4 D
7 F
9 N

Test

ETSETB
Curso 2006-07 Primavera
EXAMEN DE TRANSMISIÓN DE DATOS
28 de junio de 2007

PUBLICACIÓN DE NOTAS PROVISIONALES: 02/07/2007
FECHA LÍMITE PARA LAS ALEGACIONES: 04/07/2007 a las 14:00 horas
PUBLICACIÓN DE NOTAS DEFINITIVAS: 05/07/2007

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

D...

1. Sabiendo que $11^{1389} = 2 \ mod \ 9973$ y que $11^{4903} = 31 \ mod \ 9973$ el valor de x que satisface $11^x = 496 \ mod \ 9973$ está en el intervalo (*Nótese que* $496 = 2^4 * 31$ *que 9973 es primo*):

   a) $0 \leq x \leq 486$
   b) $487 \leq x \leq 3997$
   c) $3998 \leq x \leq 7937$
   d) $7938 \leq x \leq 9972$

$496 = 2^4 \cdot 31 \Rightarrow 496 \bmod 9973 = (2^4 \bmod 9973) \cdot (31 \bmod 9973) =$

$= (2 \bmod 9973)^4 \cdot (31 \bmod 9973) = (11^{4\cdot 1389} \cdot 11^{4903}) \bmod 9973$

$x = (4 \cdot 1389 + 4903) \bmod \overbrace{9972}^{\phi(9973)} = 10459 \bmod 9972 =$

$= \boxed{487}$

Pista → Como no está en los rangos... falta reducir módulo!!

Nota: En módulo n, todos los elementos son $0 \leq$ elementos $< n$, pero los exponentes están en módulo $\phi(n)$!

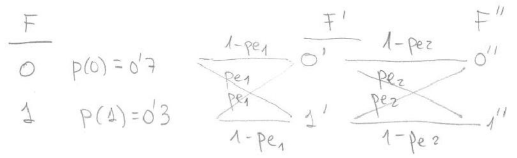
$10459 \bmod 9973 = 486$, está mal...

Si n primo, $\phi(n) = n-1 \Rightarrow \phi(9973) = 9972$.

F

2. Una fuente binaria sin memoria emite los símbolos '0' y '1' con las probabilidades $p(0) = 0{,}7$ y $p(1) = 0{,}3$. Cuando dicha fuente atraviesa dos canales binarios simétricos con probabilidad de cruce $Pe_1 = Pe$ y $Pe_2 = 0{,}9Pe$ se obtiene un 58.6528 % de ceros a la salida. Suponiendo que $Pe \leq 0{,}5$ el valor de Pe está en el intervalo:

   a) $0 \leq Pe < 0{,}125$
   b) $0{,}125 \leq Pe < 0{,}25$
   c) $0{,}25 \leq Pe < 0{,}275$
   d) $0{,}275 \leq Pe \leq 0{,}5$



$p(0'') = 0'586528$

$$P(0'') = p(0)\cdot(1-pe_1)\cdot(1-pe_2) + p(0)\cdot pe_1\cdot pe_2 + p(1)\cdot pe_1\cdot(1-pe_2) +$$

$$+ p(1)\cdot(1-pe_1)\cdot pe_2 = p(0)\left[(1-pe)\cdot(1-0'9\,pe) + pe\cdot 0'9\,pe\right] +$$

$$+ p(1)\cdot\left[pe\cdot(1-0'9\,pe) + (1-pe)\cdot 0'9\,pe\right] =$$

$$= 0'7\cdot\left[1-0'9pe - pe + 0'9pe^2 + 0'9pe^2\right] + 0'3\cdot\left[pe - 0'9pe^2 + 0'9pe - 0'9pe^2\right] =$$

$$= 0'72\,pe^2 - 0'76\,pe + 0'7 = 0'586528$$

$$0'72\,pe^2 - 0'76\,pe + 0'113472 = 0$$

$$pe^2 - 1'05555pe + 0'1576 = 0$$

$$pe = \frac{1'05555 \pm \sqrt{1'1142 - 0'6304}}{2} = \frac{1'05555 \pm 0'6955}{2} = \begin{cases} 0'8755 \\ \boxed{0'18} \end{cases}$$

