Test.

ETSETB

Curso 2002-03 Primavera

EXAMEN DE TRANSMISIÓN DE DATOS

13 de junio de 2003

F → fácil
N → normal
D → difícil

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

F

grado = r = 5   grado 4

1. 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) $e(D) = D^{14} + D^{13} + D^{12} + D^{11}$ $\rightarrow l = 4 = j - i + 1 \Rightarrow j - i = 3$ l = longitud ráfaga

   (b) $e(D) = D^{13} + D^2 = D^2(1 + D^{13-2})$

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

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

a) Si $\underset{3}{j-i} < \underset{5}{r} \Rightarrow$ Se detectan todas las ráfagas de longitud $= j-i+1 = 4$ menor que $r = 5$. OK.

b) Se detectan todos los errores dobles con separación

$j - i = 13 - 2 = 11$ $j - i < 2^m - 1 = 15$

$11 < 15 \Rightarrow$ OK, se detectan siempre. m = grado $p(D) = 4$

c) Número impar de errores $\Rightarrow e(D=1) = 1$

No se detectarían si $e(D) = g(D) \cdot m(D) = (D+1) \cdot p(D) \cdot m(D)$
otro cualquiera

¡Pero entonces $e(D=1) = \emptyset$!

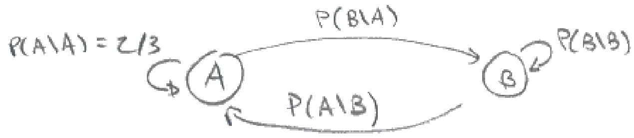
$\Rightarrow$ Se detectan siempre.

F

2. 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) 0.6372 bits inf/simb
   (b) 0.7394 bits inf/simb
   (c) 0.9181 bits inf/simb
   (d) Ninguna de las anteriores

$P(B) = 1 - P(A) = \frac{2}{3}$



$$\underset{1/3}{P(A)} = \underset{2/3}{P(A\backslash A)} \cdot \underset{1/3}{P(A)} + P(A\backslash B) \cdot \underset{2/3}{P(B)} \Rightarrow P(A\backslash B) = 1/6$$

$$\Rightarrow P(B\backslash B) = 5/6$$

$$H(F) = \underset{1/3}{P(A)} \cdot H(F\backslash A) + \underset{2/3}{P(B)} \cdot H(F\backslash B)$$

$$H(F\backslash A) = \underset{2/3}{P(A\backslash A)} \cdot \log_2 \frac{1}{P(A\backslash A)} + \underset{1/3}{P(B\backslash A)} \cdot \log_2 \frac{1}{P(B\backslash A)} = 0'91829$$

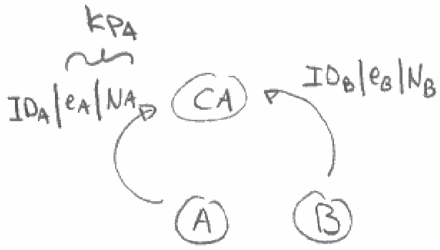
$$H(F\backslash B) = \underset{1/6}{P(A\backslash B)} \cdot \log_2 \frac{1}{P(A\backslash B)} + \underset{5/6}{P(B\backslash B)} \cdot \log_2 \frac{1}{P(B\backslash B)} = 0'6500$$

$H(F) = 0'7394$ bits/símbolo

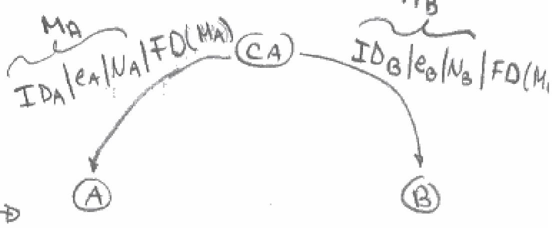
F

3. Para verificar un certificado digital necesitamos:

   (a) La clave pública de la Autoridad de Certificación
   (b) La clave privada de la Autoridad de Certificación
   (c) La clave pública del posesor del certificado
   (d) Ninguna de las anteriores

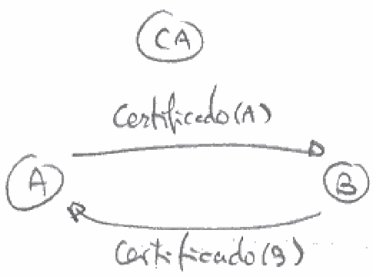


Los usuarios envían sus certificados en claro a la CA.

