Enero 2016

1- Sobre el algoritmo Ricart-Agrawala:

a. Escribe el algoritmo.

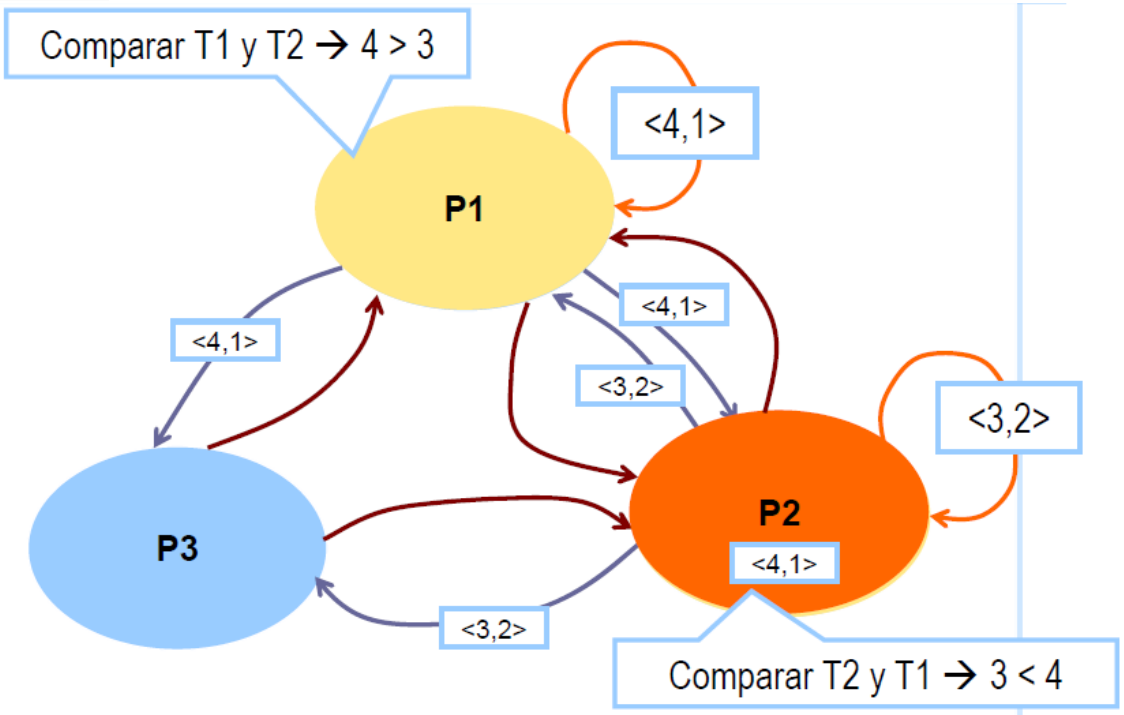
- **En la inicialización**
  estado := LIBERADA;

- **Para entrar en la sección crítica**
  estado := BUSCADA;
  Multitransmite *petición* a todos los procesos;
  T := marca temporal de la petición;
  ⇒ Se aplaza el procesamiento de peticiones
  Espera hasta que (número de respuestas recibidas = (*N* – 1));
  estado := TOMADA;

- **Al recibir una petición <T_i, p_i> en el proceso p_j (i ≠ j)**
  si (*estado* = TOMADA o (*estado* = BUSCADA *y* (*T*, p_j) < (T_i, p_i)))
  entonces
  pone en la cola la *petición* por parte de p_i sin responder;
  sino
  responde inmediatamente a p_i;
  fin si

- **Para salir de la sección crítica**
  estado := LIBERADA;
  responde a cualquiera de las peticiones en la cola;

Ejemplo:



Algoritmo de multidifusión y relojes lógicos: Ricart y Agrawala

b. Indica y explica la complejidad en número de mensajes necesarios.
    - Sin soporte multicast: 2(n – 1) mensajes.
    - Con soporte multicast: n mensajes.

c. Prueba y razona si siempre se cumplen las tres exigencias de la exclusión mutua en coordinación distribuida. [1,5 puntos]

    Sí que se cumplen siempre las tres exigencias (seguridad, vitalidad y ordenación. Se cumple la exigencia de seguridad porque en el algoritmo como máximo solo hay un proceso ejecutando la sección crítica. La exigencia de vitalidad de cumple porque a todos los procesos se le permite la entrada/salida a la sección crítica. Finalmente, cumple la exigencia de ordenación porque a todo proceso que lo solicite se le añade en una cola para permitirle la entrada a la sección crítica en orden

2- Analogías y diferencias entre los algoritmos de sincronización de relojes Cristian y NTP. Razona la respuesta, explica los aspectos clave de cada uno y contextualiza los escenarios de caso de uso. [1,5 puntos]

Aspectos clave de NTP (Network Time Protocol):

- Servicio fiable, redundante, reconfigurables si alguno cae, escalables, con autenticación de las fuentes de tiempo.

