## 1. Modos de sincronización y algoritmos.

No existe un reloj universal, pero podemos hacer algunas aproximaciones con relojes lógicos, estados globales o relojes vectoriales.

Para la sincronización de relojes, se puede realizar mediante el tiempo universal coordinado (UTC). Es un estándar para la comprobación y sincronización del tiempo, que se difunde por radio en tierra y mediante satélites. Se basa en el tiempo atómico y es calibrado eventualmente con el tiempo astronómico. Dos tipos de sincronización:

- Externa: un reloj se conecta a una fuente UTC exacta.
- Interna: dos relojes se envían mensajes para su sincronización.

Dos relojes que están sincronizados internamente no significa que lo estén externamente, puesto que pueden derivar juntos.

Podemos decir que un SD es síncrono cuando:

- se conoce tiempo máximo y mínimo de ejecución de cada paso en cada proceso.
- Se conoce tiempo máximo y mínimo para la recepción de mensajes.
- Se conocen los tiempos de deriva de los relojes implicados.

Los algoritmos de sincronización serían:

**Primera aproximación (sincronización interna):** un proceso p le envía un mensaje m a p2 con tiempo t. P2 actualizaría su reloj con tiempo t2 a t + Ttransmisión del mensaje.
**Método de Cristian (sincronización externa):** con conexión a servidor UTC S. Un proceso p solicita a S una sincronización mediante un mensaje m. S contesta y p pondrá su tiempo a t + Tround/2 (Tround es el tiempo de ida y vuelta). La precisión será de Tround/2 – min.
**Algoritmo de Berkeley (sincronización interna):** un computador actúa de maestro, y recoge los datos de reloj de todos los computadores del sistema (esclavos). Asumiendo los tiempos de ida y vuelta, realiza el promedio de los tiempos recibidos incluyéndose, enviando el tiempo calculado al resto de computadores. Si el maestro falla podremos elegir otro.

Otra forma de sincronización sería NTP (protocolo de tiempo de red). Estándar para el establecimiento del tiempo para internet. Se puede estudiar como un tipo árbol, donde los niveles primarios estarían conectados a fuentes UTC, los secundarios a los niveles primarios y la subred de sincronización sería el nivel más bajo, siendo los PC. Es tolerante a fallos. Si un primario pierde la conexión con UTC pasa a secundario, si un secundario pierde a su primario puede escoger otro. Entre pares de servidores NTP se utiliza la sincronización por mensajes en modo UDP.
Los métodos de sincronización son:

- Multicast. En redes LAN de alta velocidad. Un servidor reparte el tiempo a los demás.
- Por llamada a procedimiento. Parecido al método de Cristian pero más preciso.
- Simétrica. Para niveles superiores, con alta precisión.

Otros métodos de sincronización serían Lamport (mediante sincronización por eventos y no por relojes) y los relojes lógicos; relojes vectoriales; estados globales, con el algoritmo de Chandy y Lamport.

2. **Explicar por qué el escenario 2 "el del servidor" no es apto para comercio electrónico.**

En el caso del escenario 2, el servidor Sara es quien recoge todos los datos de credenciales de todos los implicados en la comunicación. Esto es bueno cuando hay un número de participantes concretos, pero no para un tipo de comercio en creciente evolución, como es el comercio electrónico. Debido a las constantes altas y posibles bajas de usuarios en el servidor, sería fácil una posible caída del mismo, o incluso una sobrecarga en las peticiones al mismo, por lo que este modelo sería no apto para este tipo de comercio.

3. **Definiciones.**

**Tasa de deriva:** diferencia por unidad de tiempo que difiere un reloj de un computador del reloj perfecto.
**Reloj correcto:** se dice de aquel reloj H del cual conocemos su tasa de deriva.
**Sistema distribuido asíncrono:** un sistema distribuido en general suele ser asíncrono, debido a que es complicado sincronizar todos los relojes. Imposible detectar fallos.
**Corte de la ejecución del sistema:**
**Corte consistente:** un corte tal que para todos cada evento que contiene, también contiene todos los sucesos que sucedieron antes que él.

**4.- ¿El algoritmo TEA se podría lleva a otra arquitectura hardware?**

### 5.- Definir entre los algoritmos simétricos y asimétricos criptográficos cuáles son mejor o peor

En los algoritmos criptográficos podemos encontrar:

- Algoritmos simétricos (con clave secreta). La forma usual de ataque es la fuerza bruta.
- Algoritmos asimétricos (con clave pública). Se basa en el uso de funciones de puerta falsa.

