CONTROL DE TRANSMISIÓN DE DATOS. **16 de diciembre de 2004**
GRUPO 50
DURACIÓN: 90 MINUTOS

JORDI
FORNÉ

Notas Importantes:

Un error conceptual grave, puede anular todo el problema.

Problema 1 (50%)

Sea una fuente de 2 símbolos A y B, con P(A/A) = p; y P(B/B) = q.

a) Calcule la entropía de la fuente en función de p y q. **(1 punto)**

b) Particularice el resultado anterior para p = 1-q. Justifique la respuesta. **(1 punto)**

c) Para el caso p = q, halle la entropia de la fuente, así como la probabilidad de que la fuente emita ráfagas de longitud L=k. Particularice para p = 3/4. **(1 punto)**

d) Calcule el valor mínimo de p (con $p \geq 0{,}5$) para poder transmitir 100.000 símbolos de fuente en 10 segundos por un canal con W = 1 KHz y S/N = 31 a la entrada del receptor (en escala lineal). **(1 punto)**

e) Codifique la secuencia ABCCABCD emitida por una fuente de 4 símbolos mediante el algoritmo LZ77. Considere que la posición de la coincidencia se codifica mediante 4 bits y la longitud de la coincidencia mediante 2, y que los símbolos de la fuente utilizan la siguiente codificación: A (00), B (01), C (10), D (11). Exprese la codificación en notación hexadecimal. **(1 punto)**

Problema 2 (50%)

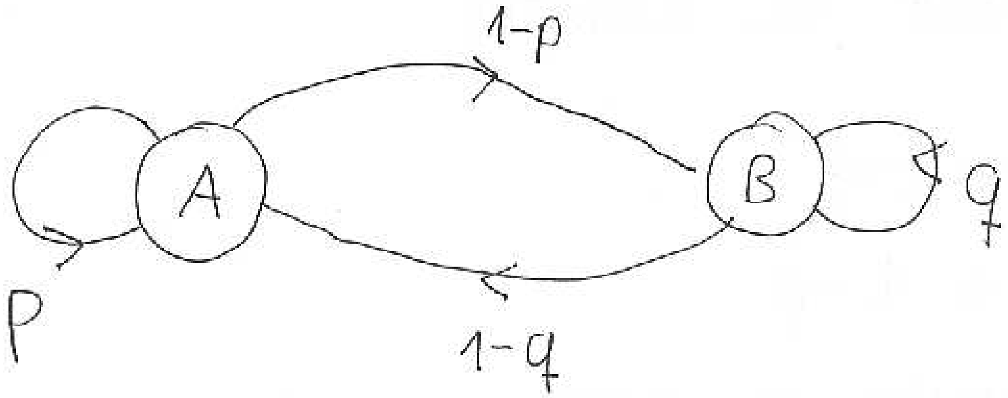
a) Sabiendo que N= 11 * 17 * 31 = 5797, calcule de la forma más eficiente que se le ocurra $X = 7^{4805} \bmod 5797$. **(1 punto)**

b) Considere un alfabeto formado por las vocales {A, E, I, O, U}. Realice un cifrado de Vignere del mensaje M=AAEIUOAEIOAI, utilizando la clave k=AIOU. **(1 punto)**

c) Sea una red de usuarios en los que son públicos los valores $\alpha = 5$ y $p = 31$.Especifique un protocolo para que dos usuarios A y B, sin hacer uso de terceras partes de confianza y sin compartir previamente ningún secreto, acuerden una clave de sesión k_{AB}. Obtenga el valor k_{AB} para el caso de que A y B generen respectivamente los números aleatorios $x_A = 13$ y $x_B = 17$. NOTA: Suponga que sobre el canal de comunicaciones sólo son posibles ataques pasivos. **(2 puntos)**

d) Dado $x_A = 13$ del apartado anterior, ¿qué valor debe tomar x_B para que $k_{AB} = 5$? **(1 punto)**