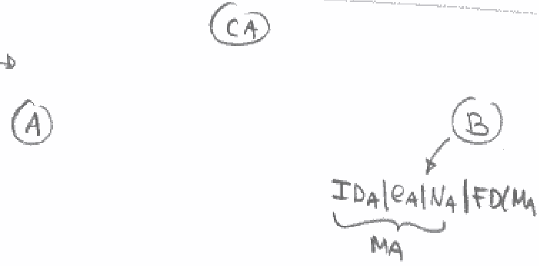


La CA les devuelve los certificados firmados con su d_{CA}:

$$FD(M_A) = H(M_A)^{d_{CA}} \bmod N_{CA}$$



A y B intercambian sus certificados digitales.



- B lee ID_A y $K_{P_A} = (e_A, N_A)$
- B averigua $H(M_A)$:

a) $\rightarrow H(M_A) = FD(M_A)^{e_{CA}} \bmod N_{CA}$

- B recalcula $H(M_A)$ y si coincide B autentica K_{P_A}.
- A hace lo mismo con la K_{P_B}.

F

4. 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) No es posible corregir ese borrón
   (b) El código ISBN correcto es 0792893910. $\Rightarrow x = 8$
   (c) El valor correcto del borrón es 4
   (d) Ninguna de las anteriores $\Rightarrow x = 3$

El código ISBN tiene capacidad correctora de borrones $e = 1$ = capacidad detectora de errores $= \delta$.

No corrige ningún error $(e = \emptyset)$.

$$S = z \cdot H^T = \emptyset$$

$$S = (0792x93910) \cdot \begin{pmatrix} 10 \\ 9 \\ 8 \\ 7 \\ 6 \\ 5 \\ 4 \\ 3 \\ 2 \\ 1 \end{pmatrix} = 235 + 6x \equiv \emptyset \mod 11.$$

$\mathbb{Z}_{11} \Rightarrow \{0,1,2,3,4,5,6,7,8,9,X\}$

$(235 + 6x) \mod 11 = \emptyset$

¿$235 + 6x = 242$? $\Rightarrow 6x = 7$. No

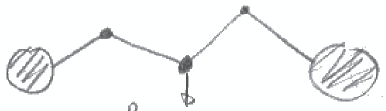
¿$235 + 6x = 253$? $\Rightarrow 6x = 18$

$$\boxed{x = 3}$$

N

5. 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 1-perfecto
(b) El código es 2-perfecto
(c) El código es 4-perfecto
(d) Nada de lo anterior puede afirmarse



¡CORRIGE 2 errores con probabilidad 50%!

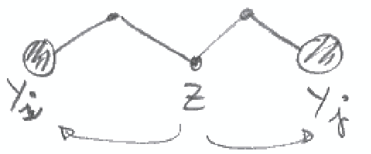
$d_{min} = 4 \Rightarrow e = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor = 1$

e-perfecto $\Rightarrow 2^r = 1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{e} \Rightarrow$ Corrige hasta e errores y NINGUNO MÁS NUNCA.

1-perfecto (Hamming) $\Rightarrow 2^r = 1 + n$

Si acaso, sería 1-perfecto (pues $e=1$).
Pero vemos que sí que a veces (50% de las veces) corregirá 2 errores!

$\Rightarrow$ No puede ser.



¡equidistan!

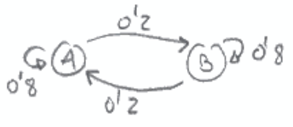
- Si envié Y_i y recibo Z, el 50% de las veces estimo que envié Y_i (OK) y el 50% estimo que envié Y_j (Error).

