CONTROL DE TRANSMISIÓN DE DATOS. 22 de Mayo de 2002

Notas Importantes:

1. Los resultados no justificados, no serán tenidos en cuenta.
2. Los problemas se entregarán por separado, poniendo su nombre y apellidos en cada hoja, y numerándolas.
3. Un error conceptual grave, puede anular todo el problema.

Problema 1 (35%)

Un codificador convolucional tiene una tasa o razón de 0'25. Los polinomios de conexiones son:

$$v_1(D) = 1$$
$$v_2(D) = D$$
$$v_3(D) = D+D^2$$
$$v_4(D) = 1+D^3$$

a) Dibuje el circuito correspondiente a dicho codificador convolucional. Indique el valor de la redundancia, de la longitud de la influencia y del número de estados. (3p)

b) Dibuje el diagrama de estados del codificador y el diagrama en enrejado equivalente TCM (*Trellis Coded Modulation*). Indique las ecuaciones del codificador. (2p)

c) Calcule la distancia libre. (1p)

d) Para la secuencia de información 1110, encuentre cuál es la secuencia codificada. (2p)

e) Si la secuencia recibida es 111000111011, encuentre el mensaje estimado. (2p)

Problema 2 (35%)

En una carrera de motos con 4 participantes A, B, C y D, las probabilidades de que ganen la carrera depende del tiempo que haga, según la siguiente tabla:

Corredor Ganador	Tiempo que hace hoy		
	Soleado (S)	Nublado (N)	Lluvioso (Ll)
A	0'4	0'1	0
B	0'3	0'35	0'5
C	0'3	0'3	0
D	0	0'25	0'5

Si ayer hizo sol, las probabilidades de que hoy haga sol, nublado o llueva son del 50%, 50% y 0% respectivamente. Si ayer hizo nublado, las probabilidades son 25%, 50% y 25% respectivamente. Si ayer llovió, las probabilidades son 0%, 50% y 50% respectivamente.

a) Calcule la mínima cantidad de información en bits necesaria para transmitir el resultado de la carrera con alcance local (donde ya se sabe el tiempo que hace en el circuito). (3p)

b) Obtenga la codificación binaria óptima para transmitir el resultado de la carrera con alcance local. (2p)

c) Calcule la mínima cantidad de información en bits necesaria para transmitir el tiempo que hace hoy, con alcance internacional (donde no saben qué tiempo hace hoy en el Circuito). (2'5p)

d) Obtenga la codificación binaria óptima para transmitir el tiempo que hace hoy en el Circuito con alcance internacional. (Suponga que el tiempo que hizo ayer ya se lo transmitió ayer, es un dato que ya saben). (1'5p)

e) Qué mensajes transmitiremos con alcance internacional, para comunicar que ha ganado el corredor C, si hoy hace sol y ayer estuvo nublado. (1p)

Problema 3 (30%)

Responda brevemente de forma precisa y bien justificada estos apartados:

a) Describa es qué consisten estos servicios de seguridad: (2'5p)

- Confidencialidad
- Autenticación de origen
- Autenticación de contenido (integridad)
- Verificabilidad

b) Indique cómo protegería su sistema de transmisión de datos para autenticar la información (origen y contenido) frente a ataques activos, si se utiliza criptografía asimétrica. Indique si hay puntos débiles y cómo solucionarlos. Ayúdese de un esquema. (2'5p)

c) Describa el algoritmo de clave pública RSA. Indique las ecuaciones de cifrado y descifrado. Indique cómo obtener las claves pública y privada. (2'5p)

d) Aplique el algoritmo RSA para los números primos p=7, q=13. Indique las claves pública y privada. Cifre y descifre el mensaje M=37. (2'5p)