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 4 mejoras de la TV Digital respecto de la Televisión analógica.
** Calidad de sonido e imagen superior*
** Multiprogración: en el mismo ancho de banda es posible enviar varios programas*
** Envío de datos: Ej. aplicaciones interactivas, guía de programación, subtítulos.*
** Envío de señal de alerta de emergencia*
** Recepción en equipos móviles*

2.- Conforme la relación señal a ruido se deteriora, la televisión analógica **gradualmente** muestra un deterioro de imagen con un efecto comúnmente llamado "nieve". Por otra parte, conforme la relación señal a ruido se deteriora, la televisión digital (TVD) mantiene su calidad de imagen hasta un punto en que de **forma abrupta** ésta se torna irreconocible ¿Qué mecanismo de la TVD explica este comportamiento?
La presencia de códigos correctores de errores en los datos enviados. Estos códigos logran corregir errores en los datos hasta cierto nivel de error. Pasado este umbral, la recuperación del códigos no logran su propósito y la imagen se torna irreconocible.

3.- En televisión analógica es común observar una superposición de la misma imagen original pero desplazada horizontalmente. Este efecto es comúnmente llamado "fantasma". Explique qué mecanismo de la televisión digital elimina la aparición de fantasmas en la imagen desplegada.
Este efecto se debe a la multi-trayectoria desde la antena transmisora hasta la receptora. Para eliminar este efecto, la TVD introduce un Tiempo de Guarda entre símbolos. Es decir hay un espacio entre símbolos de manera que evitar la superposición de éstos debido a multitrayectoria.
También se puede argumentar que la multi-trayectoría generaría una mala interpretación del símbolo lo cual se traduce en error pero no en imagen "fantasma".

4.- ¿Por qué la industria de la televisión en Chile, es decir, los canales de televisión, no han manifestado interés en impulsar GINGA?
Los canales de televisión no ven un modelo de negocios que dé ventajas a GINGA por sobre la presencia de los canales en portales Internet.
Su presencia en Internet permite además servicios no disponibles en GINGA, como la reproducción bajo demanda de programas pasados.

5.- Alguien comenta: "Para qué complicarse aprendiendo nuevos lenguajes y arquitecturas si para implementar cualquier red de sensores inalámbricos podríamos usar Raspberry Pi con módulos WiFi y programarlas de igual forma que cualquier otra aplicación distribuida en red". ¿Está usted de acuerdo? Justifique.
No. La Raspberry Pi + WiFi consume mucha energía y la hace no aplicable en situaciones donde los nodos de la red deben ser energéticamente autónomos por meses. Otra razón es su costo, algunas aplicaciones de monitorización de ambientes basta con hardware más básico y económico.

6.- ¿Bajo qué circunstancia un programador en lenguaje NesC requeriría definir un segmento de código como atómico?
Cuando ese segmento de código puede ser ejecutado por una tarea y desde manejador de interrupción.

7.- Considere un esquema de cifrado de bloques con tamaño de bloque de 64 bits.
a) Si la encriptación de cada bloque es hecha vía una función basada en 8 tablas de 8 bits de entrada y 8 bits de salida, ¿cuántos bits son necesarios para almacenar estas 8 tablas?
b) Si la encriptación de cada bloque es hecha vía una única tabla para mapear los 64 bits de entrada a 64 bits de salida, ¿cuántos bits son necesarios para almacenar esta tabla?

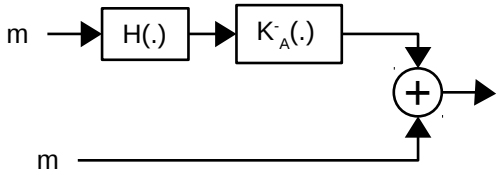
a)

$$Número\,de\,bits = 8[tablas] * 2^8[palabra/tabla] * 8[bit/palabra] = 2^3 * 2^8 * 2^3[bit] = 2^{14}[bit] = 16384[bit]$$

b) $$Número\,de\,bits = 2^{64}[palabra/tabla] * 64[bit/palabra] = 2^{64} * 2^6[bit] = 2^{70}[bit] \approx 10^{21}[bit]$$

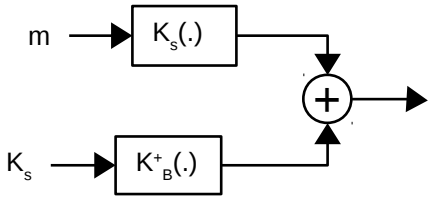
8.-Considerando el uso de Cifrado de Clave Pública para **enviar** un mensaje de correo:

a) A través de un diagrama en lado transmisor, muestre una estrategia para proveer integridad de mensaje, pero no confidencialidad.



