Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona
UNIVERSITAT POLITÈCNICA DE CATALUNYA
DEPARTAMENT D'ENGINYERIA TELEMÀTICA

Transmissió de dades, grupo 20
Fecha: 2 Diciembre 2009

Notas provisionales:	9 Dic
Período de alegaciones:	11 Dic
Fecha notas revisadas:	14 Dic

Información adicional:

- Duración de la prueba: 2 HORAS
- Cualquier error conceptual grave puede anular todo el problema

PROBLEMA 1 (30%)

Un sistema de transmisión de datos está compuesto por un regenerador de señal. El regenerador tiene por entradas (X) símbolos que pertenecen al alfabeto { 1, 0, -1 }. Las probabilidades de recepción de los símbolos son: P[X = 1] = α , P[X = 0] = 1 – α- β , P[X = - 1] =β para 0 < α+β <= 1
El regenerador restituye los valores de los borrones (X=0) en valores de salida Y=1 o Y=-1 con la misma proporción con la que se generan y mantiene el mismo valor (Y=X) cuando las entradas son X=1 o X=-1.
a) Determine H(Y)
b) Calcule H(Y/X)
c) Halle I(X; Y)
d) Calcule la capacidad del sistema regenerador en bits por símbolo para los casos:
I) α=β
II) α= 2β

PROBLEMA 2 (30%)

Se dispone de un código de canal lineal, binario y sistemático (8,4), con una matriz de generación

$$G=\begin{pmatrix}1&0&0&0&1&1&0&1\\0&1&0&0&0&1&1&1\\0&0&1&0&1&0&1&1\\0&0&0&1&1&1&1&0\end{pmatrix}$$

a) Indíquese si las siguientes matrices H_1 y H_2 pueden ser de comprobación

$$H_1=\begin{pmatrix}1&0&1&1&1&0&0&0\\1&0&1&0&0&1&1&0\\0&1&1&1&0&0&1&0\\1&0&0&1&0&0&1&1\end{pmatrix} \qquad H_2=\begin{pmatrix}1&0&1&1&1&0&0&0\\1&1&0&1&0&1&0&0\\0&1&1&1&0&0&1&0\\1&0&1&0&0&0&0&1\end{pmatrix}$$

b) Cuál es la capacidad correctora del código?
c) Supóngase que se ha recibido (1 0 1 1 1 a 0 b). ¿Cuál sería la salida del decodificador?

PROBLEMA 3 (20%)

Un atacante a un sistema criptográfico sabe que el algoritmo de cifrado utilizado es en flujo, síncrono y basado únicamente en un único LFSR con polinomio primitivo de 10 celdas. Dicho atacante puede acceder a un subconjunto de la secuencia generada por dicho LFSR. ¿Cuántos bits de dicho subconjunto necesita para poder conocer toda la secuencia? Razone la respuesta.

PROBLEMA 4 (20%)

Un usuario decide emplear la firma RSA sin usar hash (m^d mod n). Supóngase que un atacante conoce dos firmas legítimas para dos mensajes m_1 y m_2. ¿Podría conocer la firma de m_1+m_2? ¿Y la de m_1*m_2?