Segundo Certamen Tiempo: 90 min

Si algo está poco claro, anote un supuesto razonable y responde conforme a éste.
Todas las preguntas tienen igual puntaje. Sea breve en su respuestas.

1.- En comparación con la TV analógica ¿Qué características del estándar ISDB-T permiten recibir imágenes con menos ruido y sin fantasmas?
Menos ruido: ISDB-T incluye códigos correctores de errores lo cual permite corregir información que en televisión analógica se muestra como ruido.
Sin fantasmas: esto se logra gracias a la codificación OFDM.

2.- a) Mencione un ejemplo de aplicación interactiva con interactividad local.
b) Dé un ejemplo de aplicación interactiva sincronizada con programa.

a) Un juego tipo solitario o similar. También una aplicación para conocer los indicadores económicos cuando éstos son enviados a través del transport stream.
b) Una aplicación de encuesta o información sobre alguna materia que se esté tratando en el programa de televisión.

3.- Mencione una diferencia entre el estándar ISDB-T japonés y el brasileño.
El estándar brasileño incorporó GINGA en lugar del middleware de aplicaciones del estándar japonés (ése se llama ARIB).
(Otra el estándar brasileño incorporó codificación MPEG4 para el video, el japonés definió MPEG2)

4.- Explique cuál es la diferencia entre un lenguaje del tipo declarativo respecto a uno imperativo. Dé un ejemplo de cada uno.
En los lenguajes de tipo declarativo el énfasis está en expresar qué deseamos obtener como resultado, en los imperativos se indican los pasos para llegar al resultado.
(Otra: Los lenguajes declarativos son más específicos al tipo de programación deseado, mientras los declarativos son de propósito más general.)
Ejemplo de declarativo: NCL, ejemplo de imperativo Lua.

5.- NCL es un acrónimo de “Nested Context Language” ¿Qué característica de NCL lo hace ser anidado?
Se dice que es anidado porque un medio puede a su vez ser otro programa NCL.

6.- ¿Para qué se usa el rótulo “area” en NCL?
Se usa para definir un rango de tiempo dentro de la duración de un medio. Así es posible sincronizar otros medios con un punto intermedio de otro en lugar de hacerlo sólo con su inicio o término.

7.- Mencione una ventaja de crear una aplicación interactiva con NCL-Composer respecto de trabajar con Eclipse. Mencione una ventaja de trabajar con Eclipse respecto de trabajar sólo con NCL-Composer.
Ventaja de NCL-Composer respecto de Eclipse. Con NCL-Composer podemos indicar más fácilmente las regiones y tener una vista de cómo quedan en la aplicación. NCL-Composer es gráfico, con lo cual facilita la programación NCL de noo especialistas en programación.
Ventaja Eclipse: Permite desarrollar aplicaciones que incluyan programación Lua.

6.2.- Mencione dos diferencias entre una red de sensores que usa 802.15.4 y una red de nodos

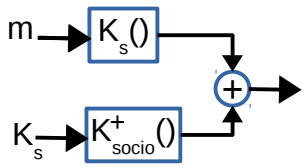
conectados vía WiFi. Considere un escenario donde un dueño de parcela desea poner una cámara de video de alta calidad para monitorear un sector de su terreno, y el caso en que el mismo agricultor desea monitorear la humedad de varios puntos de su parcela. Justifique su respuesta.
Caso video: Se hace notar la diferencia en capacidad de tráfico; en 802.15.4 la tasa es mucho menor que en WiFi. Como es un sólo punto WiFi puede ser opción haciendo llegar energía a ese punto.
Caso monitoreo de humedad: Como son varios nodos que enviarán pocos datos, se hace notar la diferencia en menor consumo de energía de las redes de sensores con 802.15.4 respecto de WiFi.

7.2.- Explique dos razones a por qué nesC es mejor lenguaje que C para programar aplicaciones de redes de sensores inalámbricos.
** nesC es mejor porque en redes de sensores inalámbricos se requiere responder a múltiples eventos, nesC permite definir múltiples eventos de espera mientras que C es secuencial, por lo cual habría que programar mucho para otorgar servicios de manejo de eventos en arquitectura pequeñas.*
** nesC permite definir hace un mejor manejo de los recursos para responder en tiempo real evitando estados de espera; por ejemplo, esperar por un dato de un conversor A/D o el envío exitoso de un mensaje..*
** otras: nesC ofrece un mecanismo para definir abstracciones del hardware, nesC permite definir zonas atómicas para variables que son accedidas por varios eventos (interrupciones).*

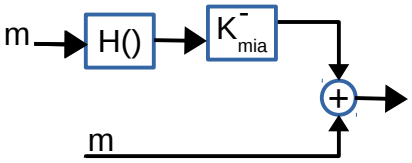
8.- Mencione una ventaja del cifrado de clave pública respecto al de clave simétrica. Mencione una ventaja del cifrado de clave simétrica respecto del de clave pública.
Clave pública resuelve el problema de distribución de claves presente en cifrado de clave simétrica.
Cifrado de clave simétrica es más rápido de procesar que el de clave pública.

9.- Qué ventaja tiene el cifrado de bloques en cadena respecto al cifrado de bloques (no en cadena).
Cifrado de bloques en cadenas genera mensajes cifrados distintos cuando un mismo texto se repite; esto no se garantiza en cifrado de bloques no en cadena.

10.- Usted tiene un mensaje m que desea enviar a su socio(a). Para cada caso, muestre un diagrama de bloques indicando los mecanismos a usar para conseguir:
a) sólo confidencialidad.
b) sólo autenticación.
La autenticación y la integridad de un mensaje van de la mano. Sí se debe diferenciar de la confidencialidad que puedo o no ir junto a la autenticación.



Sólo confidencialidad



Autenticación se caracteriza por el uso de clave privada de la fuente

11.- Usted recibe un mensaje de un cliente el cual viene: una orden de trabajo firmada y la clave pública del cliente.
¿Cómo usted puede verificar que ese pedido fue escrito por ese cliente?
¿Es posible verificar que el mensaje fue enviado por el cliente?
Explique.

Puedo verificarlo siempre y cuando la clave pública venga firmada por una autoridad certificadora que yo pueda reconocer como tal. En ese caso verifico que la clave pública pertenece al cliente y luego verifico la firma que el cliente hizo al pedido usando su clave pública.

Con sólo recibir el mensaje no puedo verificar que éste fue enviado por el cliente. Bien pudo ser una repetición de un pedido antiguo de él. Otra cosa sería si antes yo le he enviado un número único que el cliente incluye en el mensaje y así puedo verificar que no se trata de un mensaje repetido. Otra opción es que las órdenes de trabajo vengan numeradas secuencialmente por cliente. (pueden haber otros mecanismos para descubrir duplicidad)

12.- ¿Cómo se diferencia una lista de control de acceso (ACL) entre un cortafuegos con estado y uno sin estado? Explique.

La ACL de un cortafuegos con estado tiene una columna más para indicar si el estado de la conexión debe ser verificado. Esta columna no está presente en los cortafuegos sin estado.