F

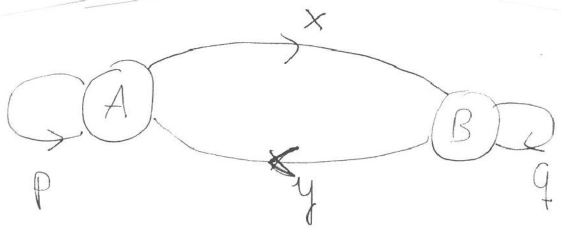
4. Sea una fuente binaria caracterizada por las siguientes probabilidades condicionadas: $P(A|A) = p$, $P(B|A) = x$, $P(A|B) = y$, $P(B|B) = q$. Puede afirmarse que:

a) Se trata de una fuente sin memoria para cualquier valor de p y q

b) Se trata de una fuente sin memoria para $p = q$

c) Se trata de una fuente sin memoria para $x = y = 1/2$

d) Ninguna de las anteriores



FUENTE SIN MEMORIA

$$\left.\begin{array}{l} p = y \\ q = x \end{array}\right\}$$

Si $x = y = \frac{1}{2} \Rightarrow p = \frac{1}{2}$ $q = \frac{1}{2}$

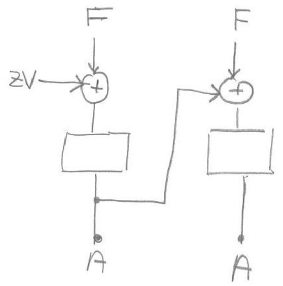
SE CUMPLE

D+

3. Si el texto claro 'FF' (hexa) se cifra con un cifrador bloque de 4 bits invertible, se obtiene el criptograma 'AA' (hexa). Se puede asegurar que:

   a) El cifrador bloque se ha usado en modo ECB (modo nativo)
   b) El cifrador bloque se ha usado en modo CBC
   c) Si se ha usado el modo CBC, el vector inicial debe valer 'A' (hexa)
   d) Nada de lo anterior puede afirmarse

a) No necesariamente, aunque es posible
b) // //
c)



$ZV \oplus F = F + A$

$\boxed{ZV = A}$

F

5. Para un cierto código convolucional la secuencia código más próxima a la secuencia todo ceros es 0...010010001110...0. La distancia libre del código es:

   a) 5
   b) 7
   c) 10
   d) Ninguna de las anteriores

d_{libre} = nº de unos sec. + próx. a la sec. nula

D++

6. En un sistema criptográfico, el criptograma c es $(34a+13)\ mod_{79}$ con $a = b^e mod_{(79*83)}$ y $b = (11m+19) mod_{79}$, siendo m el mensaje del usuario. Indíquese la respuesta FALSA: 79 y 83 son primos.

   a) Si $e = 5, m = ((7c+67)^{-31} * 36 + 27)(mod_{79})$
   b) Si $e = 5, m = ((7c+67)^{5116} * 36 + 27)(mod_{79})$
   c) Si $e = 1, m = (15c+69)(mod_{79})$
   d) Alguna de las anteriores es falsa

Pregunta 6.

$a \bmod 79 = (b^e \bmod 79 \cdot 83) \bmod 79 = b^e \bmod 79$

$\rightarrow m = (((c-13)34^{-1})^d - 19)11^{-1}$.

Si $e=1$, $d=1$ $\rightarrow$ c) puede ser cierta

Si $e=5$: $5\cdot(-31) \bmod \phi(79) = -155 \bmod 78 = 1$

$\rightarrow$ a) puede ser cierta

$5 \cdot 5116 \bmod 78 = 74$ $\rightarrow$ b) es Falsa.

