CONTROL DE TRANSMISIÓN DE DATOS. GRUPO 20

14 mayo de 2003

Ejercicio 1. (4 puntos)

Dado el código de Hamming (15, 11) determinado por la siguiente matriz de comprobación $H = \left(\alpha^{14} \quad \alpha^{2} \quad \alpha \quad 1\right)$, siendo α una raíz del polinomio D^4+D+1, indíquese

a) Matriz de generación
b) Matriz de generación y comprobación del código dual de Hamming correspondiente
c) Cuando se ha utilizado el código de Hamming se han recibido las siguientes palabras: (X 0 0 0 0 0 0 0 0 0 0 X 0 0 X) y (0 1 1 0 0 0 0 0 0 0 0 0 X X X) ¿Se puede corregir en algún caso? Justifíquese la respuesta e interprete los resultados obtenidos
d) Repita el proceso con el código dual de Hamming

Ejercicio 2 (3 puntos)

Se sabe que la firma digital debe proporcionar servicios de autenticidad e integridad.

a) Se propone un esquema con la siguiente estructura:
M → M || $RSA_{privada\_emisor}$ (M)
¿Cumpliría este esquema los requisitos? Justifique la respuesta

b) ¿Qué pasaría si se utilizase una función de hash que no fuese libre de colisiones?

Ejercicio 3 (3 puntos)

Una secuencia constituida por un alfabeto ternario (-1, 0, 1) ha sido comprimida mediante el algoritmo LZW. Como resultado se ha obtenido: 1, 2, 2, 4, 7, 3

a) Indíquese la secuencia original
b) Indíquese como se hubiese codificado dicha secuencia original si se hubiese empleado LZ-78 y LZ-SS