Taller transacciones y seguridad

Andrés Felipe Chavarro Plazas

Jesús Alfonso Pinzón Vega

**A. TRANSACCIONES**

Considerando el código anterior:

1. ¿Qué posibles errores podrían presentar las instrucciones en los tres puntos marcados? (SELECT 1<-, INSERT <--2, UPDATE <--3) Escriban las condiciones y las restricciones de integridad asociadas.

SELECT:

* Verificar que el grupo y la materia objetivo sea válido para la selección. (Se soluciona con restricciones declarativas, Definición de dominio).
* Puede haber casos de lectura sucia, pues otra transacción ocurre al mismo tiempo y realiza cambios en los datos seleccionados (Restringir la base de datos en el momento de la transacción).
* Hay casos donde una persona se inscribe con secciones distintas, se puede generar lecturas repetidas (Limitar el acceso a un dispositivo o sesión).

INSERT:

* No debe permitirse que un estudiante se inscriba dos o más veces a la misma materia o en diferentes grupos (Validar la integridad del grupo o materia).
* No se puede que un estudiante trate de inscribir desde distintas sesiones al mismo tiempo, pues habría datos repetidos o fantasmas. (Limitar el acceso a un dispositivo o sesión)
* Validar la integridad de las materias y sus respectivos grupo (Checks en base a las materias y sus grupos).

UPDATE:

* Puede haber fallos de Lectura no repetible, en caso de que se realicen 2 inscripciones al mismo tiempo (acepta al primer estudiante que realiza la inscripción).
* Por lectura repetida, validar que el grupo tenga la capacidad de inscripción, en caso contrario se aceptan ambas.

2. ¿Qué posible error no se ha comunicado? Modifique el código para considerarlo.

Es posible que no se hayan validado los tipos de datos de las columnas de las tablas, lo cual pude generar errores inesperados en las transacciones. Además, no hay una confirmación o denegación de la transacción que finalice su ejecución.

3. Incluya las instrucciones básicas para manejar TODOS los posibles casos de excepción de este procedimiento.

Generen una única excepción de aplicación con el mensaje apropiado.

4. ¿Por qué inscribir debería ser una transacción? Incluya las instrucciones necesarias: COMMIT, ROLLBACK

Pues porque inscribir una materia es un proceso que se realiza en repetidas ocasiones por varios estudiantes en un periodo de tiempo determinado, generando posibles problemas de concurrencias y haciendo ejecución del ROLLBACK. En caso contrario, se ejecuta el COMMIT que confirma los cambios.

**B. CONCURRENCIA**

Corrección.

Suponiendo que: MBDA 01 tiene 20 cupos, ya están inscritos 19 estudiantes y los estudiantes 8754623 y 4859632 existen y no están inscritos a MBDA:

1. ¿Cuáles serían lo posibles resultados de ejecución correcta de los procesos de inscripción de estos dos estudiantes? Expliquen su respuesta.

Los dos posibles escenarios validos son; que se acepte la inscripción del estudiante 4859632, o al estudiante 8754623, pero no a los dos.

**PROBLEMAS/SOLUCIONES**

Considerando la ejecución concurrente propuesta (sólo los pasos posibles, actualice el resto):

1. Si el nivel de aislamiento de las transacciones es READ UNCOMMITTED: Lectura no confirmada (sin bloqueos)

¿cómo se comportan? ¿es correcto? ¿ilustra algún problema clásico?

En este caso, la transacción no tiene ningún tipo de restricción, por lo que es propensa a los problemas de concurrencia. Por tanto, no es correcto aplicar este tipo de lectura. Para ilustrar, dos estudiantes pueden inscribir materias al mismo tiempo cuando queda un solo cupo libre y la transacción los acepta a ambos.

1. Si el nivel de aislamiento de las transacciones es REPEABLE READ: Lectura repetible: (Bloqueo exclusivo para actualizar y compartido para leer)

¿cómo se comportan? ¿es correcto? ¿ilustra algún problema clásico?