Hay que deshacer lo hecho al cifrar, para descifrar:

$c = (34a+13) \bmod 79 \longrightarrow a = [(c-13)\cdot 34^{-1}] \bmod 79$

$a = b^e \bmod 79\cdot 83 = b^e \bmod 79 \longrightarrow b = a^d \bmod 79$

$a \bmod 79$

$e \cdot d = 1 \bmod \underbrace{\phi(79)}_{=78}$

$b = (11m+19) \bmod 79 \longrightarrow m = [(b-19)\cdot 11^{-1}] \bmod 79$

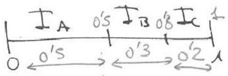
Todo junto, $m = \{[(c-13)\cdot 34^{-1}]^d - 19\} \cdot 11^{-1} \bmod 79$

F

7. Un codificador aritmético de una fuente cuyo alfabeto es $\{A, B, C\}$ envía el valor 0.34 correspondiente a la codificación de un mensaje de 4 caracteres. Sabiendo que la codificación aritmética emplea valores crecientes según el orden $\{A, B, C\}$ y que las probabilidades de estos símbolos son respectivamente 0.5, 0.3 y 0.2, indique el valor del mensaje descodificado:

a) ABBB
b) ACBA
c) CBBA
d) Ninguno de los anteriores

Definimos los intervalos



$I_A = [0, 0'5)$; $I_B = [0'5; 0'8)$; $I_C = [0'8, 1)$

Los puntos de inicio de cada intervalo son: $i_A = 0$, $i_B = 0'5$, $i_C = 0'8$
y la longitud de los segmentos es: $\Delta_A = 0'5$, $\Delta_B = 0'3$, $\Delta_C = 0'2$.

Aplicando recursivamente:

$$X_0 = 0'34$$

$$x_{n+1} = \frac{x_n - i_j}{\Delta_j} \quad \text{donde } x_n \in I_j$$

$$x_0 = 0'34 \in I_A \Rightarrow A$$ $\Rightarrow$ c) No es

$$x_1 = \frac{x_0 - i_A}{\Delta_A} = \frac{0'34 - \emptyset}{0'5} = 0'68 \in I_B \Rightarrow B$$

$$x_2 = \frac{x_1 - i_B}{\Delta_B} = \frac{0'68 - 0'5}{0'3} = 0'6 \in I_B \Rightarrow B$$

$$x_3 = \frac{x_2 - i_B}{\Delta_B} = \frac{0'6 - 0'5}{0'3} = 0'3 \in I_A \Rightarrow A$$

Descodificación ABBA $\Rightarrow$ d)

N

8. Para $t = m^k\ mod_n$, con t, m, k y n ~~todos~~ enteros mayores que cero, puede asegurarse que

a) La mínima potencia de t que es 1 módulo n es inferior a $\phi(n)$

b) t es coprimo con n, si m y n ~~lo~~ son coprimos

c) Si m y n no son coprimos entonces t puede ser coprimo con n

d) Ninguna de las anteriores

Pregunta 8.

a) Falsa : t tiene inversa mod $n \Leftrightarrow (t,n)=1$

b) Cierta : Si $(m,n)=1$, $(m^k,n)=1 \Rightarrow (m^k \bmod n, n)=1$ (primer paso del alg. de Euclides)

c) Falsa : Si $(m,n)\neq 1$, $(m^k,n)\neq 1 \Rightarrow (m^k \bmod n, n)\neq 1$ siempre (nunca podrá ser 1).

a) $t = m^k \bmod n \to mcd(t,m)=1 \to \exists\, t^{-1} \bmod n$

$t^{\phi(n)} = 1 \bmod n$

N

9. En un sistema RSA con parámetros (e,d,n) **siempre** se cumple que:

a) $e^{\phi(n)} mod_n = 1$
b) $e^{\phi(\phi(n))} mod_n = 1$
c) $e^{\phi(\phi(n))} mod_{\phi(n)} = 1$
d) Ninguna de las anteriores

Pregunta 9.

a) Falsa: $e^{\phi(n)} \equiv_n 1$ si $(e,n)=1$. En un RSA se asegura que $(e,\phi(n))=1$.

b) Falsa: $e^{\phi(\phi(n))} \equiv_n 1$, podría ser pero con $(e,n)=1$.

c) Cierta: $e^{\phi(\phi(n))} \equiv_{\phi(n)} 1$, sea $m=\phi(n) \Rightarrow$
$e^{\phi(m)} \equiv_m 1$ (Teorema de Euler).

