^{16} + D^{15} + D^2 + 1 \\ \cline{2-2} + D^{16} + D^3 + D & D \\ \hline 1 = S(D) & \end{array}$$

Como $S(D) \neq \emptyset \Rightarrow$ Error!

8. Los resultados de un millón de lanzamientos de una moneda se trasmiten de forma fiable por un canal con un ancho de banda de 1500Hz y una S/N de 3 (lineal). Si la transmisión dura 121.97 segundos ¿cuál es el valor mínimo que puede tomar la probabilidad de cara?

   (a) 0.26
   (b) 0.18
   (c) 0.07
   (d) Ninguno de los anteriores

$$C = W \cdot \log_2 (1 + S/N)$$

$$C' = 1500 \cdot \log_2 (1+3) = 3000$$

$$I_{max} = C' \cdot t = 3000 \cdot 121'97 = 365910 \text{ bits}$$

$$H_{max} = I_{max} = 365910 = 0'36591 \text{ bits/símbolo}$$

$p = p(\text{cara})$

$1 - p = p(\text{cruz})$

$$0'36591 = p \cdot \log_2\left(\frac{1}{p}\right) + (1-p) \cdot \log_2\left(\frac{1}{1-p}\right)$$

¿ $p = 0'26$? $\Rightarrow$ $1'0327$

¿ $p = 0'18$? $\Rightarrow$ $0'68$

¿ $p = 0'07$? $\Rightarrow$ $0'365923$ Sí

10. Sea un circuito LFSR utilizado como generador de secuencia aleatorias con polinomio de conexiones $C(D) = D^4+D^3+D^2+D+$ ¿Qué afirmación es cierta?

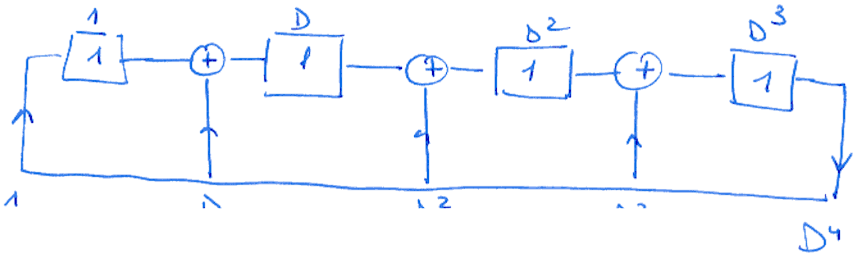
(a) Si el estado inicial es $D^3 + D^2 + D + 1$ el período de la secuencia generada es 5

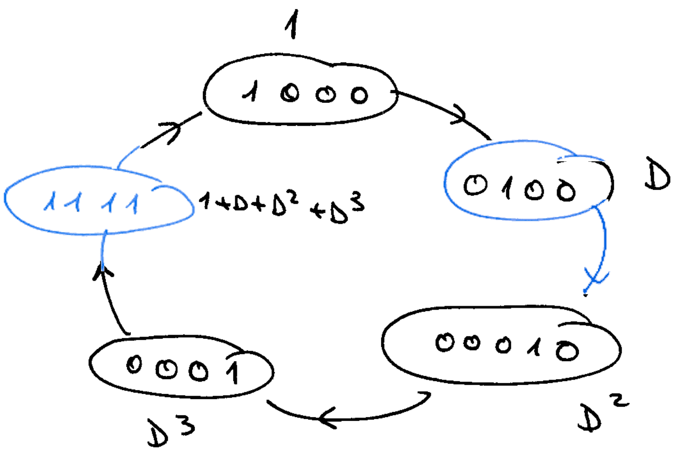
(b) Si el estado inicial es D el período de la secuencia generada es 4

(c) Independientemente del estado inicial, el período de la secuencia generada es 5

(d) Ninguna de los anteriores

a) Es completo $\rightarrow L_{max} = m+1 = 5$ para los estados iniciales del conjunto más grande.





