Segundo Certamen

Tiempo: 90 min

Nombre: _____

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 equipos del laboratorio de TV digital del Departamento de Electrónica que participan para transmitir un programas de televisión bajo la norma ISDB-Tb.
** Computador para acceder al modulador OFDM.*
** Modulador OFDM (o Playout en caso Lab ELO, USM)*
** Amplificador de potencia de la señal de modulada.*

2.- El plan de adopción de la televisión digital Chile, exige a las concesionarias (estaciones de TV) dimensionar sus equipos para transmitir al menos dos señales -programas- (HD y SD). Si ISDB-Tb permite enviar hasta 8 programas distintos ¿qué motiva a las concesionarias a dimensionar sus equipos para transmitir pocos programas simultáneamente?
La transmisión de más programas obliga a usar esquemas de codificación de mayor eficiencia (mayor número de bits por símbolo). Esto obliga usar amplificadores de mayor potencia para alcanzar buena relación señal a ruido dentro de la zona de cobertura. Los amplificadores de mayor potencia no solo son más caros sino también generan mayor costo operacional para las estaciones. Es por eso que las concesionarias tratan de ocupar la menor potencia posible para cubrir su zona de interés y eso se logra con esquemas de modulación más robustos que transmiten una menor tasa de bits en los 6 MHz asignados.

3.- Mencione qué información multiplexan cada una de las dos etapas de multiplexación de paquetes de la norma ISDB-Tb.
La primera etapa multiplexa los paquetes de los distintos flujos que componen un programa (video, audios, datos).
La segunda etapa multiplexa los paquetes que provienen de los distintos programas.
(Recordar que en los 6 MHz asignados es posible enviar varios programas y cada programa está compuesto de varios streams o flujos de datos).

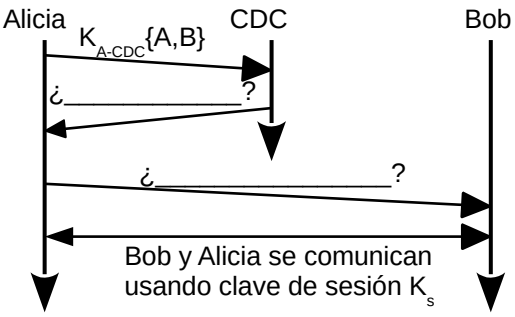
4.- ¿Qué característica define que una red inalámbrica sea **Ad-hoc**? ¿Qué característica define que una red inalámbrica sea **Multihop**?
Una red es ad-hoc si es establecida entre los mismos nodos terminales y no usa infraestructura pre-instalada.
Una red es multihop cuando los nodos terminales participan del ruteo de paquetes hacia nodos inalámbricos fuera del espacio de cobertura del transmisor.

5.- Mencione dos características consideradas en el diseño del lenguaje nesC (Networked Embedded System C) para responder a requerimientos “Soft real-time” (tiempo real no crítico).
** Modelo de concurrencia conducido por eventos.*
** Excluir manejo dinámico de memoria y punteros a funciones para permitir optimización automática del código.*
** Inclusión de operaciones de fase partida (operaciones en dos etapas).*

6.- ¿Qué significa que el límite HW/SW (hardware/software) de TinyOS puede variar dependiendo de la aplicación y la plataforma de hardware usada? (Obs.: considere que usted tiene una aplicación nesC y la compila e insta en dos plataformas de hardware levemente distintas.)
TinyOS contiene componentes basadas en los módulos de hardware disponibles en cada plataforma.

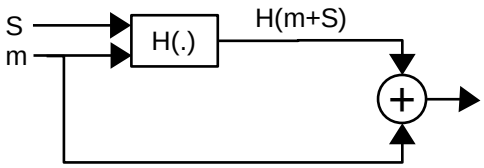
Cuando un módulo no existe directamente y éste puede ser ofrecido vía una configuración de otros módulos presentes. Por esta razón al compilar una aplicación se debe especificar la plataforma destino de la cual se usarán más o menos configuraciones según los recursos de hardware de la plataforma.