Simétricos:

- TEA: triple de veloz que el DES. Muy efectivo a pesar de su simplicidad.
- DES: su modelo original no era muy veloz. Debido a su carga de código, se implementó en VLSI.
- Triple-DES: ejecuta DES tres veces con 2 claves distintas.
- IDEA: muy parecido al TEA pero no tan veloz.
- AES.

Asimétricos:

- RSA: es el más común y el más utilizado. Para encriptar con RSA el texto es dividido en bloques.
- Curvas elípticas: nuevo modelo. Mucho más eficiente. Claves más cortas y más veloz.

Los algoritmos asimétricos son 1000 veces más lentos y no son prácticos para encriptaciones masivas. Sin embargo, sus propiedades los hacen idóneos para distribución de claves y para autenticación.

### 6. Definir los pasos de Chandy y Lamport, finalidad y cuándo se acaba.

El algoritmo de Chandy y Lamport se usa para determinar los estados globales de sistemas distribuidos. Registra un conjunto de estados de procesos de forma que el estado global sea consistente. Se registra el estado de cada proceso localmente.
Los pasos a seguir son:

- Recepción de marcador para el proceso P.
    - Si (p no ha registrado su estado). Lo registra. Registra el estado de C como el conjunto vacío. Activa el registro de mensajes.
    - Si (p ha registrado su estado). P registra el estado de C como el conjunto de mensajes recibidos desde que C guardó su estado.
- Envío de marcador para el proceso P.
    - Después de que P haya registrado su estado para cada canal de salida C, P envía un mensaje de marcador sobre C.

El algoritmo termina si se cumplen todas las restricciones de conectividad e inexistencia de fallo en la comunicación.

**7. Desarrolla el ataque del cumpleaños, en qué contexto se puede dar y qué aspectos son determinantes para protegernos de él.**

El ataque del cumpleaños puede darse en el escenario 4: firma digital con resumen seguro. Se puede dar en el caso de que la función resumen no sea segura.

El ataque del cumpleaños se basa en que es más probable encontrar un par idéntico entre un conjunto que la probabilidad de encontrar una pareja para un individuo dado.

El ataque del cumpleaños se produce cuando.

1. Alice prepara 2 versiones M y M' de un contrato para Bob.
2. Alice fabrica varias versiones sutilmente diferentes de M y M'.
3. Alice envía M a Bob, quien lo firma digitalmente usando su clave privada.
4. Cuando lo devuelve, Alice sustituye M por M', pero manteniendo la firma de Bob sobre M.

Para protegernos de esta paradoja, es necesario tener funciones de resumen seguras y funcionar con firmas digitales conocidas, de forma que sean todavía más seguras. Si encontramos firmas desconocidas en el proceso, es posible que nuestro resumen o mensaje haya sido interceptado.

**8-Desarrolla el algoritmo de acceso a sección crítica llamado "Ricart-Agrawala" ¿se cumplen en todos los casos las tres exigencias de exclusión mutua? Razona la respuesta. Además indica y justifica el número de mensajes que se necesitan en su funcionamiento.**

Dicho algoritmo es un algoritmo basado en relojes lógicos. Se trata de que cuando un proceso quiera entrar en la sección crítica compartida, preguntará a todos los demás si puede hacerlo. Cuando obtenga respuesta de TODOS, podrá entrar. La comunicación se realiza mediante mensajes en forma de tuplas.

El número de mensajes necesario para su funcionamiento depende de las infraestructuras:

- Si no se permite envío multicast se necesitará 2(n-1) mensajes.
- Si se permite envío multicast serán necesarios n mensajes.
- El algoritmo fue refinado para usar n mensajes en envío no multicast.

Se cumplirían con este algoritmo las exigencias EM1 y EM2 (seguridad y vitalidad), pero no aseguraríamos EM3 (ordenación), debido a que este método puede hacer que el servidor sufra caídas. Además dicho método tendría igual o peor congestión en el servidor que el método de servidor central, y sería más costoso.

## Examen Julio 2013.

Las 3 primeras son del parcial 1.