Para las otras 4-tuplas el período es menor

No, es $L_{max} = 5$

No, depende del estado inicial

11. Se realiza la codificación binaria de Huffman de una fuente extendida agrupando símbolos de dos en dos. La fuente elemental carece de memoria y sus símbolos tienen las probabilidades P(A)=0.56; P(B)=0.22 ; P(C)=0.22. Indique cuál de las siguientes afirmaciones es FALSA:

(a) La entropía de la fuente extendida se relaciona proporcionalmente con la entropía de la fuente elemental

(b) La longitud media de la codificación de la fuente extendida es necesariamente mayor que 2

(c) La codificación del símbolo 'AA' requiere de al menos 2 bits

(d) Alguna de las anteriores es falsa

a) $H(F^2) = 2 \cdot H(F)$

b) $H(F) = \dfrac{}{\log_{10} 2}\left(0'56 \log 0'56 + 2 \cdot 0'22 \cdot \log 0'22\right) = 1'43$

$H(F^2) = 2'85$ bits/símbolo $\leq L$ ok!

c) Cod ('AA') > 2 bits por construcción de Huffman

Para que tenga 1 bit, $P(\text{'AA'}) \geq \frac{1}{3}$

$P(\text{'AA'}) = (P(A))^2 = 0'31 < \frac{1}{3}$

Por lo tanto, al menos tiene 2 bits ok!

12. Indique cuál de las siguientes afirmaciones es FALSA:

(a) En el cifrado de César (monoalfabético) la operación de cifrado y descifrado es la misma

(b) La verificabilidad de un mensaje garantiza su integridad

(c) El algoritmo DES se basa en técnicas de trasposición y sustitución

(d) Alguna de las anteriores es falsa

a) La operación de cifrado de César es:

$$C = (M + 3) \bmod n$$

La operación de descifrado de César es

$$M = (C \quad 3) \bmod n$$

Son distintas!

b) Por construcción, un mensaje verificable mantiene su integridad

c) El DES es un cifrador basado en permutaciones y sustituciones en las S-Cajas

d) No aplica

13. Para un adecuado diseño de un cifrador en flujo basado en un LFSR con una función no lineal, es FALSO que:

(a) La secuencia cifrante debe presentar un comportamiento suficientemente aleatorio

(b) El LFSR debe tener un polinomio de conexiones primitivo de grado igual o superior a la longitud del mensaje a cifrar

(c) La secuencia cifrante debe presentar una complejidad lineal alta para garantizar su impredictibilidad

(d) Alguna de las anteriores es falsa

b) El período de la secuencia cifrante

no el polinomio de conexiones)

es el factor de diseño de un

cifrador en flujo

14. Para un código binario de repetición Cod(5,1) sistemático, ¿cuál de las siguientes afirmaciones es FALSA?

(a) La palabra 11001 tiene por síndrome 0110

(b) Todos los vectores de error e_1 y e_2 que verifican: $e_1 + e_2 = 11111$ tienen el mismo síndrome

(c) Este código puede corregir siempre hasta cuatro borrones (o borrados)

(d) Alguna de las anteriores es falsa

$$k=1 \qquad n=5$$

$$1 \longrightarrow 1 \vdots 1111$$

$$G_{(k \times n)} = \big(1 \vdots \underbrace{1\,1\;\;1\,1}_{P} \big) = (I_k \quad P)$$

$$H^T_{(n \times r)} = \begin{pmatrix} P \\ \cdots \\ I_k \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

a) $s = z \cdot H = (1\,1\,0\,0\,1) \cdot H^T = 0110$ ok

b) $(\vec{e_1} + \vec{e_2}) \cdot H^T = (1\,1\,1\,1\,1)\, H^T = (0\,0\,0\,0)$

$$\vec{e_1}\, H^T + \vec{e_2} \cdot H^T = 0000$$

$$\underbrace{\vec{e_1} \cdot H^T}_{s_1} = \underbrace{\vec{e_2} \cdot H^T}_{s_2} \qquad \text{ok!}$$

c) $d_{min} = 5 \Rightarrow \rho = d_{min} - 1 = 4$ ok!

15. Sea un LFSR realimentado por un polinomio primitivo de grado 10. Si el estado incial es $S(D) = D^4 + D^6 + D^8$, el estado al cabo de 2043 iteraciones es:

(a) $D^2 + D^5 + D^9$

(b) $D + D^3 + D^9$

(c) $D + D^7 + D^9$

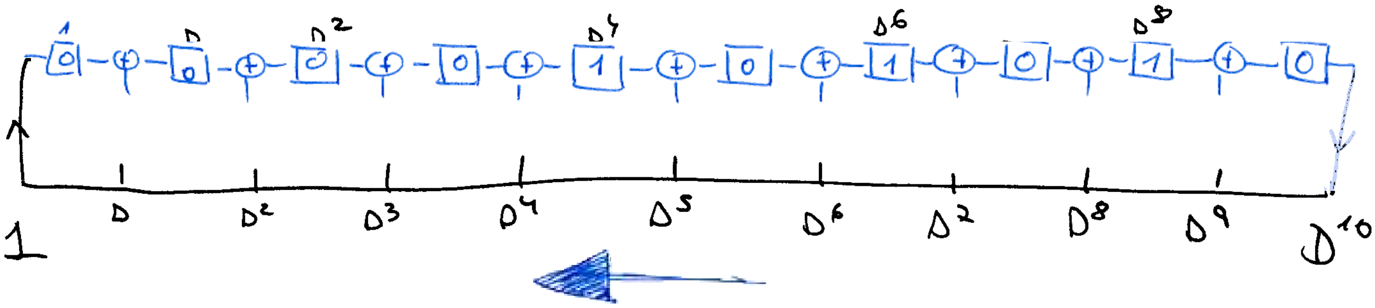
(d) Ninguna de las anteriores

$L = 2^{10} - 1 = 1023$

$2043 \bmod 1023 = 1020$

$p^{(1020)}(D) = p^{(-3)}$

$p^{(1023)}(D) = p^{(0)}(D)$



Tiro hacia atrás 3 estados:

0 1 0 1 0 1 0 0 0 0 $\equiv D + D^3 + D^5$

1 D D^3 D^5

16. Se transmiten 10^3 símbolos de fuente en un tiempo de 10 s por un canal con $v_t = 10^3$ bps. La fuente consta de 256 carácteres y se utiliza codificación de canal mediante un código bloque binario lineal 1-perfecto con redundancia r=4. ¿Cual es la entropía máxima de la fuente?

(a) 8 bits/símbolo

(b) 7.33 bits/simbólo

(c) 13.64 bits/símbolo

(d) Ninguna de las anteriores

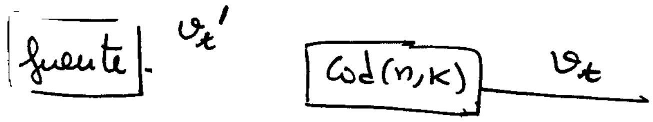
bits transmitidos $= 10^3 \frac{\text{bits}}{\text{seg}} \cdot 10 \text{ seg} = 10^4$ bits emitidos al canal.

Código 1-perfecto $\Rightarrow 2^r = 1 + \binom{n}{1} = 1 + n$

$\llcorner_{e=1}$

$r = 4 \Rightarrow n = 15 \Rightarrow k = 11$

Código (15, 11)



v transmisión de fuente ($\text{símbolos fuente}/\text{seg}$)

v transmisión al canal (bits/seg)

$v_t' = v_t \cdot \frac{k}{n}$

$v_t = 10^3 \frac{\text{bits}}{\text{seg}} \cdot \frac{11}{15} = 733'33 \frac{\text{bits}}{\text{seg}}$ efectiva de usuario.

La fuente emite $733'33 \frac{\text{bits}}{\text{seg}} \cdot 10 \text{ seg} = 7333'33$ bits

La fuente emite 10^3 símbolos

$H_{max} = \frac{7333'33}{10^3} \frac{\text{bits}}{\text{símbolo}} = 7'33$ bits/símbolo

18. Se emplea un método de cifrado en bloque consistente en sumar XOR bit a bit el mensaje con la clave. Para $k = 10101010$ y un tamaño de bloque de 8 bits, codifique el mensaje $M = 1111111100000000$ en modo CBC. Suponga que $C_{-1} = 00000000$

(a) $C = 0101010100000000$
(b) $C = 0101010111111111$
(c) $C = 0101010110101010$
(d) Ninguna de las anteriores

1 1 1 1 1 1 1 1 | 0 0 0 0 0 0 0 0
⊕ 1 0 1 0 1 0 1 0 | 1 0 1 0 1 0 1 0 (*)