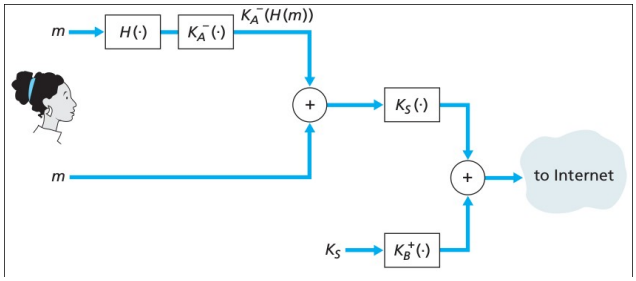
A es transmisor (Alice)

b) En otro diagrama en lado transmisor, muestre una estrategia para proveer confidencialidad pero no integridad de mensaje.



B es el Receptor (Bob)

9.- El esquema de la figura muestra una estrategia para enviar mensajes de correos. Mencione **dos razones** a por qué esta estrategia no es empleada en cada paquete intercambiado entre un browser y un servidor WEB al acceder al portal de un banco.



** Este esquema es ineficiente porque envía la clave simétrica (de sesión) cada vez. Es mejor enviarlas al comienzo de todos los mensajes entre browser y portal.*
** Esta estrategia no protege contra ataques de reproducción de un mensaje.*
** Esta estrategia no protege contra cambios de orden de los mensajes.*
** Esta estrategia no protege contra un cierre prematuro de la conexión.*

10.- Considere el siguiente protocolo pseudo-WEP. En éste la clave (secreto compartido) es de 4 bits y el IV (vector de iniciación) es de 2 bits. El IV es agregado a la clave para generar el flujo pseudoaleatorio (keystream). Suponga que el secreto compartido es 1010 y el keystream para IV=11 es: 1111101010000000 1010...
Suponga que todos los mensajes son de 8 bits. Suponga que el ICV (chequeo de integridad) es de 4 bits, y es calculado haciendo el OR-EX bit a bit de los primeros 4 bits de datos con los últimos 4 bits de datos. Suponga que el paquete pseudo-WEP consiste de tres campos: primero el campo IV, luego el campo mensaje, y el último el campo ICV, con algunos de estos campos encriptados igual que en WEP.
a. ¿Cuál sería el valor para los tres campos del paquete a enviar si el mensaje fuera 10100001 y IV=11?
b. ¿Qué puede decir respecto del mensaje enviado si el paquete recibido fuera: 11 00101100 0011

a) *Campo IV:* 11
ICV: 1010 OR-EX 0001 = 1011
Los campos dato e ICV van encriptados: 101000011011
OR-EX 111110101000
= 010110110011
Luego los tres campos a enviar son: 11 01011011 0011 *// 1 + 2 +2 pts*

b) Descifrando los datos e ICV: 001011000011
OR-EX 111110101000
= 110101101011
Luego el campo datos es: 11010110 *// 3 pts.*
recalculando ICV: 1101 OR-EX 0110 = 1011, *se verifica que el dato es íntegro. // 2 pts.*

Sólo para estudiantes cursando IPD438:
a) ¿Cuáles son las componentes claves de un artículo? Lístelas en el orden en que ellas deberían aparecer en su artículo.
** Resumen del estado del arte*
** Identificación de la brecha de conocimiento no cubierta*
** Especificar la novedad, los objetivos y alcance de la investigación*
** Descripción de la metodología de investigación usada*
** Resultados obtenidos*
** Conclusiones*

b) Mencione dos formas que muestran falta de respeto hacia el trabajo de publicaciones previas.
** Efectuar revisión limitada de la literatura ignorando parte parte de las publicaciones previas.*
** Atribuyendo el trabajo previo a autores equivocados*
** Proporcionando comentarios despectivos sobre las otras publicaciones*
** Sobre estimando la importancia o novedad de las contribuciones propias*