CONTROL DE TRANSMISIÓN DE DATOS. GRUPO 20. 28 ABRIL 2004

Ejercicio 1 (3,5 puntos)

Una fuente ternaria con memoria se caracteriza por las siguientes probabilidades de transición: p(A/A)=0,7, p(A/B) = 0, p(C/A)=0, p(B/B)=0,7, p(B/C)=0,2 y p(C/C) = 0,6. Dichos datos se transmiten a través de un canal equivalente binario sin memoria con tasa de error 0,2, equidistribuida entre todos los posibles errores e independiente del símbolo enviado. Cálculese

a) ¿Cuál es la SNR mínima para poder transmitir 40000 símbolos/seg por un canal de 1,5 Khz de ancho de banda?
b) Cuál es la entropía a la salida del canal?

Ejercicio 2. (3,5 puntos)

Se dispone de un cifrador en flujo constituido por un LFSR y una función de salida no lineal. La salida del generador es periódica y es la siguiente: 01101100100010111

a) ¿Satisface los dos primeros postulados de aleatoriedad de Golomb?
b) ¿Puede ser que el polinomio de realimentación utilizado sea primitivo? ¿En tal caso, de que grado sería?

Posteriormente y utilizando un polinomio primitivo de grado considerable, se modifica la función no lineal y se observa que la secuencia contenida en un periodo se puede comprimir y enviar utilizando la mitad de bits.

c) ¿Podría considerarse este esquema como un buen cifrador? Justifique la respuesta.

Ejercicio 3. (3 puntos)

Un usuario A de un sistema RSA tiene como clave pública d=41, N=1961. Un usuario fraudulento captura el criptograma C=935 destinado a A y que teóricamente ofrece confidencialidad. Calculese:

a) La clave privada de A (e, F(N))
b) El mensaje en claro