RSA $\Rightarrow \exists\ e^{-1} \bmod \phi(N) \Rightarrow mcd(e,\phi(N))=1$

Teorema Euler $\Rightarrow$ si $mcd(e,n)=1 \Rightarrow e^{\phi(n)} = 1 \bmod n$

$n=\phi(N) \Rightarrow$ si $mcd(e,\phi(N))=1 \Rightarrow e^{\phi(\phi(N))} = 1 \bmod \phi(N)$

N

10. Un polinomio de conexiones $c(D)$ de grado m de un LFSR es un factor irreducible del binomio $(1 + D^n)$ donde $n = 2^m - 1$ es un número primo. Se puede asegurar que:

- (a) El LFSR genera una secuencia de periodo n
- b) $c(D)$ podría no ser un polinomio primitivo
- c) $(1 + D^{4n})\ mod_{c(D)}$ es diferente de 0
- d) Ninguna de las anteriores

Pregunta 10.

"es factor de"

Si $C(D) | (1+D^n)$ entonces $C(D) | (1+D^{k \cdot n})$ $\rightarrow$ c) Falsa.

Supongamos que $C(D) | (1+D^p)$ con $p<n$, entonces $C(D) | (1+D^{q \cdot p})$ pues como n es primo, no existe q tal que $q \cdot p = n$. Si $C(D) | (1+D^n)$, $C(D)$ no divide a otro con $p<n$, es decir, es primitivo puesto que $n = 2^m - 1$ (primo de Mersenne).

$\rightarrow$ a) Cierta

b) Falsa.

— Para $C(D)$ primitivo de grado m, $L = 2^m - 1$, $(1 + D^L) \bmod C(D) = \emptyset$.

— Para $C(D)$ no primitivo, el periodo de la secuencia pseudoaleatoria generada (p) es divisor de $L = 2^m - 1$, $(1 + D^p) \bmod C(D) = \emptyset$.

— Si L es primo, no tiene factores (L y 1 solo) p.

$\Rightarrow$ Ese $C(D)$ ha de ser primitivo!

N

11. Si se elimina una columna en la matriz de comprobación de paridad de un código de Hamming (7,4), para el código resultante es FALSO que:

   a) Corrige todos los errores simples
   b) Es un código 1-perfecto
   c) Puede corregir 1 único error doble
   d) Alguna de las anteriores es falsa

1-perfecto

Pregunta 11.

Se obtiene un código recortado de Hamming $(\overset{n}{6},\overset{k}{3})$ con $2^3-1=7$ síndromes diferentes de $\emptyset$.

Como hay 6 errores simples pueden corregirse todos y sobra 1 que puede adjudicarse a 1 error doble:

a) cierta, $e=1$ igualmente. Pero no es de Hamming!

c) cierta

b) Falsa (no corrige exactamente hasta 1 error).

N

12. Para transmitir 4 símbolos se ha elegido un subconjunto de 4 palabras de un código sistemático (7,4) generado por $D^3 + D + 1$. Si estas palabras corresponden a los mensajes 1111, 1011, 0110 y 1000, puede asegurarse que:

a) Añadir 1 bit de paridad a la palabra código no incrementa la distancia mínima

b) Puede corregir dos borrones y detectar dos errores (en la misma palabra recibida) !

c) El código (5,2) generado por $D^3 + D + 1$ tiene la misma distancia mínima

d) Ninguna de las anteriores

¡No es un código Lineal!

Pregunta 12.

$D^3 \bmod g(D) = D+1 \rightarrow 0\ 1\ 1$

$D^4 \bmod g(D) = D^2+D \rightarrow 1\ 1\ 0$

$D^5 \bmod g(D) = D^3+D^2 \bmod g(D) = D^2+D+1 \rightarrow 1\ 1\ 1$

$D^6 \bmod g(D) = D^3+D^2+D \bmod g(D) = D^2+1 \rightarrow 1\ 0\ 1$

K=4

1111 → (1111 ⋮ 111)

1011 → (1011 ⋮ 000)

0110 → (0110 ⋮ 001)

1000 → (1000 ⋮ 101) (*)

$D^3\ D^2\ D\ 1$ — D^6 — $D^2\ \ 1$

(**) La $d_{min} = 4$, hay que calcular la $d_{Hamming}$ de cada dos palabras y coger la mínima. NO ES CÓDIGO LINEAL, ESTE SUBCONJUNTO (NO TIENE ELEMENTO NEUTRO, ETC.)

