CONTROL DE TRANSMISIÓN DE DATOS. **15 de Mayo de 2003**
GRUPO 50

Notas Importantes:

1. Un error conceptual grave, puede anular todo el problema.

Problema 1 (50%)

Sea una fuente de 3 símbolos A, B y C, cuyas probabilidades son: P(A)=0,5; P(B)= 0,25; P(C)=0,25. Se sabe que P(A/A)=0,75; P(B/A) = P(C/A); y P(B/B)=P(B/C)=P(C/B)=P(C/C).

a) Calcule el tiempo mínimo para transmitir 100.000 símbolos de fuente por un canal con W = 1 KHz y S/N = 15 a la entrada del receptor (en escala lineal). **(2 puntos)**

b) Calcule la eficiencia de una codificación de Huffman de la fuente original del enunciado (es decir, sin considerar extensión de fuente) **(1 punto)**

c) Codifique la secuencia AABCABCABCAAC mediante el algoritmo LZW. Considere que utiliza un diccionario de 16 posiciones (a codificar con 4 bits). Exprese la codificación en hexadecimal **(2 puntos)**

Problema 2 (50%)

Sea un sistema de clave pública RSA. El valor de la clave pública de un usuario A es N=221; e=77. Se pide que el alumno actúe como ATACANTE del sistema:

a) Calcule el valor de la clave privada de A. **(2 puntos)**

b) Un usuario B envía confidencialmente a A el siguiente mensaje cifrado C=01001100 (utilizando el sistema RSA del enunciado, bit más significativo el de la izquierda). Obtenga el valor del mensaje enviado (en binario). **(2 puntos)**

c) Sabiendo que el mensaje capturado en el apartado anterior era una clave de Vernan (de 8 bits), decodifique el siguiente mensaje cifrado (C=00110011) que A transmite a B **(1 punto)**