D

6. 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) 1 bit información/símbolo
   (b) 0.7203 bits información/símbolo
   (c) 0.9044 bits información/símbolo
   (d) Ninguna de los anteriores

$$\boxed{\text{Fuente}} \xrightarrow{\{A, B\}} \boxed{\text{Canal}}_{p=0.2} \longrightarrow ¿H_s(F')?$$



$$\Rightarrow \; p(A) = p(A|A)\cdot p(A) + p(A|B)\cdot p(B)$$

$$\left.\begin{array}{l} 0'2 \cdot p(A) = 0'2 \cdot p(B) \\ p(A) + p(B) = 1 \end{array}\right\} \Rightarrow \left[\, p(A) = p(B) = \frac{1}{2} \,\right]$$

$$H_s(F') = H_s(F'|A)\cdot \underset{0'5}{p(A)} + H_s(F'|B)\cdot \underset{0'5}{p(B)}$$

$$H_s(F'|A) = P_s(A|A)\cdot \log_2 \frac{1}{P_s(A|A)} + P_s(B|A)\cdot \log_2 \frac{1}{P_s(B|A)}$$

$$H_s(F'|B) = P_s(A|B)\cdot \log_2 \frac{1}{P_s(A|B)} + P_s(B|B)\cdot \log_2 \frac{1}{P_s(B|B)}$$

$$P_s(A|A) = p(A|A)\cdot(1-p) + p(B|A)\cdot p = 0'8\cdot 0'8 + 0'2\cdot 0'2 = 0'68$$

$$P_s(B|A) = 1 - P_s(A|A) = 0'32$$

$$P_s(B|B) = p(A|B)\cdot p + p(B|B)\cdot(1-p) = 0'68$$

$$P_s(A|B) = 1 - P_s(B|B) = 0'32$$

$$\begin{array}{l} H_s(F'|A) = 0'90438 \\ H_s(F'|B) = 0'90438 \end{array} \Rightarrow \left[\, H_s(F') = 0'9044 \,\right]$$

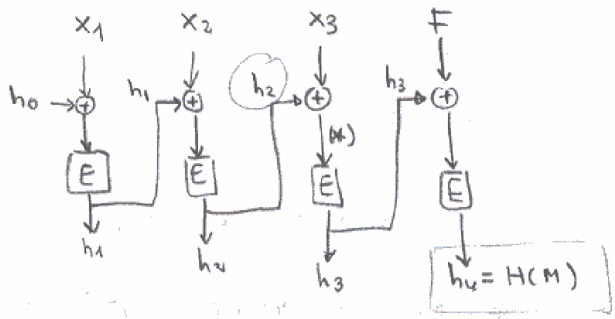
ERROR si no se contempla memoria: $P_s(A) = p(A)\cdot(1-p) + p(B)\cdot p = 0'5$

$P_s(B) = 0'5$

$H_s(F') = 1$ bit/símbolo

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



$h_i \in \{0, 1 ... F\}$

- El hash de FFFF tiene un determinado valor de h_3.
- $(*) \rightarrow \boxed{E} \rightarrow h_3$ $\Rightarrow$ tiene un determinado valor de (*).
- $\forall$ h_2, sé qué valor X_3 hará que obtenga ese valor (*).
  $h_2 \oplus X_3 = (*)$
- He de calcular cuántos $X_1 X_2$ hay $\Rightarrow$ fijarán h_2 $\Rightarrow$ fijarán X_3.

$\Rightarrow$ Elección libre de X_1 y X_2 $\Rightarrow$ Valor fijado de X_3.

$16 \cdot 16 = 256$

F

$\to m=4$

8. 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) El estado al cabo de 58 iteraciones es $D^2 + D^3$

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

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

(d) Ninguna de las anteriores.

a) $L = 2^m - 1 = 15$

$58 \bmod 15 = 13 \Rightarrow p^{(58)}(D) = p^{(13)}(D)$;; $p^{(15)}(D) = p^{(0)}(D)$

