**Examen Enero 2016**

1. Sobre el algoritmo Ricard-Agrawala: (a) Escribe el algoritmo, (b) Indica y explica la complejidad en número de mensajes necesarios; (c) Prueba y razona si siempre se cumplen las tres exigencias de la exclusión mutua en coordinación distribuida. [1,5 puntos]  
   2- Analogias 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]  
   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]  
   4- Define los siguientes conceptos [0,5 puntos cada uno] (a) Algoritmo criptográfico simétrico; (b) Ataque de cumpleaños; (c)Corte inconsistente; (d) Sistema distribuido asíncrono; (e) Tiempo UTC; (f) Función de resumen seguro; (g) Reloj de Lamport; (h)Sincronización interior de relojes.  
   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]

**Otro examen**

1.- Modos de Sincronización y algoritmos  
2.- Explicar por que el escenario 2 ("el del servidor") no es apto para el negocio electrónico/transacciones en un negocio electrónico.

No es apto para los negocios electrónicos ya que Sara almacena TODOS los participantes y sus claves. La ingente cantidad de proveedores y posibles clientes hace inviable este almacenamiento. Sirve para organizaciones donde tienes un número concreto de participantes.

3.- Definiciones: Corte Consistente, Deriva de Reloj, ...  
4.- ¿El algoritmo TEA se podría lleva a otra arquitectura hardware?

la operación de desplazamiento depende de la arquitectura, no es lo mismo en un equipo de 32 que 64 bits, existen problemas a la hora de trasladar el algoritmo a otra arquitectura hw

5.- Definir entre los algoritmos simétricos y asimétricos criptográficos cuáles son mejor o peor  
6.- Definir los pasos de Chandy- Lamport, cuando se acaba y finalidad

**Otro examen**

1. Define brevemente los siguientes conceptos referidos al tema Tiempo y estados globales:   
   a)Tasa de deriva  
   b)Reloj correcto  
   c)Sistema distribuido asíncrono  
   d)Corte de la ejecución del sistema  
   e)Corte consistente  
   2- Desarrolla el ataque del cumpleaños indicando en que se basa, en que contexto se puede dar y qué aspectos son determinantes para protegernos de ese ataque.

Se basa en que la probabilidad de encontrar un par idéntico en un conjunto es mucho mayor que la de encontrar la pareja para un individuo dado, con paciencia se pueden crear dos documentos con el mismo resultado. Por ejemplo, Alice crea dos documentos M y M', M favorable y M' desfavorable, crea diferentes versiones de M y M' con cambios sutiles y compara los valores de dispersión hasta encontrar un par igual, Alice envía M a Bob con el contrato favorable y Bob lo firma, cuando lo devuelve sustituye M por M' pero manteniendo la firma de Bob.

Pero no entiendo muy bien que ocurre osea: "Alice prepara dos versiones M y M’ de un contrato para Bob. M favorable y M’ desfavorable"-  
Vale y que pasa con esto? luego con eso de que envia M cuando encuentra uno igual y el otro lo devuelve etc, ¿que se esta intentando conseguir, por que es un ataque?

Se puede utilizar para falsificar un contrato de compraventa cambiando algún parámetro relevante como el precio de adquisición.

Vale creo que ya lo veo, entonces Alice seria en este ejemplo la falsificadora no?, le envía el bueno, y después de que lo firme lo reemplaza por el que tiene algo cambiado manteniendo la firma, pero no entiendo muy bien eso de que crea muchos M y M' hasta encontrar un par idéntico en lugar de copiar directamente.

Porque tienen que tener el mismo resultado al codificarlos, para eso va haciendo muchos distintos hasta que dos de ellos dan el mismo resultado en la codificación  
  
Para protegernos del ataque del cumpleaños se necesita una función de resumen segura h=H(M)  
que cumpla que dado M, debe ser muy dificil encontrar otro M' tal que H(M)=H(M').  
  
3-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.

Creo recordar que el año pasado entró una pregunta del tema 6, nose si fue ricart-agrawala o el anillo, alguien se acuerda?

**Otro examen**

1.- Modos de Sincronización y algoritmos  
2.- Explicar por que el escenario 2 ("el del servidor") no es apto para el negocio electrónico/transacciones en un negocio electrónico  
3.- Definiciones: Corte Consistente, Deriva de Reloj, ...  
4.- ¿El algoritmo TEA se podría lleva a otra arquitectura hardware?

Esa pregunta nos la planteó Jerónimo en clase. El algoritmo TEA utiliza operaciones que dependen de la arquitectura como es el desplazamiento lógico. No será lo mismo en 32 que en 64 bits. Si sigues desarrollándolo por ahí, como comenta Lady Sun, sacas más problemas de arquitectura.  
5.- Definir entre los algoritmos simétricos y asimétricos criptográficos cuáles son mejor o peor  
6.- Definir los pasos de Chandy- Lamport, cuando se acaba y finalidad.