7.- Una estrategia para distribuir una clave simétrica a dos usuarios Alicia y Bob utiliza un centro de distribución de claves (CDC). El CDC es un servidor que comparte una clave secreta simétrica con cada usuario registrado en él. Estas claves son diferentes entre usuarios. Para los usuarios registrados Alicia (A) y Bob (B) denote estas claves simétricas como $K_{A\text{-}CDC}$ y K_{B_CDC}. Proponga una estrategia que use el CDC y distribuya una clave simétrica K_s a usar en la comunicación entre Alicia y Bob. La estrategia debería usar 3 mensajes para distribuir la clave de sesión: un mensaje de Alicia al CDC (mostrado); un mensaje del CDC a Alicia; y un mensaje de Alicia a Bob. Complete dos mensajes de la figura. $K_{A\text{-}CDC}\{A,B\}$ corresponde a "A,B" encriptado con clave $K_{A\text{-}CDC}$



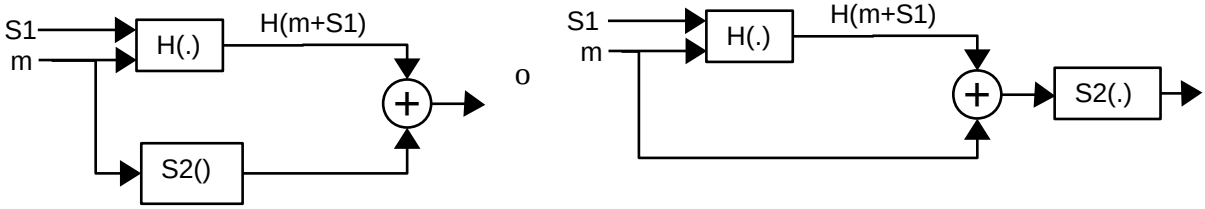
Mensaje del CDC a Alicia: $K_{A\text{-}CDC}\{K_s, K_{B\text{-}CDC}\{A,K_s\}\}$
Mensaje de Alicia a Bob: $K_{B\text{-}CDC}\{A,K_s\}$

8.- a) ¿Qué servicio(s) provee el esquema adjunto? S: es un secreto compartido, m el mensaje y H la función de hash.



Se provee Integridad (se puede reconocer autenticación)

b) Suponga que el transmisor y el receptor comparten dos claves secretas: una clave de autenticación S1 y una clave de encriptación simétrica S2. Complete (o modifique) el esquema dado en **a** para proveer integridad y confidencialidad.



9.-a) ¿Qué ataque se resuelve en SSL al incorporar números de secuencia?
Si los mensajes con cambiados de orden, SSL lo detecta.

b) ¿Qué ataque se resuelve en SSL al usar un número único (random nonce)?
El ataque de reproducción es detectado.

10.- a) ¿Cuál es la función que cumplen las autoridades certificadoras?
Verificar la identidad de los solicitantes y firmar sus claves públicas.

b)¿Cómo su navegador obtiene la clave pública de una autoridad certificadora?

Ésta viene incluida en el software del navegador desde el momento de su instalación.

Solo para estudiantes cursando IPD438: Preguntas basadas en el artículo: “10 tips for writing a truly terrible journal” By Bert Blocken, PhD. January 11, 2017

a) ¿Mencione dos recomendaciones dadas por el autor para hacer la revisión de (todo) lo publicado sobre un tema?

Acotar el campo de estudio específico y
Seleccionar lo publicado revisando los títulos y abstract de los artículos.
Con esas dos ideas se puede acotar el estudio de lo publicado en el campo de estudio del investigador.

b) ¿En relación a qué el doctor Blocken menciona que un artículo no es una novela? (o qué diferencia un artículo de una novela)

Un artículo científico no es una novela porque no debe dejar cosas a interpretación del lector. Si eso ocurre, el autor del artículo ha fallado. Una novela puede excluir metáforas o usar otros términos para no repetir una palabra. Mientras una novela puede contener ambigüedad, un artículo debe ser preciso y no debe dejar espacio a interpretaciones.