Aspectos clave de Cristian:

- Algoritmo centralizado:
    - Servidor de tiempo.
    - Clientes que se sincronizan con el servidor.
- Cada nodo, periódicamente hace una petición al servidor.
- El algoritmo solo sincroniza si el tiempo de respuesta es razonablemente más corto que la precisión requerida.

Escenarios de caso de uso:

- El algoritmo de Cristian se diseñó con el propósito de ser utilizado en intranets. En cambio, el algoritmo NTP está diseñado para poder salir de la Intranet.

3- Explica las tres razones principales por las que proteger una red WIFI y las medidas que debemos aplicar para evitar su ataque o reducir el peligro. [1,5 puntos]

Las tres razones son:

- El tráfico de la red puede ser capturado y examinado.
- Los recursos de la red están expuestos a usuarios desconocidos directamente por la vulnerabilidad del canal de transmisión.
- Uso de la red con fines maliciosos.

Medidas para evitar su ataque o reducir el peligro:

- Cambiar las opciones por defecto del router y webs de configuración.
- Actualizar el firmware y hardware.
- Apagar el AP cuando no se usa.
- Filtrado de MAC y número de clientes simultáneos.
- Bajar al mínimo útil la potencia de transmisión de AP.
- Encriptación WPA o WPA2 con claves largas.
- Encriptar los volúmenes – particiones y ficheros del sistema.
- Incorporar siempre antivirus, firewalls de dos direcciones y software anti-intrusión.

4- Define los siguientes conceptos [0,5 puntos cada uno]:

a. Algoritmo criptográfico simétrico.
   - Es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes en el emisor y el receptor. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez que ambas partes tienen acceso a esta clave, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y éste lo descifra con la misma clave.
   - La clave es secreta.
   - E y D tienen la misma clave.
   - M debe ser difícil de computar si se desconoce K.
   - La forma usual de ataque es la fuerza bruta. Resistente haciendo K suficientemente grande (aproximadamente 128 bits).

b. Ataque de cumpleaños.
   - Es un tipo de ataque criptográfico que se basa en la matemática detrás de la paradoja del cumpleaños, haciendo uso de una situación de compromiso espacio-tiempo informática.

c. Corte inconsistente.
   - Un corte es inconsistente si para todo par de eventos (e, e') no se cumple que $(e \in C) \wedge (e' \rightarrow e) \rightarrow e' \in C$.

d. Sistema distribuido asíncrono.
    - Es el modelo que siguen los sistemas distribuidos reales, como por ejemplo Internet.
    - No tienen limitaciones en cuanto a velocidad de procesamiento, retardos en la transmisión de mensajes ni tasas de derivada de los relojes.
    - Una solución válida para un sistema asíncrono también lo es para un sistema síncrono.

e. Tiempo UTC.
    - Sus siglas significan Universal Time Coordinated (Tiempo Universal Coordinado).
    - UTC es un estándar internacional de establecimiento y mantenimiento del tiempo transcurrido.
    - Está basado en el tiempo atómico y ocasionalmente ajustado al tiempo astronómico.
    - La señal se difunde mediante estaciones de radio por tierra y mediante satélites. Los ordenadores pueden sincronizar sus relojes mediante receptores adecuados.

f. Función de resumen seguro.
    - Son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado (es decir, a partir de los datos de la entrada crea una cadena que *solo* puede volverse a crear con esos mismos datos).

g. Reloj de Lamport.
    - Es un tipo de reloj lógico. En este tipo de reloj no se sincronizan relojes, sino que se ordenan eventos según la relación “suceder antes”.

h. Sincronización interior de relojes.
    - Es el resultado de obtener en diferentes máquinas las mismas referencias de tiempo para un instante dado.
    - Al alcanzar la sincronización interna con un error acotado y conocido, se pueden medir eventos como el tiempo de transmisión de un mensaje, en donde las dos marcas de hora serán producto de dos relojes ubicados en máquinas distintas pero sincronizadas.

