Control de Transmisión de Datos.

Grupo 50. 5 de diciembre de 2003.

Notas:

1. Los resultados no justificados no serán tenidos en cuenta.
2. Los problemas se entregarán por separado, numerando las hojas y poniendo nombre y apellidos en cada hoja.
3. Un error conceptual grave puede anular todo el problema.

Problema 1 (5 puntos).

Responda a las siguientes cuestiones sobre codificación de fuente.

a) Qué propiedad deben cumplir los símbolos que genera una fuente para que la codificación de *Huffman* que se aplique resulte beneficiosa (aporte algún beneficio).

b) Sea $\mathbf{F_1}$ una fuente que ha emitido la secuencia de caracteres AAAABBCD.

   b.1) Genere el código *Huffman* binario asociado (utilice 

).

   b.2) Calcule el número de bits necesarios para transmitir la secuencia anterior.

   b.3) Calcule la longitud media del código *Huffman* diseñado.

   b.4) Calcule la eficiencia del código *Huffman* diseñado.

   b.5) Determine cuál es el ahorro en recursos al utilizar el código *Huffman* diseñado respecto de utilizar un código ASCII de 7 bits por carácter.

c) Determine si existe algún código instantáneo en estos dos casos:

   c.1) Fuente que emite 10 símbolos diferentes y utiliza un código con alfabeto de 4 símbolos. Las longitudes de las palabras código son {1, 1, 1, 2, 2, 2, 2, 3, 3, 3}.

   c.2) Fuente que emite 5 símbolos diferentes y utiliza un código con alfabeto de 3 símbolos. Las longitudes de las palabras código son {1, 1, 2, 2, 3}.

d) Sea una fuente $\mathbf{F_2}$ que emite 10 símbolos diferentes {A, B, C, D, E, F, G, H, I, J} con probabilidades {0.05, 0.05, 0.05, 0.05, 0.1, 0.1, 0.1, 0.1, 0.2, 0.2} respectivamente y unas longitudes de las palabras código {1, 2, 2, 2, 3, 3, 3, 3, 3, 3} respectivamente. El alfabeto del código tiene 4 símbolos {a, b, c, d}. Determine si es posible hallar un código fuente más eficiente que el utilizado.

e) En caso afirmativo, proponga uno y calcule la eficiencia del código propuesto. En caso negativo, justifique el porqué.

f) Considere otra fuente $\mathbf{F_3}$ que utiliza el mismo alfabeto código que $\mathbf{F_2}$ (apartado d). Esta fuente $\mathbf{F_3}$ emite dos símbolos A y B. La fuente $\mathbf{F_3}$ emite sus símbolos según estas reglas:

   - Cuando $\mathbf{F_2}$ emite un símbolo del conjunto {A, B, C, D, E} la fuente $\mathbf{F_3}$ emite A.
   - Cuando $\mathbf{F_2}$ emite un símbolo del conjunto {F, G, H, I, J} la fuente $\mathbf{F_3}$ emite A con probabilidad 0.2 y B con probabilidad 0.8.

   Obtenga la entropía conjunta de ambas fuentes.

Problema 2 (5 puntos).

Sea un sistema de clave pública RSA. Considere dos usuarios A y B y una entidad CA que expende certificados para autenticar el origen de los mensajes. Los usuarios del sistema utilizan criptografía asimétrica RSA para intercambiar una clave de sesión, utilizada a su vez para codificar mensajes mediante cifrado en flujo síncrono. Las secuencias binarias se consideran con más peso a la izquierda (MPI).

El algoritmo de cifrado en flujo trabaja sobre bloques de 2 bits, donde el mensaje de entrada se coloca como estado inicial de un LFSR con polinomio de conexiones $c(D)=D^2+D+1$. El criptograma se obtiene como el estado del LFSR al cabo del número de iteraciones que indique la clave de sesión.

Parámetros RSA de los usuarios y la entidad certificadora, e identificadores de cada usuario:

Usuario A	p_A=3, q_A=11, e_A=3	ID_A=0001
Usuario B	p_B=7, q_B=17, d_B=35	ID_B=0010
Entidad certificadora CA	p_{CA}=7, q_{CA}=11, d_{CA}=13	

La función de *Hash* H(M) de un mensaje M, que se emplea en el sistema es la siguiente:

- Las secuencias binarias se consideran con más peso a la izquierda (MPI).
- Se añaden a la izquierda del mensaje tantos unos como sea necesario para que la longitud sea múltiplo de 4.
- Se divide el mensaje resultante desde la izquierda en n bloques de 4 bits, m_i $0 = i = n-1$.
- $h_{i+1}=E(h_i \text{Å} m_i)$, $0 = i = n-1$, siendo $h_0=4$.
- La función $E(\cdot)$ es un cifrador bloque que convierte un bloque $entra_i$ de 4 bits en otro bloque $sale_i$ de acuerdo con la expresión: $sale_i=E(entra_i)=(5*entra_i+2) mod 16$.
- $H(M)=h_n$
- $H(M)$ debe ocupar 4 bits y expresarse en hexadecimal.

La autoridad certificadora CA sigue el siguiente esquema para expender los certificados: Un usuario i entrega a la CA el certificado en claro correspondiente a la concatenación (||) de su identificador ID_i y de su clave pública K_{Pi}. La CA firma digitalmente dicho certificado en claro y añade la firma detrás: *Certificado firmado = certificado en claro || firma digital.*

a) Genere las claves pública y privada de los usuarios A y B.

b) Obtenga los certificados que la entidad CA genera a los usuarios A y B. Exprese los certificado en claro y los certificados firmados en hexadecimal.

c) A y B desean intercambiar una clave de sesión para cada sentido de la comunicación: $K_{A->B}$=10 y $K_{B->A}$=5. Enumere los pasos del protocolo a seguir para lograr dicho intercambio, de forma que cada usuario autentique al otro.

d) Codifique las claves de sesión que se intercambian A y B.

e) A envía el mensaje M_{AB}=0010011011 a B. B responde con el mensaje M_{BA}=111001 a A. Cifre dichos mensajes con el algoritmo de cifrado en flujo para codificar mensajes descrito en el enunciado.