4. **Justifica la existencia o no de un reloj universal de referencia. Razona también la respuesta en el contexto de los SD.**

No existe un reloj universal de referencia. El tiempo es relativo. En relación con los SD, el tiempo es una de las problemáticas más usuales, ya que no existe dicho reloj. Podríamos realizar algunas aproximaciones que resultarían muy precisas, utilizando relojes lógicos, relojes vectoriales o algoritmos para determinar el estado global de SD en cada momento.
Cada computador que conforma el SD tendría un reloj local, que sería el utilizado por cada uno de los procesos que se ejecutasen en dicho computador. De manera que aunque nosotros sincronizáramos todos los relojes al mismo tiempo, dicho reloj global variaría significativamente con el tiempo.
Es cierto que hay aproximaciones muy válidas para marcar los eventos en cada computador, como por ejemplo utilizando estándares de sincronización como NTP (protocolo de tiempo de red) o ajustándonos al UTC( coordinación de tiempo universal), relojes con gran precisión y baja tasa de deriva.
Por la diferencia existente entre los relojes de un SD tenemos dos términos:

- Sesgo: diferencia de tiempo entre dos relojes en un instante determinado.
- Tasa de deriva: diferencia por unidad de tiempo que difiere el reloj de cada computador del reloj perfecto.

5. **Desarrolla el concepto de reloj vectorial y compáralo con el reloj lógico de Lamport, indicando las características principales, reglas de fijación de marcas temporales y álgebras de comparación del orden de sucesión de los eventos en cada caso.**

Los relojes lógicos de Lamport son contadores software monocrecientes. No debemos confundirlos nunca con los relojes físicos. Todos los procesos de un sistema tienen un reloj lógico.
Mattern y Fidge crean los relojes vectoriales para arreglar las deficiencias de los relojes lógicos de Lamport. Un reloj vectorial es un array de N enteros que utilizan los procesos para llevar a cabo su ejecución. Cada uno de los procesos utiliza este reloj para establecer marcas de sus eventos locales.

6. **Describe los conceptos de difusión y confusión en criptografía y pon un ejemplo razonado de cada aspecto.**

7. **Explica en qué consisten los cifradores de bloques, tipos y para qué se utilizan. Pon un ejemplo de cada uno, funcionamiento y debilidades.**

La mayoría de cifradores de bloques se basan en bloques de 64 bits. La debilidad de un cifrador simple es que los patrones repetidos pueden ser detectados. La conexión debe ser fiable, no se pueden perder bloques.
Los tipos y sus ejemplos son:

- Simétricos. El TEA es el más rápido a pesar de ser muy simple.
- Asimétricos. El RSA es el más utilizado actualmente. Para la encriptación necesita dividir el texto en varios bloques.
- De resumen seguro. SHA. Basado en MD4 pero más seguro.

Los algoritmos asimétricos con 1000 veces más lentos que los simétricos y no son adecuados para trabajar con gran carga. A pesar de ello, son útiles para la distribución de claves y autenticación.
En los algoritmos de resumen seguro se pueden producir ataques de cumpleaños, por lo que los algoritmos de resumen deben trabajar sobre firmas digitales conocidas y resúmenes seguros.

8. **Describe las 3 exigencias de los algoritmos de exclusión mutua distribuida. Además razona si se cumplen en anillo y Ricart-Agrawala.**

EM1. Seguridad. Sólo un proceso en ejecución en la zona de sección crítica compartida del sistema distribuido.
EM2. Vitalidad. Si un proceso solicita entrar a la sección crítica, se le debe conceder el permiso en algún momento de su ejecución.
EM3. Ordenación. Los procesos deberán entrar en la sección crítica según el orden parcial de "suceder antes".

En el algoritmo de anillo, el testigo pasa de computador en computador, conociendo cada uno de éstos solamente la dirección de su vecino. Se cumplirán la EM1 y EM2, ya que si un computador tiene el testigo será el que entre en SC si lo requiere y en algún momento se otorgará permiso para que un proceso que lo ha solicitado entre en la SC. La EM3 no siempre se cumplirá, debido a que al conocer solamente la dirección del vecino no podemos asegurar que las peticiones se atiendan en el orden correcto.

En el algoritmo de Ricart-Agrawala cumpliremos las mismas reglas, ya que al preguntar a todos los demás nos aseguramos que no hay nadie ocupando la SC y además siempre entraremos en la misma si lo hemos pedido. El único problema es que no podemos asegurar la EM3, debido a que si se produce fallo en el servidor o cuello de botella podemos perder el orden.

9. **Indica y justifica el número de mensajes necesarios para la elección de coordinador mediante el algoritmo "Bully".**

El número de mensajes para elegir coordinador:
- En el caso mejor: se da cuenta el segundo más alto (n-2) mensajes.
- En el caso peor: se da cuenta el más bajo ($n^2$)