5- Dentro de las prácticas no guiadas realizadas este curso, de sockets, RMI y servicios WEB, explica esquemáticamente (con un gráfico y breve explicación del funcionamiento) la comunicación e interacción del controlador con los servicios web y componentes RMI [1 punto] ¿Qué ventajas e inconvenientes relacionados con los conceptos de SD has encontrado en el uso de cada una de las dos propuestas? [0,5 puntos]

Preguntas mías

- **¿Qué es la exclusión mutua?**
  - Son un tipo de algoritmo que se utilizan en la programación concurrente para evitar el ingreso a sus secciones críticas por más de un proceso a la vez. La sección crítica es el fragmento de código donde puede modificarse un recurso compartido.
  - Requisitos (exigencias) de la exclusión mutua:
    - EM1 : **Seguridad** → en todo momento, como máximo hay un solo proceso ejecutando la sección crítica.
    - EM2 : **Vitalidad** → a todo proceso que lo solicita se le concede la entrada/salida en la sección crítica en algún momento. Esto evita el abrazo mortal y la inanición.
    - EM3 : **Ordenación** → la entrada en la sección crítica debe concederse según la relación sucedió – antes.

- **Explica el algoritmo de Berkeley.**
  - Algoritmo centralizado:
    - Distinto a Cristian porque en el algoritmo de Berkeley, el servidor (maestro) se elige entre todos los nodos conectados (esclavos).
  - No provee su tiempo, sino que lo estima a partir de todos los nodos conectados.
  - Estima la derivada de cada reloj y manda la corrección.
  - Es un algoritmo difícil de escalar.

- **Explica el funcionamiento del algoritmo de Berkeley.**

  1º Un maestro consulta y recoge valores de reloj del resto de computadores esclavos.

  2º El maestro utiliza los tiempos de ida y vuelta de los mensajes para estimar el valor de los relojes esclavos.

  3º Promedia los resultados incluyéndose y eliminando cualquier valor que no sea consistente.

  4º Envía la magnitud de ajuste de cada reloj. Esto puede ser positivo o negativo.

- **¿Cuáles son los objetivos de NTP?**
  - Proporcionar un servicio que permita a los clientes a lo largo de Internet sincronizarse con UTC.
  - Proporcionar un servicio fiable que pueda aguantar pérdidas de conectividad prolongadas.
  - Permitir a los clientes sincronizarse de manera lo suficientemente frecuente como para compensar las tasas de derivada usuales.
  - Proporcionar protección a las interferencias con el servicio de tiempos.

- **¿Cuál es la diferencia entre los relojes Lamport y los vectoriales?**
  - Los relojes de Lamport son contadores que se actualizan de acuerdo con la relación "suceder antes" entre eventos.
  - Los relojes vectoriales mejoran a los relojes Lamport. Determinan si dos eventos están ordenados por la relación "suceder antes" o son concurrentes, comparando los vectores de marcas.

- **Explica los relojes Lamport.**
  - No se sincronizan relojes, sino que se ordenan eventos según "suceder antes". Si los eventos ocurren en p_i (i = 1, 2, … N) entonces ocurren en el orden observado por p_i
  - Es un tipo de reloj lógico.
  - Un reloj lógico es un contador software monótono creciente. No se debe confundir con un reloj físico.
  - Cada proceso p_i tiene su reloj lógico (L_i) que se utiliza para fijar las marcas temporales a los eventos.

- **Explica los relojes vectoriales.**
  - Fueron desarrollados para superar la eficiencia de los relojes lógicos de Lamport.
  - Un reloj vectorial V_i en el proceso p_i es un array de N enteros, que cada proceso utiliza para establecer marcas de sus eventos locales.

- **¿Cuáles son los algoritmos de encriptación simétrica que hay?**
  - TEA, DES, Triple-DES, IDEA y AES
  - Todos estos algoritmos realizan operaciones de confusión y de difusión sobre bloques de datos binarios.

- **¿Cuáles son los algoritmos de encriptación asimétrica?**
  - RSA y Curcas elípticas.
  - Todos ellos dependen del uso de funciones de puerta falsa:
    - Son funciones de un solo sentido con una salida secreta.
  - Los algoritmos asimétricos son aproximadamente 1000 veces más lentos y no son prácticos para encriptaciones masivas; sin embargo, sus propiedades los hacen idóneos para la distribución de claves y para la autentificación.

- **¿Cuáles son los algoritmos de resumen seguro que conoces?**
  - MD5: calcula un resumen de 128 bits.
  - SHA: vasado en MD4 pero es más seguro, produce un resumen de 160 bits.

- **¿Qué es un hash?**
  - Es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.