$\boxed{0\,1\,0\,1\,0\,1\,0\,1}$ | 1 0 1 0 1 0 1 0
⊕ 0 1 0 1 0 1 0 1

$\boxed{1\,1\,1\,1\,1\,1\,1\,1}$

C = 0 1 0 1 0 1 0 1 1 1 1 1 1 1 1 1

(*) La clave se va repitiendo lo que haga falta para cubrir todo el mensaje

17. Sea un sistema RSA en que todos los usuarios usan como exponente de cifrado e. Sea $Pca = (Nca)$ y $Sca = (dca)$ respectivamente las clave pública y privada de una tercera parte de confianza, y sea un usuario A con un identificador $ID_A, Pa = Na$ y $Sa = da$ ¿Cuál de los siguientes documentos permite demostrar ante terceras partes que el usuario A posee la clave pública Pa? *NOTA: H(.) es una funcion de hash y el símbolo "|" denota la concatenación binaria de los campos del mensaje.*

(a) $ID_A|Na|((H(ID_A|Na))^{da})mod_{Na}$
(b) $ID_A|Na|((H(ID_A|Na))^{dca})mod_{Nca}$
(c) $ID_A|Na|((H(ID_A|Na))^{e})mod_{Nca}$
(d) Ninguna de las anteriores

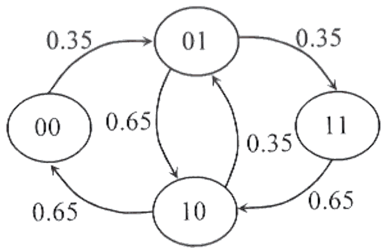
19. Una fuente de símbolos binarios está modelada estadísticamente con la cadena de Markov representada en la figura, donde cada estado representa los dos últimos simbolos binarios emitidos (el más antiguo a la izquierda) y cada transición representa la emisión de un único símbolo binario. Se puede afirmar que:

(a) La memoria es de orden 2

(b) No tiene memoria

(c) La memoria es de orden 1

(d) Ninguna de las anteriores



NOTA: Solo están dibujadas las probabilidades de transición

Desde cada estado va al siguiente
con probabilidades simétricas

Planteando las ecuaciones de transición,
se ven simétricas

La probabilidad de (estando en un estado)
r al siguiente $\binom{0}{1}$, es siempre igual.

Por inspección se ve que no hay memoria

20. Sea una fuente binaria que emite dos símbolos independientes con probabilidades 0.65 y 0.35. Se puede afirmar que:

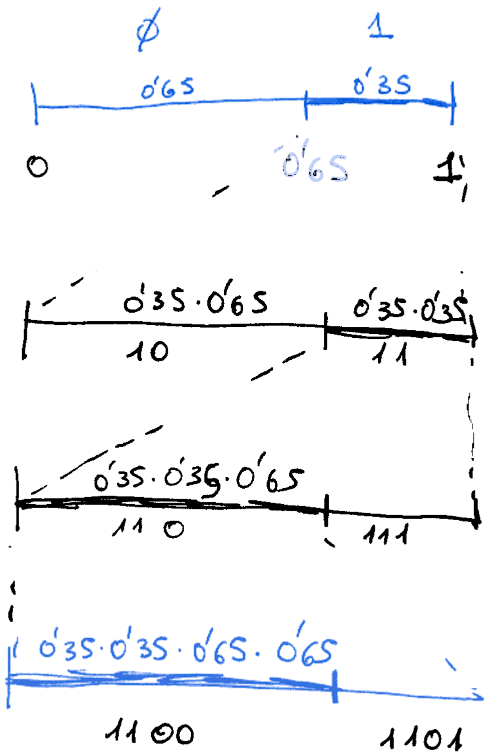
(a) La entropía es superior a 1.85 bits/símbolo

(b) El número real que codifica aritméticamente a 1100 se encuentra en un intervalo de longitud inferior a 0.052

(c) Con agrupaciones de 2 símbolos binarios es posible conseguir una eficiencia unitaria

(d) Ninguna de las anteriores

$H(F) = 0'93$ bits/símbolo No!



Nota si la asignación se hace al revés,

$p(\phi) = 0'35$

$p(1) = 0'65$

sale lo mismo:

$0'65 \cdot 0'65 \cdot 0'35 \cdot 0'35$

$0'35 \cdot 0'35 \quad 0'65 \cdot 0'65 = 0'05175 < 0'052$ OK!

c)

	prob.
00	$0'65 \cdot 0'65$
01	$0'65 \cdot 0'35$
10	$0'35 \cdot 0'65$
⋮	$0'35 \cdot 0'35$

Como no son de la forma $\frac{1}{2^{algo}}$, no va a salir $E = 1$.

$E = \frac{\bar{L}}{H}$