$(58+2) \bmod 15 = \phi$

$p^{(58)}(D) = p^{(-2)}(D)$ $\to$ Retrocedo 2 estados: $p^{(0)}(D) = D$

una de las 2.
$$\begin{cases} D\cdot p^{(-1)}(D) = C(D)\cdot 1 + p^{(0)}(D) = 1+D+D^4+D = 1+D^4 \to \text{No!} \\ D\cdot p^{(-1)}(D) = C(D)\cdot \phi + p^{(0)}(D) = D \Rightarrow p^{(-1)}(D) = 1 \to \text{OK.} \end{cases}$$

$$\begin{cases} D\cdot p^{(-2)}(D) = C(D)\cdot 1 + p^{(-1)}(D) = 1+D+D^4+1 = D+D^4 \Rightarrow \boxed{p^{(-2)}(D) = 1+D^3} \\ D\cdot p^{(-2)}(D) = C(D)\cdot\phi + p^{(-1)}(D) \to \text{No!} \end{cases}$$

b) $D^L \bmod C(D) = 1$

$D^{15} \bmod C(D) = 1$

$D^{15} \,\underline{|\, C(D)}$
$1 \quad Q(D)$

$D^{15} = C(D)\cdot Q(D) + 1$

$D^{15} + 1 = C(D)\cdot Q(D)$

$(D^{15}+1)^3 = D^{45}+1 = C^3(D)\cdot Q^3(D)$

$\Rightarrow C(D)$ es divisor de $D^{45}+1$. (lo más parecido ...)

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

$p^{(1)}(D) = D^2$

$p^{(2)}(D) = D^3$

$p^{(3)}(D) = D^4 \bmod D^4+D+1 = D+1$

$p^{(4)}(D) = (D^2+D) \bmod D^4+D+1 = D^2+D$

$p^{(5)}(D) = D^3+D^2$ $\quad$ '' $\quad = D^3+D^2$

$\boxed{p^{(6)}(D) = D^4+D^3 \bmod \text{''} = D^3+D+1}$

D

$\boxed{k=8}$

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

   (a) 3
   (b) 5
   (c) 7
   (d) Ninguno de los anteriores

$\log_2 8 = 3$ //

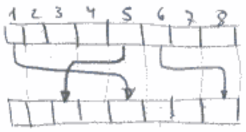
1er mensaje →	0	0	0	0	1	1	1	1
2º mensaje →	0	0	1	1	0	0	1	1
3er mensaje →	0	1	0	1	0	1	0	1

} Con 3 parejas texto claro – texto cifrado, hay suficiente.

– Coloco en columnas todas las 8 ternas!

– Si cifro cada una de las 3 filas, los bits habrán ido a otra posición.

– Lo mismo pasa para cada fila.



– Colocando las tres filas cifradas una encima de la otra, veremos dónde ha ido cada columna:

0	0	0	0	1	1	1	1
0	0	1	1	0	0	1	1
0	1	0	1	0	1	0	1

Podré identificar cuál es la permutación fija que se ha aplicado.

Error → 7 parejas ⇒ 10000000
01000000
00100000
⋮
00000010
7 parejas texto claro → texto cifrado

¡No hace falta!
Con 3 es suficiente

(la última no hace falta: es obvio dónde fue.

F

10. Sea un código de Hamming $\boxed{\text{sistemático}}$ 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 = 0011
(b) X = 0100
(c) X = 0111
(d) X = Ninguno de los anteriores

$H(r \times n) \Rightarrow r = 3$ filas ; $n = 7$ columnas $\Rightarrow k = n - r = 4$

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

$I_r = I_3$ ¡falta!

$$\Rightarrow H = \left(\begin{array}{cccc|ccc} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right)$$

$Y = 0000000 \Rightarrow z = 0111100$

$$s = z \cdot H^T = (0111100) \cdot \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (1\,1\,0) = 2^a \text{ fila } H^T$$

$\Downarrow$

$e = 0100000$

$$\hat{Y} = z + e = \underbrace{0011}_{k=4}100 \Rightarrow \boxed{\hat{X} = 0011}$$

N

11. 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 para un código $2 - perfecto$ en detección:

(a) ~~El número de síndromes debe ser mayor o igual que 16~~ Código paridad par $\overset{n}{(3},\overset{k}{2})$ es 2-perf. en detec.

(b) ~~La redundancia debe ser mayor que 3~~ Código repet. $(3,1)$ es 1 perf. en detec.

(c) ~~Las palabras código son equidisantes~~ Código paridad par $(4,3)$ es 1 perf. en detecc.

