INF-343 Sistemas Distribuidos Martes 22 de Octubre de 2024
Prof. Jorge Díaz M

Certamen 2
Capítulo 3: Naming y Seguridad
Capítulo 4: Coordinación

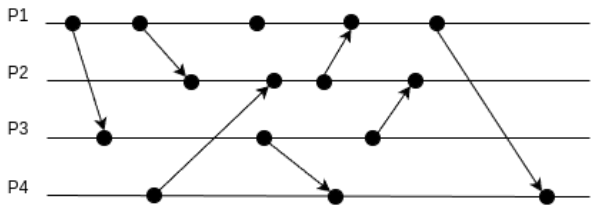

Fig. 1

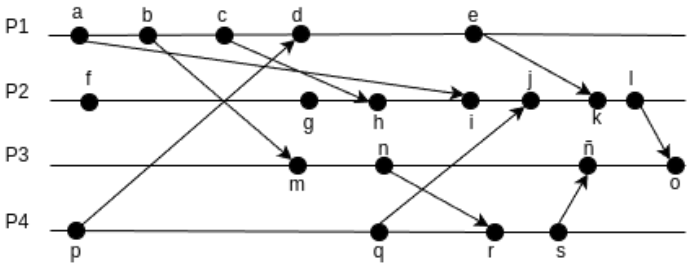

Fig. 2

Nombre: _____ **Rol**: _____ **Par**: _____

I. **(5pts c/u)** Marque con **V** si cree que la frase es correcta y con una **F** si cree que es falsa. En caso de marcar como falso debe justificar su respuesta.

1) _____ Un String compuesto por la MAC y un puerto de un host es válido como identificador de un proceso.

2) _____ Podemos llegar a consenso en un sistema sincrono o asincrono siempre y cuando los nodos que estén fallando o “mintiendo” sean menos del 30% del sistema.

3) _____ Los certificados digitales corresponden a un archivo o contraseña que busca verificar la autenticidad de un servidor o usuario mediante el uso de una clave pública.

4) _____ Cualquier algoritmo de Exclusión Mutua es un ejemplo de un algoritmo de Consenso, no así al revés.

5) _____ Las Tablas de Hash Distribuidas son un ejemplo de Structured Naming, donde la búsqueda no es escalable pero la complejidad de mantenimiento es baja.

6) _____ Tanto en un algoritmo de exclusión mutual distribuido como por token en un anillo lógico tienen N puntos de falla.

II. **(6pts c/u)** Encierre en un círculo la alternativa que considere correcta. Solo debe seleccionar una alternativa por pregunta.

1) ¿Cuál de las siguientes alternativas **NO** corresponde a un método de ataque a un sistema distribuido?

a) Suplantación
b) Alteración de mensajes
c) Fraccionamiento
d) Denegación de servicios

2) Respecto al algoritmo de elección Bully, ¿Cuál de las siguientes alternativas es falsa?

a) Cada nodo tiene un ID único que representa algo válido para el sistema.
b) Cualquier nodo puede notificar al resto que el coordinador está caído
c) Se puede asegurar la cantidad total de mensajes que se necesitarán sabiendo el ID del nodo que notificó y la cantidad de nodos totales.
d) En cada paso, si al nodo actual le responde un nodo con ID mayor, el nodo actual sabe que él no será el nuevo coordinador.

3) ¿Cuál de las siguientes alternativas **NO** es una característica de un sistema de nombres de tipo plano (flat naming)?

a) En los enfoques jerárquicos las entidades se pueden repetir dentro del árbol por tener varias direcciones.
b) Una desventaja de los punteros de reenvío es la cadena que se puede generar al cambiar una entidad de dirección.
c) Los sistemas de Flat Naming son los más convenientes para los casos de búsquedas realizadas por humanos
d) El sistema debe tener métodos de localización a los puntos de acceso que son independientes del nombre.

4) Respecto a un algoritmo de consenso, ¿Cuál de las siguientes alternativas es falsa?

a) Se debe asegurar que todos los nodos estén activos y funcionando correctamente durante la ejecución del algoritmo de consenso
b) Todos los nodos deben respetar el resultado obtenido del algoritmo de consenso.
c) Todos los nodos del sistema deben tener el mismo resultado
d) Cualquier algoritmo de consenso debe asegurar que terminará y retornará una decisión.

5) Respecto a los relojes lógicos, ¿Cuál de las siguientes afirmaciones es falsa?

a) Se crean ya que puede que no sea necesario siempre acordar una hora actual.
b) El algoritmo de Berkeley se basa en el uso de relojes lógicos
c) Si dos procesos no interactúan, no es necesario que sus relojes estén sincronizados.
d) A veces puede ser suficiente para ponerse de acuerdo sobre el orden en que ocurren los eventos.

III. **(11pts c/u)** Responda las siguientes preguntas relacionadas con los temas vistos en clases. (El puntaje va en la calidad de su respuesta)

a) Dada la **Fig. 2**, asuma que todos los relojes de vectores comienzan con el valor (1,0,2,3) y que suman 1 por defecto cuando hay un evento nuevo a la posición que corresponde. ¿Cuál es el reloj de vector de **O**?

b) Dada la **Fig. 1**, donde los procesos P1, P2, P3 y P4 intercambian mensajes en el tiempo (flechas). Si P1 tiene como valores/relojes de sus eventos 0, 3, 6, 9, 12, de izquierda a derecha, y P3 valores/relojes de sus eventos 3, 6, 9, ¿Cuáles podrían ser los valores/relojes de los eventos de P2 y P4 para que sean los relojes lógicos de Lamport válidos ?

c) Explique cómo funcionan los algoritmos de encriptación simétricos y asimétricos. Además, haga una pequeña tabla de comparación entre ellos.

IV. **(7pts)** Usando la siguiente función de Hash H(X), genere 3 bloques blockchain teniendo la siguientes condiciones:

x	0	1	2	3	4	5	6	7	8	9
H(x)	7	0	6	4	5	6	0	9	2	1

A. El Id inicial es 2016.
B. El valor a almacenar en cada bloque es 2021, 2022 y 2023, respectivamente.
C. A cada bloque debe sumarle un valor tal que el resultado del Hash, tenga dos 00 al comienzo, vale decir, el resultado hash de cada bloque debería ser de la forma **00ab.**
D. En caso de desbordamiento, se suma al primer número de la derecha