Control de Transmisión de Datos.

Grupo 30. 23 de mayo 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).

Sea un sistema de transmisión de datos que tiene implementados los servicios de seguridad confidencialidad, autenticación de origen y de contenido. Considere dos usuarios A y B y una entidad CA que expende certificados utilizando clave pública RSA. Los usuarios del sistema utilizan criptografía asimétrica RSA para intercambiar una clave de sesión, utilizada a su vez para codificar mensajes mediante la técnica de sustitución monoalfabética monográmica vista en clase (*cifrado de César*).

Considere estos datos numéricos para los usuarios y la entidad certificadora, donde en la primera columna dispone de los parámetros RSA (recuerde que cada valor debe ocupar un octeto al expresarlo en binario) y en la segunda columna de los identificadores de cada usuario dentro del sistema (en binario):

Usuario A	p_A=3, q_A=11, d_A=7	ID_A=00001111_b
Usuario B	p_B=5, q_B=11, e_B=3	ID_B=11110000_b
Entidad certificadora CA	p_{CA}=7, q_{CA}=17, d_{CA}=5	

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

- Las secuencias binarias se consideran con más peso a la izquierda (MPI).
- Se añaden al inicio del mensaje tantos unos como sea necesario para que la longitud sea múltiplo de 6.
- Se divide el mensaje resultante desde la izquierda en n bloques de 6 bits, m_i $0 \le i \le n-1$.
- $h_0=DCD(m_0)$, siendo DCD = Desplazamiento Circular a Derecha.
- $h_{i+1}=DCD(h_i \oplus m_{i+1})$, $0 \le i \le n-2$.
- $H(M)=h_{n-1}$
- $H(M)$ debe ocupar un octeto.

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 (utilice el símbolo || para indicar 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.*

El usuario A desea enviar el mensaje "apuesta por flecha" al usuario B. Una vez que B haya apostado por el caballo *Flecha*, responderá con "apuesta flecha ok". La clave de sesión utilizada es 5.

a) Enumere y explique paso a paso qué acciones irá realizando cada identidad del sistema en orden secuencial. Calcule los mensajes que se irán intercambiando las entidades implicadas. Indique claramente en los recuadros los resultados parciales que vaya obteniendo señalando claramente cuál es la composición de cada mensaje.

Problema 2 (5 puntos).

Sea una fuente F_1 de Markov, con memoria de segundo orden, con un alfabeto binario {0, 1}. Suponga que las probabilidades condicionales son:

P(0\00) = P(1\11) = 0.8

P(1\00) = P(0\11) = 0.2

P(0\01) = P(0\10) = P(1\01) = P(1\10) = 0.5

a) Averigüe las probabilidades estacionarias de cada estado.

b) Calcule la entropía de la fuente F_1.

c) Suponga ahora que la fuente binaria no tuviera memoria. Calcule la entropía de la fuente resultante F_2 para la misma probabilidad de emisión de los símbolos. Comente el resultado obtenido.

d) Calcule la eficiencia del código Huffman para la fuente F_2.

e) Calcule o al menos acote la entropía conjunta de las fuentes F_1 y F_2. Calcule $H(F_1/ F_2)$ y $H(F_2/F_1)$.

f) Halle la codificación Lempel-Ziv (LZ-78) de la secuencia binaria 101011010010011101010000. Considere que el diccionario tiene capacidad para almacenar las 16 palabras más utilizadas. Las posiciones se numeran de la 1 a la 16, en binario. Cada palabra código se determina así:

- Todos los bits de la posición en el diccionario (en binario) de la frase previamente introducida que es igual a la actual excepto en el último bit. Y se añade al final el último bit de la nueva frase introducida. Inicialmente, se parte de 0000 seguido de la nueva frase, para codificar una frase inicial que no ha aparecido aún.

Discuta sobre el valor de la tasa de compresión alcanzado.

Control de Transmisión de Datos. Hoja de respuestas.

Grupo 30. **23 de mayo de 2003.**

Nombre: ____

Problema 1.

Nombre de la acción:
Mensaje intercambiado:
Resultado:

Nombre de la acción:
Mensaje intercambiado:
Resultado:

Nombre de la acción:
Mensaje intercambiado:
Resultado:

Nombre de la acción:
Mensaje intercambiado:
Resultado:

Nombre de la acción:
Mensaje intercambiado:
Resultado:

Nombre de la acción:
Mensaje intercambiado:
Resultado:

Nombre de la acción:
Mensaje intercambiado:
Resultado:

Nombre de la acción:
Mensaje intercambiado:
Resultado:

Nombre de la acción:
Mensaje intercambiado:
Resultado:

Nombre de la acción:
Mensaje intercambiado:
Resultado:

Problema 2.

a)

P(00) =	P(01) =
P(10) =	P(11) =

b)

$H(F_1)$ =

c)

$H(F_2)$ =

d)

E =

e)

$H(F_1, F_2)$

$H(F_1/ F_2)$ =

$H(F_2/F_1)$ =

f)

tasa compresión =

justificación =