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

Transmissió de dades, grupo 40

Fecha: 14 Diciembre 2006

Información adicional:

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

Problema 1 (50%)

Sea una fuente ternaria equiprobable $F_1 = \{1, 2, 3\}$. Sea una fuente (F) cuya salida es el valor máximo del símbolo actual y el símbolo anterior de F_1, es decir, el símbolo de F en el instante i vale: $F(i) = \max (F_1(i), F_1(i-1))$

a) Calcule la eficiencia de una codificación de Huffman binaria de la fuente F, suponiendo que F no tiene memoria. **(1 punto)**

b) Realice una codificación aritmética de la secuencia 3321132 generada por la fuente F. Indique el intervalo que codificaría esta secuencia y su longitud **(2 punto)**

c) Determine un modelo markoviano de F y calcule la entropía de la fuente F (suponiendo memoria 1) **(2 puntos)**

Problema 2 (50%)

Sea un LFSR caracterizado por $C(D) = D^6 + D^5 + D^4 + D^3 + D^2 + D + 1$. Utilizamos este LFSR para generar una clave simétrica de 6 bits que será el contenido del LFSR al cabo de un cierto número de iteraciones (para un estado inicial conocido).

a) Si el estado inicial vale $S(D)= D^4$, calcule el polinomio de estado al cabo de 772 iteraciones. Indique en binario el valor de la clave simétrica generada **(1 punto)**

Tenemos dos usuarios, **A**: $p_A = 59$, $q_A = 73$, y **B**: $p_B = 37$, $q_B = 97$, $e_B = 31$.

b) La clave del apartado anterior fue generada por el usuario A, que debe transmitirla confidencialmente a B. Halle el criptograma correspondiente. **(1,5 puntos)**

c) Ahora el usuario B recibe el criptograma C=5, que codifica una clave que le ha enviado A. Halle esta clave y exprésela en binario como un número de 12 bits **(1,5 puntos)**

d) Realice un cifrado de Vernam del mensaje M=101100111101 utilizando la clave calculada en el apartado anterior. **(1 punto)**