(d) Ninguna de las anteriores

a)

X		Y
00		000
01	$\Rightarrow$	011
10		101
11		110

$d_{min} = 2 \rightarrow \delta = 1$

No detecta 2 errores!

No es 2-perfecto en detección

Es 1-perfecto en detección

b)

X	Y
0	000
1	111

$d_{min} = 3 \rightarrow \delta = 2$

Detecta 1, 2 errors.

No detecta 3 errors.

Es 2-perfecto en detección

c)

X	Y
000	0000
001	0011
010	0101
011	0110
100	1001
101	1010
110	1100
111	1111
$\longleftrightarrow$ $k=3$	$\longleftrightarrow$ $n=4$

$d_{min} = 2 \rightarrow \delta = 1 \rightarrow$ detecta 1 error.

¿Nunca detecta 2 errors?

No.

$m=4$

$r=4$

D

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) 17/465
(b) 16/465
(c) 13/465
(d) Ninguna de las anteriores

errores dobles $\Rightarrow e(D) = D^i + D^j = D^i \cdot (1 + D^{j-i}) = D^i \cdot (1+D^\lambda)$

$g(D) = D^4 + D + 1$ $\qquad \lambda = j - i$

- Esos errores dobles se detectan si $e(D) \neq g(D) \cdot Q(D)$ ↳ otro cualquiera.

- $g(D)$ es primitivo $\Rightarrow$ No divide a $D^\lambda + 1$, $m \leq \lambda < L = 2^m - 1 = 15$

$\lambda = m, m+1 \ldots L-1$

$\lambda = 4, 5, 6, \ldots 14$

- Esos errores **no** se detectan en caso contrario:

$e(D) = D^i \cdot (1 + D^{15})$, $\quad 0 \leq i \leq 15$

$\lambda = 15 = j - i$

$i=0 \rightarrow e(D) = 1 + D^{15}$
$i=1 \rightarrow e(D) = D + D^{16}$
$i=2 \rightarrow e(D) = D^2 + D^{17}$
$\vdots$
$i=15 \rightarrow e(D) = D^{15} + D^{30}$

$\rightarrow$ Hay 16 casos favorables, sobre $\binom{31}{2} = 465$ casos posibles.

OJO: En este caso, hay otro error no detectable:

$e(D) = (1 + D^{15})^2 = 1 + D^{30}$

$\Rightarrow \boxed{\dfrac{17}{465}}$

F

13. 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) ADADDADADDAD

(b) ADADDAADD

(c) ADDAADDDAA

(d) Ninguno de los anteriores

000	A
001	B
010	C
011	D
100	AD
101	DA
110	ADD
111	DAA

000	011	100	101	110
↓	↓	↓	↓	↓
A	D	AD	DA	ADD

100 AD, 101 DA, 110 ADD, 111 DAA

F

14. Para una clave pública del algoritmo RSA de valor $n = pq = 23 * 59 = 1357$ y $e = 17$, es verdadero que:

(a) La clave secreta tiene por valor $d = 1200$

(b) El cifrado del mensaje $m = 59$ tiene por criptograma $c = 354$

(c) Para un mensaje M cuyo hash o resumen es $h(M) = 236$ la firma será $(M|118)$

(d) Ninguna de las anteriores

a) $e \cdot d = 1 + K \cdot \phi(N) \longrightarrow 17 \cdot d = 1 + K \cdot 1276 \longrightarrow d = \dfrac{1276K + 1}{17}$

$\phi(N) = (p-1) \cdot (q-1) = 22 \cdot 58 = 1276$

$d = \dfrac{(75 \cdot 17 + 1)K + 1}{17} = 75 \cdot K + \dfrac{K+1}{17}$

$K = 16 \rightarrow \boxed{d = 1201}$

b) $C = M^e \bmod N = 59^{17} \bmod 1357$

$17 \equiv 10001 \Rightarrow 59^{17} = \left(\left(\left(59^2\right)^2\right)^2\right)^2 \cdot 59$