- **¿Cuáles son los modos de sincronización de servidores NTP?**
  - Multidifusión (multicast):
    - En LAN de alta velocidad. Un servidor reparte el tiempo al resto que establecen su tiempo asumiento un retraso de transmisión (no preciso).
  - Llamada a procedimiento:
    - Similar a la de Cristian. El servidor acepta peticiones.
    - Tiene una precisión más alta.
  - Simétrica:
    - Pares de servidores se intercambian mensajes conteniendo información de tiempo.
    - Usado en los casos en que se necesita muy alta precisión.

- **¿Qué son los algoritmos de elección?**
  - Es un procedimiento para elegir a un proceso dentro de un grupo. P
    - Ejemplo: elegir a un proceso que sustituya a uno especial (coordinador, maestro, …) cuando éste cae.
  - Su principal exigencia es la elección única incluso si varios procesos lanzan el algoritmo de elección de forma concurrente.
  - E1 → Seguridad.
  - E2 → Vivacidad.
  - Sus dos algoritmos son:
    - Algoritmo basado en anillo.
    - Algoritmo del matón (bully).

- **Explica el algoritmo basado en anillo.**
  - Es un tipo de anillo lógico en el que cada proceso sólo sabe comunicarse con su vecino.
  - Se elige al proceso con identificador más alto.
  - Se supone procesos estables durante la elección.
  - Número de mensajes para elegir coordinador:
    - Peor caso: lanza elección sólo el siguiente al futuro coordinados → (3n – 1) mensajes.
    - Mejor caso: lanza elección el futuro coordinador → 2n mensajes.
  - No detecta fallos.

- **Explica cómo funciona el algoritmo basado en anillo.**
  - Inicialmente todos los procesos son no-candidatos, cualquiera puede empezar una elección:
    - Se marca como candidato.
    - Envía mensaje de elección con su identificador.
  - Cuando un proceso recibe un mensaje de elección:
    - Si el identificador del mensaje es mayor que el suyo, entonces envía el mensaje a sus vecinos.
    - Si es menor:
      - Si es no-candidato, entonces sustituye el identificador y envía mensaje al vecino y se marca como candidato.
    - Si es el suyo:
      - Se marca como no-candidato.
      - Envía mensaje de elegido a su vecino añadiendo su identidad.
  - Cuando un proceso recibe un mensaje de elegido:
    - Se marca como no-candidato.
    - Lo envía a su vecino.

- **Explica el algoritmo Bully**
  - El algoritmo selecciona al miembro superviviente con mayor identificador.
  - Los procesos pueden caer durante la elección.
  - Requisitos:
    - Todos los miembros del grupo deben conocer las identidades y direcciones de los demás miembros.
    - Se supone que tienen comunicación fiable.
  - Hay 3 tipos de mensajes:
    - Mensaje de elección: para comunicar elección.
    - Mensaje de respuesta a un mensaje de elección.
    - Mensaje de coordinador: anuncia identidad de nuevo coordinador.
  - Número de mensajes para elegir coordinador:
    - Caso mejor: se da cuenta el segundo más alto → (n – 2) mensajes.
    - Caso peor: se da cuenta el más bajo → $O(n^2)$ mensajes.

- **Explica como funciona el algoritmo de Bully:**
    - Un algoritmo inicia una elección al darse cuenta de que el coordinador ha caído:
        - Envía mensaje de elección a los procesos con identificador mayor que el suyo.
        - Espera algún mensaje de respuesta:
            - Si vence temporizador, entonces el proceso se pone como coordinador y envía mensaje de coordinador a todos los procesos con identificadores más bajos.
        - Si recibe alguna respuesta, entonces espera mensaje de coordinador:
            - Si vence temporizador, lanza una nueva elección.
    - Si un proceso recibe un mensaje de coordinador:
        - Guarda el identificador y trata a ese proceso como nuevo coordinador.
    - Cuando un proceso de reinicia:
        - Lanza una elección a menos que sea el de identificador más alto <8en cuyo caso se pondría como nuevo coordinador).

- **¿Qué es un DFS (Sistema de Ficheros Distribuidos)?**
    - Tiene las mismas funciones que el sistema de ficheros de un SO convencional, pero más complejo.
    - Los usuarios y los dispositivos de almacenamiento se encuentran dispersos por la red.
    - Un SFD debe permitir:
        - Compartir la información remotamente.
        - Movilidad de los usuarios.
        - Disponibilidad.

- **¿En qué componentes se puede estructurar un SFD?**
    - Servicio de almacenamiento.
    - Servicio de ficheros.
    - Servicio de nombres o de directorio.
    - Módulo cliente (biblioteca de funciones o API).