- Añadir 1 bit de paridad global supone añadir el mismo bit a las 4 palabras código (todas tienen un número impar de 1's y un número par de 0's) → a) Cierta.
- La d_{min} es 4 (**) → b) Falsa $e = \lfloor \frac{d_{min}-1}{2} \rfloor = 1$; $\rho = d_{min} - 1 = 3$
- El código (5,2) generado por D^3+D+1 es un código recortado de Hamming con $d_{min} = 3$ → c) Falsa.

(*) $\begin{cases} Y(D) = D^r \cdot X(D) + R(D) \\ R(D) = D^r \cdot X(D) \bmod g(D) \end{cases}$

p.ej. $X(D) = D^3$;; $D^r \cdot X(D) = D^6$;; $D^6 \bmod (D^3+D+1) = D^2+1$.

$Y(D) = D^6 + D^2 + 1$

$$\begin{array}{l|l} D^6 & D^3+D+1 \\ \hline D^6+D^4+D^3 & D^3+D+1 \\ D^4+D^3 & \\ D^4+D^2+D & \\ D^3+D^2+D & \\ D^3+D+1 & \\ D^2+1 & \end{array}$$

N

13. Una fuente binaria sin memoria con entropía $H(X) = 0{,}8$ bits/símbolo emite sobre un canal binario simétrico cuya probabilidad de error es $1/8$. Siendo $H(Y)$ la entropía a la salida del canal, se puede asegurar que:

a) $0 < H(Y/X) < 0{,}45$
b) $0 < H(X/Y) < 0{,}55$
c) $0{,}55 < H(Y) \leq 0{,}8$
d) $0{,}55 < I(X;Y) \leq 0{,}8$

$p = 1/8$; $H(p) \triangleq p \log_2 1/p + (1-p)\log_2 \frac{1}{1-p} = 0'543$

a) $H(Y/X) = H(p) = 0'543 \Rightarrow$ Falso $\quad 0 < H(Y/X) < 0'45$

c) $H(Y) \geq H(X)$ con $H(X) > H(p)$

$H(Y) \geq 0'8$ la igualdad se produce si $H(p) = 0$

Luego es falso que $H(Y) \leq 0'8$

d) $I(X;Y) = H(Y) - H(Y/X) = H(Y) - H(p)$

$0'55 < I(X;Y) \leq 0'8$ es equivalente a:

$0'55 < H(Y) - 0'543 \leq 0'8$ que ~~es~~ equivalente a:

$1'093 < H(Y) \leq 1'343$ que es siempre

falso porque $H(Y) \leq 1$ al ser binaria la fuente.

b) $H(X/Y) = H(X) - H(Y) + H(Y/X) = 1'343 - H(Y)$

$0'8 + 0'543 = H(X) + H(Y/X)$

$0 < H(X/Y) < 0'55$ es equivalente a:

$0'793 < H(Y) < 1'343$ que es cierto, ya que

$0'8 < H(Y) < 1$.

F

14. Una fuente de información emite símbolos de un alfabeto {A,B,C,D,E,F,G,H,I} con probabilidades:
P(A)= P(B)=1/3; P(C)= 1/9; P(D)=P(E)=P(F)=P(G)=P(H)=P(I)=1/27.
Para un sistema de transmisión que utiliza un codificador de fuente **ternario**, es FALSO que:

a) Existe un código instantáneo donde la codificación de todos los símbolos de fuente dé lugar a palabras código de longitud 2
b) La codificación ternaria de Huffman tiene eficiencia 1
c) La entropía de la fuente es mayor que 2 bits/simb
d) Alguna de las anteriores es falsa

