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.- Mencione dos razones que justifiquen el envío de una señal separada para equipos móviles (one-seg) y no pedir que éstos reciban el mismo programa sintonizando la señal enviada para receptores fijos.
** Los equipos móviles en general poseen menor resolución que las pantallas grandes de equipos fijos. Entonces se justifica enviar imagen de calidad ajustada a estos receptores con codificación más robusta pues están sometidos a mayores variaciones del canal.*
** La limitación de recursos de CPU y energía hacen recomendable el envío de una señal ocupe menos recursos para su visualización.*

2.- En ISDB-Tb, además de video, mencione tres flujos de paquetes que pueden ser trasmitidos asociados a un mismo programa.
Además del video se puede transmitir: Varios canales de audio, la guía electrónica de programación, aplicaciones GINGA.

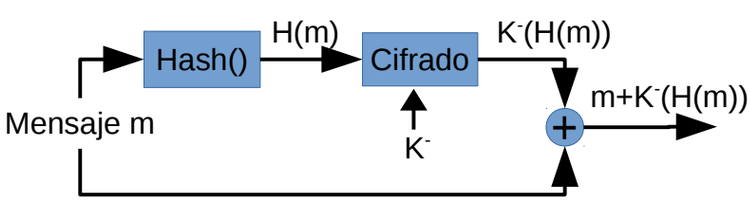
3.- ¿En Nested Context Language (NCL) qué rótulo permite especificar el o los medios a ser mostrados al iniciar una aplicación GINGA-NCL?
GINGA definió dos lenguajes para desarrollar aplicaciones interactivas: NCL (GINGA-NCL) y Java (GINGA-J). ¿Qué razón han dado algunos países para no apoyar el desarrollo de aplicaciones GINGA-J?
El rótulo <port> especifica los medios a mostrar al inicio.
Java fue desarrollado por SUN, empresa que luego fue adquirida por Oracle. Desde entonces el uso de una máquina virtual Java requeriría el pago de licencias que encarecen cada receptor. NCL y Lua son lenguajes código abierto.

4.- Mencione dos ventajas de poder incluir código LUA en aplicaciones GINGA-NCL.
** A través de LUA es posible incluir programación procedural, la cual complementa la declarativa de NCL, pues hay lógicas mucho más simples de expresar en un lenguaje procedural.*
** LUA es un lenguaje muy desarrollado; por ejemplo, en programación de juegos, así con el uso de LUA se puede acceder a módulos para programación en red entre otros.*
** LUA es código abierto y su interpretador ocupa muy poco espacio.*

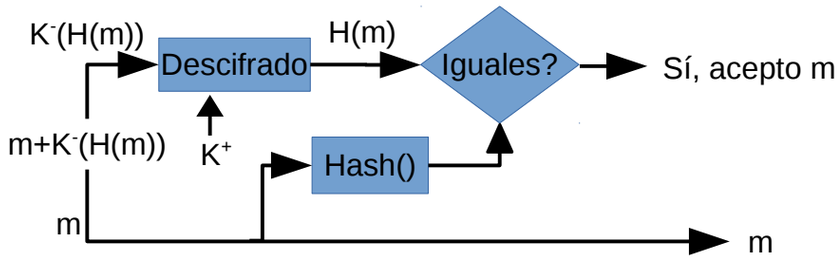
5.- ¿Por qué se dice que las redes de sensores inalámbricos son redes multihop?
Porque los mismos nodos pueden ser usados como elementos de ruteo para alcanzar a equipos más lejanos.

6.- En el contexto de NesC, ¿Qué ventaja tiene hacer que las funciones sean in-line? Explique su respuesta.
Se logra mayor optimización en tamaño de código y tiempo de ejecución (o uso de CPU). Esto se logra porque en los lugares donde hay llamados a función el compilar pone allí el código de la función misma. Esto ahora código cuando las funciones son pequeñas (se ahora el paso de parámetros y el código asociado al salto y retorno). También hay ahorra CPU porque no se rompe la secuencia del pipeline propia de los procesadores actuales.

7.- Dos personas desean comunicarse vía Internet y cada una conoce la clave pública de la otra. Sugiera un esquema de comunicación de mensajes que provea autenticación de fuente. Muestre esquema para el transmisor y para el receptor. Además de autenticación de fuente, consigue usted algún otro servicio de seguridad?
Esquema transmisor:



Esquema receptor:



Además se consigue integridad del mensaje.

8.- ¿Por qué el estándar 802.11 WEP incluye un vector de inicialización en cada paquete? ¿Se lograría el mismo resultado si el vector de inicialización fuera cifrado? Explique.
Lo incluye para garantizar que dos mensajes iguales puedan generar versiones cifradas distintas.
Sí. En el caso que el vector de inicialización vaya cifrado, éste en receptor debe poseer la clave de descifrado para así poder descifrar el respto del mensaje usando el VI.

9.- Sitios como gmail.com utilizan https y todo funciona normal para el usuario aún cuando los datos enviados a través de la capa de transporte van cifrados (usando SSL por ejemplo). Otros sitios, como https://git.elo.utfsm.cl/, generan un mensaje de advertencia del tipo: “This Connection is Untrusted...” ¿Qué explica la diferencia? ¿Qué permite a su navegador no mostrar esa advertencia cuando usted accede a gmail?
La diferencia se explica por el certificado de clave púbica que hace llegar el servidor. En el caso gmail, el servidor posee un certificado firmado por una autoridad certificadora acreditada y conocida desde ya por el navegador. Es así como el navegador puede comprobar que el servidor es quien dice ser (y no un impostor). En el caso git.elo.utfsm.cl, el certificado no está firmado por un ente reconocido por el navegador (esto involucra un costo). Esta opción se suele usar al interior de instituciones para servicios locales donde ellos firmas sus certificados.

10.- Menciones una ventaja de SSL respecto a IPsec. Mencione una ventaja de IPsec respecto de SSL.
** SSL permite dar confidencialidad a los datos de una comunicación de un servicio sin requerir de alguna aplicación o configuración previa. IPsec requiere tener software (o routers) específico y configurado para comunicarse con una contra-parte específica.*
** IPsec tiene ventaja cuando se desea dar confidencialidad a todo el tráfico entre un usuario y otra red o entre dos redes. Esto permite dar confidencialidad a todo tipo de tráfico (UDP, TPC, etc) cosa lo lograda con SSL. Además IPsec permite dar anonimato a la aplicación e IPs de los entes que se comunican.*