- **¿Cuáles son los modelos de acceso a ficheros remotos que existen?**
    - Modelo de servicio remoto:
        - Las operaciones se realizan en los servidores.
        - Tiene problemas de eficiencia.
    - Modelo de caché de datos:
        - Se accede a los ficheros de forma remota.
        - Aumento de rendimiento.
        - Tiene problemas de consistencia.

- **¿Qué es un servidor sin estado (stateless)?**
    - Son servidores que no almacenan información entre solicitudes de un mismo cliente.
        - Tolerancia a fallos.
        - No requieren llamadas para abrir y cerrar ficheros.
        - No se desprecia memoria en tablas.
        - No existe límite para el número de ficheros en uso (ficheros abiertos).
        - No se producen problemas si cae un cliente.

- **¿Qué es un servidor con estado (stateful)?**
    - Es un servidor que almacena información entre solicitudes de un mismo cliente.
        - Los mensajes de solicitud de servicio son más cortos.
        - Mejor rendimiento.
        - Es posible realizar operaciones de lectura anticipada.
        - Permiten el bloqueo de ficheros.

- **¿Qué ventaja aporta la replicación de ficheros?**
    - Aumenta la disponibilidad.
    - Aumenta la fiabilidad.
    - Mejora el tiempo de respuesta.
    - Reduce el tráfico en la red.
    - Mejora el rendimiento.
    - Beneficia la escalabilidad.
    - Permite trabajar en modo de operación desconectada.

- **¿Cuáles son las buenas prácticas de seguridad?**
    - Educar a los usuarios: Nada puede protegerlos, deben sensibilizarse.
    - Defensa elástica: no para el ataque, lo ralentiza.
    - Robustecimiento del sistema: quitar programas no esenciales, parar servicios innecesarios, configurar arranque, etc.
    - Actualizaciones automáticas: parches y mejoras.
    - Virtualización: mejoran consumos, mantenimiento y recuperación.
    - Usar herramientas de control (unix).
    - Registros externalizados: guardar copias de seguridad en los mismos.

- **Define los siguientes conceptos:**
    - Reloj vectorial.
        - Es un algoritmo para la generación de un ordenamiento parcial de eventos en un sistema distribuido y detecta violaciones casuales.

- Algoritmo criptográfico asimétrico.
  - Es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es *pública* y se puede entregar a cualquier persona, la otra clave es *privada* y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.
  - La clave es pública.
  - Las claves de encriptación y desencriptación están separadas.
  - Se basa en el uso de funciones de puerta falsa, tienen un alto coste computacional y las claves son muy grandes (> 512 bits).

- Algoritmo criptográfico híbrido.
  - Son usados en SSL (actualmente llamado TLS).
  - Utiliza criptografía asimétrica para transmitir la clave simétrica que se usa para encriptar la sesión.

- Ataque de negación de servicio.
  - Consiste en el uso excesivo de los recursos hasta el punto de impedir su uso a los usuarios legítimos. (Pj: ataque a Amazon y Yahoo en febrero del 2000).

- Caballos de Troya y otros virus.
  - Los virus sólo pueden entrar en los ordenadores cuando el código de programa es importado.

- Sistema Distribuido síncrono.
  - El tiempo de ejecución de cada etapa de un proceso tiene ciertos límites inferior y superior conocidos.
  - Cada mensaje transmitido sobre un canal se recibe en un tiempo límite conocido.
  - Cada proceso tiene un reloj local cuya tasa de derivada sobre el tiempo de referencia tiene un límite conocido.
  - A nivel teórico, podemos establecer unos límites para tener una idea aproximada de cómo se comportará el sistema, pero a nivel práctico es imposible garantizar esos límites siempre.

- Reloj defectuoso.
  - Es aquel que no cumple ninguna de las condiciones de corrección.

- Sincronización exterior de relojes.
  - Se produce cuando, por ejemplo, si se desea saber en una máquina concreta a qué hora del día sucedió un evento, es necesario sincronizar la hora de esa máquina con algún reloj o fuente de hora autorizada.

- Fichero replicado.
  - Es aquél del que existen varias copias, cada una de las cuales está en un servidor diferente.

- Needham-Schroeder.
  - Es un protocolo de autenticación y distribución de claves para redes locales.
  - Protege los servidores frente a ataques enmascarados.
  - Utiliza autenticación de clave secreta.

- Kerberos.
  - Hace lo mismo que Needham-Schroeder y está basado en este.
  - Fue desarrollado en el MIT en los 80 y está estandarizado e incluido en muchos SO.

- Firma digital.
  - Es un mecanismo criptográfico que permite al receptor de un mensaje firmado digitalmente identificar a la entidad originadora de dicho mensaje y confirmar que el mensaje no ha sido alterado desde que fue firmado por el originador.