a) Se verifica la desigualdad de Kraft

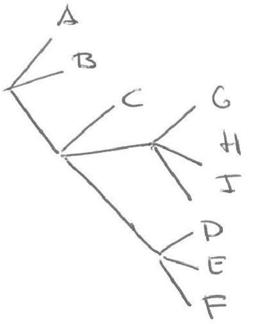
$$\sum_{i=1}^{9} 3^{-2} = 1 \leq 1 \Rightarrow \text{cierto}$$

c) $H = \frac{2}{3}\log_2 3 + \frac{1}{9}\log_2 9 + \frac{6}{27}\log_2 27 = 2'46$ bits/simb

cierto >2

$H = \frac{2}{3}\log_3 3 + \frac{1}{9}\log_3 9 + \frac{6}{27}\log_3 27 = 1'55$ trits/simb.

b)



$E = \frac{H}{L} = 1$

$L = 1'55$ dig. ternarios/simb.

cierto.

d) Falso.

D

15. Para el código polinómico Cod(5,3), cuyo generador es el polinomio completo de grado 2, es cierto que:

a) Es un código recortado de Hamming
b) Detecta cualquier número impar de errores
c) Detecta siempre 2 errores en el bloque
d) La probabilidad de detección de ráfagas de error de 3 bits es 1/2

a) $n = 5$, $k = 3$, $r = 2$

El código de Hamming de menor redundancia con $n > 5$ es el Cod(7,4) que tiene $r = 3$. Los códigos recortados tienen el mismo valor de r. Por lo tanto, Falso.

b) D^2+D+1 es irreducible por lo tanto no contiene a $D+1$, condición necesaria y suficiente para detectar ~~los~~ un número impar de errores. Falso

c) Si existe un polinomio $D^{j-i}+1$ divisible por D^2+D+1 es falsa la afirmación cuando $j-i < 5$. Como $D^{2=m}+D+1$ es primitivo divide a $D^{3=2^m-1}+1$ y por lo tanto es falso

d) Una ráfaga de error de 3 bits tiene la forma $D^2+ * D+1$ con $* \in \{0,1\}$.
Hay dos polinomios y sólo detecta a $* = 0$.
Por lo tanto, $1/2 \Rightarrow$ Cierto

N

16. Para un código bloque binario 2-perfecto, es FALSO que:

a) Siempre detecta 4 errores
b) La redundancia debe tener como mínimo 4 símbolos
c) Sea un código de repetición Cod(5,1)
d) Alguna de las anteriores es falsa

a) $\underset{e}{2}$-perfecto $\Rightarrow$ $d_{min} = 5$ $\Rightarrow$ detecta 4 errores
$= 2e+1$
cierto $\delta = d_{min} - 1 = 4$

b) Si $d_{min} = 5 \Rightarrow r \geq \underset{2e=4}{4}$ cierto

c) El cod $(\underset{n}{5}, \underset{k}{1})$ es 2-perfecto $\Rightarrow$ cierto

d) Falso

$2^r = 1 + \binom{n}{1} + \binom{n}{2} = 1 + n + \frac{n!}{2!(n-2)!} =$

$= 1 + n + \frac{1}{2} \cdot n \cdot (n-1)$

$2^4 = 1 + 5 + \frac{5 \cdot 4}{2}$?

$16 = 6 + 10$? sí.

F

$e=1$

17. Un código sistemático de Hamming, Cod(7,4), se emplea como $\boxed{\text{corrector}}$ para un canal cuya probabilidad de error de bit es 1/700. La probabilidad de error de $\boxed{\text{bit}}$ del usuario destinatario es:

a) 21/490000
b) 12/490000
c) 9/490000
d) 3/490000

$$P_{bloque} = \sum_{i=2=e+1}^{7} \binom{7}{i} p^i (1-p)^{7-i} \simeq \binom{7}{2}\left(\frac{1}{700}\right)^2$$

Si el bloque es erróneo una vez corregido dispone de 3 errores ya que $d_{min}=3$ y es 1-perfecto. La probabilidad de que un bit de usuario sea erróneo en ese bloque será: $\frac{3 = e+1+e}{7 = n}$

