Escuela Técnica Superior de Ingeniería de Telecomunicación de Barcelona

CONTROL DE TRANSMISIÓN DE DATOS
17 de diciembre de 2004

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 (50%)

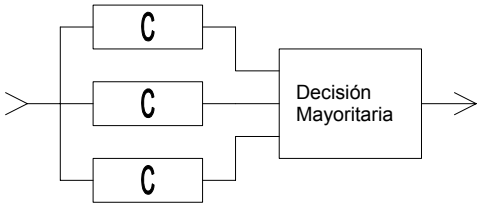
Una fuente emite dos símbolos (A, B) quedando completamente caracterizada por las siguientes probabilidades de emisión condicionadas:

$$p(A/A) = 0.6$$
$$p(A/B) = 0.3$$

Dicha fuente atraviesa un canal binario simétrico, **C**, con una tasa de error de 0.2
Se pide:

a) ¿Cuál es la entropía de la fuente? **(1 puntos)**
b) ¿Cuál es la entropía a la salida del canal? Coméntese el resultado. **(3 puntos)**

Se decide utilizar tres canales idénticos a C en paralelo según el esquema:



c) ¿Cuál es la capacidad del nuevo canal? **(3.5 puntos)**
d) ¿Cuál es la entropía a la salida del nuevo canal? Coméntese el resultado **(2.5 puntos)**

SIGUE DETRÁS

Problema 2 (25%)

Se quiere llevar a cabo un cifrador bloque de 4 bits mediante un LFSR de longitud 4. Para ello se carga como estado del LFSR el cuarteto de los bits a cifrar y se hace evolucionar ***k*** ciclos, siendo el **estado resultante** el valor del cuarteto cifrado. Como polinomio de conexiones se usa un valor ***C(D)*** fijo para todos los valores de ***k***.

Se pide:

a) Si ***C(D)*** es primitivo ¿cuál es número de claves distintas? **(1.5 puntos)**
b) Para ***k***=4 el cifrado de [0001] (en todas las ternas el mayor peso se halla a la izquierda) es [0011]. ¿Cuánto vale ***C(D***)? **(2.5 puntos)**
c) Para ***k***=7 ¿Cuánto vale el cifrado de [0001]? **(1.5 puntos)**
d) Para ***k***=7, el cifrado del mensaje [0001] [0001] [0001] es [1011] [0010] [1110]. Razone por qué puede asegurarse que el cifrado no se está usando en modo nativo o ECB. **(1.5 punto)**
e) Sabiendo que se trata de un cifrado CBC, ¿cuál es el vector inicial **(3 puntos)**

Problema 3 (25%)

El módulo de un sistema Diffie-Hellman es $p=2q+1$, donde q es un número primo. La base de dicho sistema es α.

Se pide:

a) ¿Qué propiedad debe cumplir α?¿por qué?**(1.5 puntos)**

Para un valor X aleatorio

b) ¿Cuál es el valor más probable de $\alpha^X \ mod$ p? **(1 punto)**
c) ¿Cuál es el valor más probable de $X^{p-1} \ mod \ p$? **(1.5 puntos)**
d) ¿Cuál es el valor más probable de $X^{(p-1)/2} \ mod \ p$? **(2.5 puntos)**
e) Para un cierto valor β, se tiene que $\beta^q \ mod \ p \neq p-1$. ¿puede ser β primitivo?¿por qué? **(2.5 puntos)**
f) Para un cierto valor γ, se tiene que $\gamma^q \ mod \ p \neq p-1$ y $\gamma^q \ mod \ p \neq 1$,¿cuánto vale γ?¿por qué? **(1 puntos)**