CONTROL DE TRANSMISIÓN DE DATOS. 14 de diciembre de 2007

GRUPO 40

Notas Importantes:

1. Un error conceptual grave, puede anular todo el problema.

Problema 1. CODIFICACIÓN DE FUENTE (50%)

Sea una fuente binaria $F_1=\{-1, 1\}$, con $P(F_1=-1)=2P(F_1=1)$. Sea una fuente (F) cuya salida es la suma del símbolo actual y el símbolo anterior de F_1, es decir, el símbolo de F en el instante i vale: $F(i) = F_1(i) + F_1(i-1)$

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

b) Determine un modelo markoviano de **F** y calcule la entropía de **F** (suponiendo memoria 1)

c) Calcule la información mutua **$I(F, F_1)$**

d) Realice una codificación aritmética de la secuencia -2 0 2 -2 generada por la fuente anterior.

Problema 2. CRITOGRAFÍA (50%)

Alice desea enviar a Bob el mensaje en claro HOLA cifrando con el sistema RSA byte a byte.
Los datos son:

	Clave de **A**lice	Clave de **B**ob
Primo p	43	31
Primo q	61	59
Clave pública e	19	13

Se pide:

a) Calcule la clave privada de Alice.

b) Usando el algoritmo de exponenciación rápida cifre sólo el primer byte del mensaje HOLA que Alice desea enviar de forma confidencial a Bob. Use la codificación ASCII para codificar el mensaje: H_{ASCII} = 0100 1000

c) Calcule la firma de Alice sobre el último byte de la palabra HOLA (A_{ASCII} = 0100 0001). Suponga que H(M)=00000101.

d) Alice y Bob desean intercambiar una clave usando el algoritmo de Diffie y Hellman. El primo elegido es p=661 y como generador han optado por $\alpha = 6$. Alice elige el valor privado $x_A = 12$, mientras que Bob elige x_B=8. Calcule la clave de sesión que se intercambian Alice y Bob.