PROB 1



FUENTE BINARIA CON $P(A|A) = p$
$P(B|B) = q$

a) ENTROPIA DE LA FUENTE en función de p y q

$$H(F) = p(A)\, H(F|A) + p(B)\, H(F|B)$$

$$H(F|A) = -p \log_2 p - (1-p) \log_2 (1-p)$$
$$H(F|B) = -q \log_2 q - (1-q) \log_2 (1-q)$$

$$(1-p)\, P(A) = (1-q)\, P(B)$$
$$P(A) = \frac{1-q}{1-p}\, P(B)$$

$$\boxed{\begin{array}{l} P(A) = \dfrac{1-q}{2-p-q} \\ P(B) = \dfrac{1-p}{2-p-q} \end{array}}$$

$$P(A) + P(B) = 1$$

$$\left(\frac{1-q}{1-p} + 1\right) P(B) = 1 \qquad \frac{1-q+1-p}{1-p}\, P(B) = 1$$

b] PARTICULARIZE PARA $p = 1 - q$ $(p+q=1)$
JUSTIFIQUE EL RESULTADO

$$P(A) = 1-q$$

$$P(B) = 1-p$$

LA FUENTE NO TIENE MEMORIA

$$\boxed{H(F) = -\overset{p}{(1-q)} \log_2 \overset{p}{(1-q)} - (1-p) \log_2 (1-p)}$$

c] $p = q$

C.1] ENTROPIA FUENTE

$$H(F) = -p \log_2 p - (1-p) \log_2 (1-p)$$

C.2] Prob de que la fuente emita ráfagas de long $L=k$ y Longitud media de las ráfagas

$$\text{Prob}\,[L=k] = p^{k-1} (1-p)$$

PARA $p = 3/4$ codif Huffman longitudes

$$\text{prob}\,[L=1] = \frac{1}{4} \qquad P[L=k] = 0'25 \cdot (0'75)^{k-1}$$

$$\text{prob}\,[L=2] = \frac{3}{4} \cdot \frac{1}{4} = \frac{3}{16}$$

$$\text{prob}\,[L=3] = \frac{9}{16} \cdot \frac{1}{4} = \frac{9}{64}$$

$$\text{Prob}\,[L=4] = \frac{27}{64} \cdot \frac{1}{4} = \frac{27}{256}$$

d) $C = 5 \cdot 10^3$ bps

$V_t = 100.000$ símbolos/seg $\Rightarrow$

$I = V_t \cdot t$

$100.000\ H(F) = 5 \cdot 10^3 \cdot 10$

$\boxed{H(F) = 0'5}$

$(1-p)\log_2(1-p) + p\log_2 p = 0'5$

$\boxed{p = 0'89}$ $(0'875 - 0'9)$

$= 0'875$

$0'9$

LZ77

A B C C A B C D

| (0,0) A | (0,0) B | (0,0) C | (1,1) A | (4,2) D |

0000.0000. 0000.0001 | 0000.0010 | 0001 0100 | 0100 1011

| ∅ ∅ | ∅ 1 | ∅ 2 | 1 4 | 4B |

PROB 2

a) $N = 11 \cdot 17 \cdot 31 = 5747$
$\phi(N) = 10 \cdot 16 \cdot 30 = 4800$ } $x = 7^{4805} \bmod 5747$?

$x = 7^{(\phi(N)+5)} \bmod 5747 = 7^5 \bmod 5747 =$

$\boxed{x = 5213}$

b) M = AAEIUOAEIOAI
k = AIOU AIOU AIOU

$\boxed{\text{AIUEUAOAIAOE}}$ C

c) D-H

$K_{AB} = \alpha^{X_A X_B} \bmod p = 5^{17 \cdot 13} \bmod 31 = \boxed{25}$

d) $X_A \cdot X_B = k\,\phi(N) + 1$

$\phi(31) = 30$ $\boxed{13\, X_B = k \cdot 30 + 1}$

$\boxed{X_B = 7}$ *

$K_{AB} = 5^{91} \bmod 30 = 5$ $\boxed{X_B = 28}$ también

ó $X_B = 4$

$$30 = 1 \cdot 30 + 0 \cdot 13$$

$$(-2) \quad 13 = 0 \cdot 30 + 1 \cdot 13$$

$$(-3) \quad 4 = 1 \cdot 30 + (-2) \cdot 13$$

$$1 = (-3) \cdot 30 + 7 \cdot 13$$

$$\boxed{x_B = 7}$$

$$\begin{array}{l|l} 13 & 3 \\ 1 & 3 \end{array}$$