$59^2 = 3481 \xrightarrow{\bmod 1357} 767$

$767^2 = 588289 \longrightarrow 708$

$708^2 = 501264 \longrightarrow 531$

$531^2 = 281961 \longrightarrow 1062$

$1062 \cdot 59 = 62658 \longrightarrow \boxed{236}$

c) $FD = H(M)^d \bmod N$

$H(M) = FD^e \bmod N = 118^{17} \bmod 1357 \underset{6}{=} \boxed{767 \neq 236}$

$118^2 = 13924 \longrightarrow 354$

$354^2 = 125316 \longrightarrow 492$

$492^2 = 242064 \longrightarrow 236$

$236^2 = 55696 \longrightarrow 59$

$59 \cdot 59 = 3481 \longrightarrow 767$

F

15. Indique cuál de los siguientes polinomios es primitivo:

(a) $D^6 + D^2 + 1$
(b) $D^6 + D^3 + D + 1$
(c) $D^6 + D + 1$
(d) $D^6 + D^5 + D^4 + D^3 + D^2 + D + 1$

a)
$$
\begin{array}{l|l}
D^6 + D^2 + 1 & D^3 + D + 1 \\
\cline{2-2}
D^6 + D^4 + D^3 & D^3 + D + 1 \\
\cline{1-1}
D^4 + D^3 + D^2 + 1 & \\
D^4 \quad + D^2 + D & \\
\cline{1-1}
D^3 + D + 1 & \\
D^3 + D + 1 & \\
\cline{1-1}
\emptyset &
\end{array}
$$

Es reducible, divisible por D^3+D+1.

b) Tiene un nº par de términos ⇒ es divisible por $D+1$.

d) Es completo → No es primitivo.
$m \neq 2$

c) Por descarte, este es primitivo.

N

$r=4$

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

   (a) El código es capaz de detectar cualquier número impar de errores
   (b) Es un código 2-perfecto
   (c) No detecta una ráfaga de errores de longitud 5 con una probabilidad 0.125
   (d) Nada de lo anterior puede afirmarse

$\boxed{\text{MPI}}$

D^4	D^3 D^2 D 1
0	0000
1	1001

$k=1$

$Y(D) = D^r \cdot X(D) + R(D) = 0$

$R(D) = D^r \cdot X(D) \bmod g(D) = 0$

$\downarrow$

$X(D) = 0$

$Y(D) = D^4 + D^3 + 1$

$R(D) = D^4 \bmod D^4 + D^3 + 1 = D^3 + 1$

$\downarrow$

$X(D) = 1$

$D^4 \mid \underline{D^4 + D^3 + 1}$

$D^4 + D^3 + 1 \quad 1$

$D^3 + 1$

a) Si se producen 3 errores, se pasa de una palabra código a la otra. NO

b) $d_{min} = 3 \rightarrow e = \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor = 1$. NO

c) longitud ráfaga $= 5 = j - i + 1 \Rightarrow j - i = 4$

prob(no detectable) $= \frac{1}{2^{r-1}} = \frac{1}{2^r} = 0'125$.

N

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

(a) La distancia mínima del código es 3

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

(c) Es un código 1-perfecto

(d) Alguna de las anteriores es falsa

Código:

$$\begin{array}{c|cc} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 2 & 2 & 2 \\ k=1 & & r=2 \end{array} \quad d=3 \quad d=3 \quad d=3$$

a) $d_{min} = 3$ cierto

b) Será equivalente a tener 1 error por palabra, que se corregirá. cierto

c) $e = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor = 1$ Tiene capacidad correctora 1 error.

Código e-perfecto:

$$q^r = \binom{n}{0} + \binom{n}{1}\cdot(q-1) + \binom{n}{2}\cdot(q-1)^2 + \dots + \binom{n}{e}(q-1)^e$$

Código 1-perfecto:

$$q^r = 1 + n\cdot(q-1)$$

$$q=3 \quad \Rightarrow \quad 3^2 = 1 + 3\cdot 2 = 7$$

$$\begin{array}{c} \shortparallel \\ 6 \end{array}$$

¡NO!

