Escuela Técnica Superior de Ingeniería de Telecomunicación de Barcelona

CONTROL DE TRANSMISIÓN DE DATOS
22 de Mayo de 2003

NOTAS IMPORTANTES:

1.- *No se responderá ninguna pregunta acerca del enunciado o su interpretación. El alumno responderá según su criterio, especificando en sus respuestas las hipótesis que realice.*
2.- *Se valorará la justificación, discusión y claridad de los resultados.*
3.- ***Los resultados no reflejados en la hoja de resultados anexa no serán tenidos en cuenta.***
4.- *Un **error conceptual grave** puede anular todo el problema.*
5.- *Nótese que **los problemas constan de distintas partes que pueden resolverse por separado**. Se recomienda saltar aquellas partes que no sepan resolverse.*

Problema 1 (40%)

Una fuente emite dos símbolos (A y B) quedando completamente caracterizada por las siguientes probabilidades de emisión condicionadas:

$$p(A/A) = 0.7$$
$$p(B/B) = 0.2$$

Dicha fuente atraviesa un canal binario simétrico con una tasa de error de 0.1
Se pide:

a) ¿Cuál es la entropía de la fuente? **(2.5 puntos)**
b) ¿Cuál es la entropía a la salida del canal? Coméntese el resultado. **(4.5 puntos)**
c) Si se utiliza un código de Hamming (7,4) a la salida del canal para corregir errores, ¿Cuál es la entropía observada a la salida del decodificador? **(3 puntos)**

(***NOTA**: supóngase que la probabilidad de que el canal introduzca tres o más errores es nula)*

SIGUE DETRÁS

Problema 2 (60%)

Se dispone de un cifrador de cuatro bits de entrada y cuatro bits de salida que, para una cierta clave **k** tiene la siguiente relación entrada salida [M,E_k(M)]

M	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
C=E_k(M)	7	4	1	E	B	8	5	2	F	C	9	6	3	0	D	A

Se pide:

a) ¿Cuál es el tamaño mínimo de la clave para que pueda suponerse perfectamente aleatorio? **(1.5 puntos)**
b) El cifrado del mensaje **FFF** es **6A6**. Razone por qué puede asegurarse que el cifrado no se está usando en modo nativo o ECB. **(1 punto)**
c) Cuando se realiza un encadenado, como en este caso, es usual utilizar un vector de inicialización. Indique que alternativas utilizaría para este vector inicial y que ventajas aportan. **(1 punto)**
d) Sabiendo que la únicas operaciones usadas son $E_k(\cdot)$ y XOR, encuentre de forma razonada las ecuaciones del cifrador y del descifrador. ¿Cuánto vale el vector inicial? **(3 puntos)**

Como función de hash de un mensaje **n** bloques se usa el algoritmo

$$h_i = E_k(M_i + h_{i-1}) \quad i = 1..n \;\; h_0 = 0$$
$$H = h_n$$

e) Calcule el hash de mensaje **FFF**. ¿Cuántos mensajes de tres bloques hay que generen el mismo hash que **FFF** y que difieran únicamente en los dos primeros bloques del mensaje? (M1 y M2 distintos de F)**(2 puntos)**
f) Obtenga de forma razonada, y no por pruebas exhaustivas, el valor de **M** que hace que el mensaje **M1F** tenga el mismo hash que **FFF**. **(1.5 puntos)**