En este caso, tampoco es recomendable usar este tipo de transacción, pues al permitir la lectura compartida a la par de restringir la actualización, puede haber casos de lecturas repetidas, permitiendo así, la inscripción de estudiantes en casos donde queden menos cupos que estudiantes a inscribir.

1. Si en el caso 2. se adiciona el mecanismo de control de bloqueo mortal, ¿cómo se comportan? ¿es correcto?

Este tipo de restricción tampoco sería muy recomendable en este caso, pues al ser una inscripción de materias, no se debería limitar la cantidad de transacciones por un único estudiante.

**C. SEGURIDAD**

Considerando que el mecanismo de seguridad seleccionado es de permisos mínimos sobre datos. Escriba los permisos que debería tener cada uno de los actores considerando el diagrama de casos de uso y las reglas de negocio.

DECANO:

Texto

Descripción generada automáticamente

CORDINADOR:

Texto

Descripción generada automáticamente con confianza media

ESTUDIANTE:

Texto

Descripción generada automáticamente

PARA TODOS:

Texto

Descripción generada automáticamente con confianza baja

VISTA:

Texto

Descripción generada automáticamente

D. CIFRADO

1. Si queremos mantener en secreto las inscripciones de cada uno de los cursos, ¿Qué dato, tabla o tablas se requerirían mantener cifradas para proteger esta información? Sea eficiente en la solución y justifique su respuesta

Para mantener en secreto las inscripciones de cada uno de los cursos, se requeriría mantener cifrada la tabla de inscripciones (INSCRIPCIONES). Esta tabla contiene información sensible sobre qué estudiantes están inscritos en qué cursos y grupos, por lo que cifrarla sería una medida eficiente para proteger esta información confidencial.

2. Considerando que el método de cifrar de la ESCUELA es de sustitución (por el carácter siguiente en la tabla (ASCII1) y el método de cifrar de la NACIONAL es de permutación (dos caracteres a la izquierda).

• ¿Qué algoritmo debe conocer cada uno de ellos? CE, DE, CN, DN (Cifrado Descifrado, Escuela-Nacional)

• Si el ESCUELA quiere enviar a NACIONAL el mensaje “ELECTIVA CONJUNTA PREPARADA” ¿Cómo se cifra el mensaje? ¿Cómo se descifra el mensaje?

• Si NACIONAL quiere contestar el mensaje con “ENVIAR ESPECIFICACIONES”, ¿cómo se cifra y descifra el mensaje?

Algoritmos necesarios:

- CE: Cifrado Escuela (sustitución por el carácter siguiente en la tabla ASCII).

- DE: Descifrado Escuela (inverso del cifrado Escuela).

- CN: Cifrado Nacional (permutación, dos caracteres a la izquierda en ASCII).

- DN: Descifrado Nacional (inverso del cifrado Nacional).

Cifrado del mensaje "ELECTIVA CONJUNTA PREPARADA":

- Cifrado Escuela: Cada carácter se reemplaza por el siguiente en la tabla ASCII.

- Cifrado Nacional: Cada carácter se reemplaza por el carácter dos posiciones a la izquierda en la tabla ASCII.

Descifrado del mensaje "ENVIAR ESPECIFICACIONES":

- Descifrado Nacional: Cada carácter se reemplaza por el carácter dos posiciones a la derecha en la tabla ASCII.

- Descifrado Escuela: Cada carácter se reemplaza por el anterior en la tabla ASCII.

Por ejemplo, para cifrar "ELECTIVA CONJUNTA PREPARADA" con el método de la Escuela y luego con el método Nacional:

- Escuela: "FMDFUJB DPOKVUB QSFQBSBE"

- Nacional: "CMBCTUZ ALHGJKR NCNCPBQBMT" (considerando la tabla ASCII dada).

Para descifrar el mensaje "ENVIAR ESPECIFICACIONES":

- Nacional: "CLTFQP GQPAGKHGZJACSL"

- Escuela: "BKSHQO FOODBHGBYI`ZQRH"

En este caso, se aplican los algoritmos de descifrado en el orden inverso al cifrado, primero el descifrado Nacional y luego el descifrado Escuela.