Finalmente $$\frac{3}{7}\cdot\binom{7}{2}\cdot\left(\frac{1}{700}\right)^2 = \frac{9}{490000}$$

$$\frac{3}{7}\cdot\frac{7!}{2!\,5!}\cdot\frac{1}{490000} = \frac{9}{490000}$$

c)

2

18. Para un código **ternario** de repetición Cod(3,1) es FALSO que:

- *a*) La matriz de generación es $G = (111)$
- *b*) El subespacio ortogonal al código está generado por la base $< (1,0,2), (0,1,2) >$
- *c*) El número de síndromes no nulos es 8
- *d*) Alguna de las anteriores es falsa

Cod (3,1) ternario de repetición

a) $G = (1\ 1\ 1)$ <u>cierto</u>

b) $(1,0,2)$ y $(0,1,2)$ son linealmente independientes

El subespacio ortogonal tiene dimensión $r = 2$

$\left.\begin{array}{l}(1,0,2)\cdot(1,1,1) = 0\\(0,1,2)\cdot(1,1,1)=0\end{array}\right\}$ ortogonales a $(1\ 1\ 1)$

<u>cierto</u>

c) El nº de síndromes es $3^r = 3^2 = 9$

excluyendo el nulo quedan 8 $\Rightarrow$ cierto

d) Falso

F

19. En la tabla se muestra el análisis estadístico de 3 criptogramas procedentes de textos castellanos. ¿Qué afirmación es más verosímil? *Nota: La estadística de las vocales del castellano es: p(A)=11.9 %, p(E)=14.6 %, p(I)=7.1 %, p(O)=9.1 %, p(U)=3.3 %*

Frec./Cript.	A	E	I	O	U
Cript. 1 (%)	11.9	14.6	7.1	9.1	3.3
Cript. 2 (%)	0.2	1.1	0.7	11.9	6.6
Cript. 3 (%)	3	4.1	4.4	4.6	3.9

a) El criptograma 1 procede de un cifrado por sustitución monoalfabética y el criptograma 2 de un cifrado por sustitución polialfabética.

b) El criptograma 2 puede proceder de un cifrado por sustitución monoalfabética y el criptograma 3 de un cifrado de transposición.

c) El criptograma 1 procede de un cifrado por transposición y el criptograma 3 de un cifrado por sustitución polialfabética.

d) Ninguna de las anteriores afirmaciones es verosímil

Criptografía Clásica
- Substitución
  - Monoalfabética ($= $ castellano, $\neq$ letras)
    - Monográmica → César
    - Poligrámica → Playfair
  - Polialfabética ($\simeq$ aleatorio)
    - Periódica → Vigenère
    - Aperiódica → Vernan
- Transposición → Escítalo ($=$ castellano, $=$ letras)

Cript. 1 ⇒ Estadista = castellano, = letras ⇒ Transposición
Cript. 2 ⇒ " " ≠ letras ⇒ Subs. Monoalf.
Cript. 3 ⇒ " ≃ aleatorio ⇒ Subs. Polialf.

⇒ c

N

20. Sabiendo que 748063=761*983 (con 761 y 983 primos), el valor de $521^{746319} mod_{748063}$ puede ser:

a) 707860
b) 746320
c) 423
d) Ninguna de las anteriores

Si $mcd(a,n)=1 \Rightarrow a^{-1} \bmod n = a^{\phi(n)-1} \bmod n$

$a = 521$
$n = 748063$
$\phi(n) = 760 \cdot 982 = 746320$

$a \cdot a^{-1} = 1 + k \cdot n$ Piden un posible a^{-1}

$521 \cdot a^{-1} = 1 + k \cdot 748063$, k entero

a) $521 \cdot 707860 = 1 + k \cdot 748063$? $k = 493$ Sí

b) $521 \cdot 746320 = 1 + k \cdot 748063$? $k = 519'78$ NO

c) $521 \cdot 423 = 1 + k \cdot 748063$? $k = 0'29$ NO