**Otro examen 2012**

Reloj universal, firma digital, reloj vectorial, reloj logico.

criptografia, confusion,difusion y el nerdham screider ese, los pasos que tiene ese protocolo.

1.- Modos de Sincronización y algoritmos  
2.- Explicar por que el escenario 2 ("el del servidor") no es apto para el negocio electrónico

el escenario 2 es del autenticación con servidor. Es un escenario pensado para una organización. Las claves están administradas por el servidor de todos los participantes. En el comercio electrónico existen infinitos participantes por lo que es inviable ("es decir, imposible") conocer las claves (o gestionar las claves) a todos los participantes. Lo tienes mejor explicado en la página 247 de "Sistemas Distribuídos" Coulouris  
3.- Definiciones: Corte Consistente, Deriva de Reloj, ...  
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  
6.- Definir los pasos de Chandy- Lamport, cuando se acaba y finalidad

**Preguntas interesantes del foro:**

Donde tengo más duda es en los estados globales, no entiendo mucho que son los estados   
y el metodo de Chandy-Lamport no entiendo muy bien lo que hace  
  
si alguien puede opner asi una expicacion sencilla para que me quede un poco mas claro y empezar a pillarlo algo mejor!!

Un estado global del sistema es un estado en el que si haces un corte, este corte es consistente, es decir, para cada evento que contiene este corte también contiene todos los sucesos que sucedieron antes de él.  
  
Y el algoritmo de Chandy-Lamport se encarga de ir sacando instantáneas para determinar estados globales, registrando el estado de cada proceso localmente. Si un proceso no ha registrado su estado, es obligado a hacerlo (regla de recepción del marcador) y después de registrar su estado son obligados a enviar un marcador antes de enviar cualquier otro mensaje (regla de envío del marcador).

Más o menos.

Relojes sincronizados internamente no necesariamente lo están externamente, puesto que pueden derivar juntos.  
  
Si el conjunto P está sincronizado externamente con un límite D, ¿también lo está internamente?  
  
Respecto a este planteamiento seria que sí ¿no?, ya que si están sincronizados internamente entre ellos como dice podría derivar el conjunto difiriendo de la fuente exacta S, pero si están sincronizados cada uno de ellos con la fuente externa precisa siguiendo ese mismo tiempo entonces también lo estarán internamente ¿no?

En el peor caso posible P1 está sincronizado externamente con S con un sesgo de +D (unidades de tiempo) y P2 está sincronizado externamente con S con un sesgo de -D. Por tanto, estarán sincronizados con un límite 2\*D.

Entonces la respuesta sería no, porque para estar sincronizados el sesgo tiene que ser menor que D?

La respuesta es que están sincronizados internamente con un límite de 2D

"Modos de Sincronización y algoritmos".  
  
Este no seria muy extenso??  
  
Hablar de la sinc. interna y externa, de UTC, la primera aproximacion por sincronizacion interna de SD, metodo cristian (externo), Berkeley(interno), todo lo de NTP con sus modos de sincronizacion... Lamport y relojes logicos tambien??

Supongo que solo seria contestar con sincronizacion interna y externa, y sus respectivos algoritmos no? (primera aproximacion y berkeley para interna y cristian para externa). Alguien puede confirmarlo? -thumbup

Es que en NTP tambien se habla de sincronizacion... y ya se mete muchisima materia xD

Yo creo que sería:   
sistema síncrono con sincronización interna ->Berkeley  
sistema síncrono con sincronización externa ->Cristián  
sistema asíncrono con sincronización interna->No existe algoritmo  
sistema asíncrono con sincronización externa-> NTP  
Sería hablar de todo eso, creo que Lamport no va en esta pregunta, de hecho, Chandy y Lamport lo ponen como una pregunta a parte.

Además Chandy & Lamport es un algoritmo para obtener instantáneas, eso entraría si se hablara de estados globales. Yo diría que son, como ha dicho Javier, sólo los algoritmos de sincronización de relojes físicos (Berkeley, Cristian, NTP...) como mucho... si eso... tal vez... se podría hablar de los relojes lógicos (Lamport y relojes vectoriales) peeeeroooooooooo.... yo diría que no xD  
Siempre podemos preguntar en el examen.

**ErikPardo escribió:**En el algoritmo de Ricart-Agrawala, se cumplen en todos los casos las tres exigencias de exclusión mutua? No lo encuentro en las transparencias -nosweat .