F

18. Una fuente emite símbolos según este algoritmo:
-Se lanza un dado, sea X el resultado
-Se lanza una moneda
-Si cara, se emite $X mod 4$
-Si cruz, se emite $(X mod 3) + 4$

La entropía de la fuente es:

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

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

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

(d) Ninguna de las anteriores

p(cara) = 1/2

X	X mod 4
1	1
2	2
3	3
4	0
5	1
6	2

p(cruz) = 1/2

X	X mod 3	+ 4 =
1	1	5
2	2	6
3	0	4
4	1	5
5	2	6
6	0	4

i	P(i)
0	1/12
1	1/6
2	1/6
3	1/12
4	1/6
5	1/6
6	1/6

$$H(F) = 5 \cdot \frac{1}{6} \cdot \log_2 6 + 2 \cdot \frac{1}{12} \cdot \log_2 12 = \frac{5}{6}\left(\log_2(2\cdot 3)\right) + \frac{1}{6}\log_2(4\cdot 3)$$

$$= \frac{5}{6}\left(1 + \log_2 3\right) + \frac{1}{6}\left(2 + \log_2 3\right) = \frac{7}{6} + \log_2 3$$

F

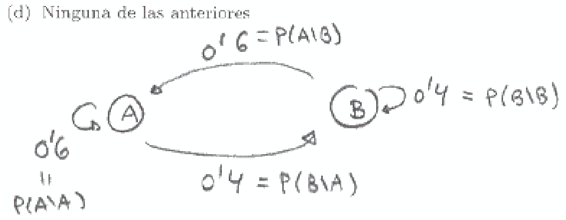
19. Una fuente emite dos símbolos A y B con probabilidades: $P(B|A) = P(B|B) = 0.4$. Para una extensión de fuente de orden 1 (agrupaciones de 2 símbolos), ¿cuánto vale la entropía de dicha fuente extendida?

(a) 0.950 bits inf/simb

(b) 1.942 bits inf/simb

(c) 1.900 bits inf/simb

(d) Ninguna de las anteriores



$$P(A) = \underbrace{P(A\backslash A)}_{0'6} \cdot P(A) + \underbrace{P(A\backslash B)}_{0'6} \cdot P(B) = 0'6 \cdot \underbrace{(P(A) + P(B))}_{1} = 0'6$$

Si $P(\underline{A}\backslash A) = P(\underline{A}\backslash B) = P(\underline{A}) \rightarrow$ No hay memoria!!

$$AA \rightarrow P(A\backslash A)\cdot P(A) = P(A)\cdot P(A) = 0'6^2 = 0'36$$
$$AB \rightarrow P(B\backslash A)\cdot P(A) = P(B)\cdot P(A) = 0'6 \cdot 0'4 = 0'24$$
$$BA \rightarrow P(A\backslash B)\cdot P(B) = P(A)\cdot P(B) = 0'6 \cdot 0'4 = 0'24$$
$$BB \rightarrow P(B\backslash B)\cdot P(B) = P(B)\cdot P(B) = 0'4^2 = 0'16$$

$$H(F^2) = 0'36 \cdot \log_2 \frac{1}{0'36} + 0'16 \cdot \log_2 \frac{1}{0'16} + 2 \cdot 0'24 \cdot \log_2 \frac{1}{0'24} =$$

$$= 1'9419 \text{ bits/símbolo}$$

* Para fuente sin memoria:

$$H(F^2) = 2 \cdot H(F) = 1'9419$$

$$H(F) = 0'6 \cdot \log_2 \frac{1}{0'6} + 0'4 \cdot \log_2 \frac{1}{0'4} = 0'97095$$

P

20. 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) 11.1623 KHz
(b) 1.1782 KHz
(c) 2.5885 KHz
(d) Ninguna de las anteriores

$$H(F) = 2 \cdot 0'3 \cdot \log_2 \frac{1}{0'3} + 0'4 \cdot \log_2 \frac{1}{0'4} = 1'57095 \ \frac{\text{bits}}{\text{símbolo}}$$

$$v_F = 3000 \ \frac{\text{símbolos}}{\text{seg}}$$

$$\Rightarrow 3000 \cdot 1'57095 = 4712'85178 \ \frac{\text{bits}}{\text{seg}} = v_t$$

$$v_t \leq C = W \cdot \log_2 (1 + \underset{15}{\underset{\shortparallel}{S/N}}) = 4W$$

$$4712'8517 \leq 4W$$

$$\boxed{W \geq 1'1782 \ \text{KHz}}$$