Yo tengo en mis apuntes que a pesar de ser un algoritmo distribuido, el **fallo de cualquier proceso bloquea el sistema**, por lo que sí se cumplen suponiendo que no hay caídas ni fallos, que es lo mismo que le pasa al algoritmo basado en el servidor central, el cual tampoco es tolerante a fallos, no??

**Manu7 escribió:**

**cphcarolina escribió:**

**ErikPardo escribió:**En el algoritmo de Ricart-Agrawala, se cumplen en todos los casos las tres exigencias de exclusión mutua? No lo encuentro en las transparencias -nosweat .

Yo tengo en mis apuntes que a pesar de ser un algoritmo distribuido, el **fallo de cualquier proceso bloquea el sistema**, por lo que sí se cumplen suponiendo que no hay caídas ni fallos, que es lo mismo que le pasa al algoritmo basado en el servidor central, el cual tampoco es tolerante a fallos, no??

Claro, yo creo que sin caidas se cumple, el orden se consigue por la información de las tuplas de los mensajes y la propia mecánica, pero es que en servidor central si se cae el servidor se elige otro y no se asegura E3, ya no estoy tan seguro en ricart y agrawala como argumentar esa parte porque es un bloqueo del sistema, ¿¿¿eso podría llevar a que no solo E3 sino las demás tampoco???, es que no se especifica pero como no dice nada de reconfiguración...

Si se bloquea el sistema pocas exigencias puede cumplir, porque ni siquiera funciona. Un sistema bloqueado y una piedra ofrecen más o menos lo mismo xD  
  
Si preguntan sobre la exclusión mutua tampoco me complicaría tanto, porque hay mucho que decir. Sólo sobre la solución de la exclusión mutua distribuida hay tres algoritmos: basado en el servidor central, en el anillo y en los relojes lógicos (Ricart & Agrawala). Por lo que para éste, con explicar cómo funciona, decir que cumpliría las exigencias de exclusión mutua, PERO...  
1. no es tolerante a fallos, ya que cualquier fallo bloquearía el sistema entero  
2. es más costoso que el del servidor central, puesto que ya con el algoritmo refinado aún necesitas n mensajes para obtener el recurso, mientras que en el servidor central necesitabas 2 para la entrada en la sección crítica y 1 para salir  
3. y además su congestión es igual o peor que en el servidor central porque los procesos implicados reciben y procesan cada solicitud  
no haría falta centrarse mucho más en él.  
  
Creo que lo importante es recalcar que ninguno de los algoritmos puede tratar bien la caída de un proceso, pero que entre los menos malos está el del servidor central, puesto que a pesar del cuello de botella, es el que menos mensajes requiere con diferencia. Así que, que cada uno gestione sus recursos, encargándose de su exclusión mutua.

**RuSSe escribió:**

**cphcarolina escribió:**

**ErikPardo escribió:**En el algoritmo de Ricart-Agrawala, se cumplen en todos los casos las tres exigencias de exclusión mutua? No lo encuentro en las transparencias -nosweat .

Yo tengo en mis apuntes que a pesar de ser un algoritmo distribuido, el **fallo de cualquier proceso bloquea el sistema**, por lo que sí se cumplen suponiendo que no hay caídas ni fallos, que es lo mismo que le pasa al algoritmo basado en el servidor central, el cual tampoco es tolerante a fallos, no??

Si no me equivoco en el de Ricart-Agrawala se cumplen las tres exigencias, mientras que en el algoritmo basado en el servidor central no se cumpliría la tercera ya que si un proceso P1 manda una petición primero y después la manda un proceso P2, si P2 llega antes que P1, P2 entraría antes que P1, por tanto no se cumple la exigencia sucedio-antes.

No te lies, la exigencia 3 sí se cumple en el servidor central. El orden se refiere el orden de llegada al servidor. Si mi petición llega antes que la tuya, se resolverá antes. Pero no permitirá que las que lleguen después se te cuelen

Lo que dicen es que se cumple la exigencia 3 PARA EL ORDEN DE LLEGADA DE LOS MENSAJES AL SERVIDOR, vamos que es relativamente ordenado.

**ENLACES CON INFORMACION**

<http://carteleras.webcindario.com/tpr5-unlz.pdf>

<http://distribui2.blogspot.com.es/>

POsile ejercicio optativo:

Un servidor B de ntp recibe un mensaje del servidor A a las 16:34:23,480 llevando una marca de tiempo 16:34:13,430 y lo responde A recibe el mensaje a las 16:34:15,725 llevando una marca de tiempo 16:34:25,7 de B. Estimar la deriva entre B y A y la precisión de la estimación.

ejercicio de la diapositiva 41 del tema 4 (el ejercicio propuesto del algoritmo de Chandy y Lamport)