

# ESCUELA COLOMBIANA DE INGENIERIA

## MODELOS Y BASES DE DATOS

### TRANSACCIONES Y SEGURIDAD

#### S13-S14: 2023-2

En este trabajo vamos a trabajar en una versión simplificada de un sistema de inscripciones (sin manejo de prerequisites). Estudie la definición de las tablas y el procedimiento INSCRIBIR.

<pre>CREATE TABLE MATERIAS(   sigla CHAR(4) NOT NULL,   nombre VARCHAR(30) NOT NULL; ALTER TABLE MATERIAS ADD CONSTRAINT PK_MATERIAS   PRIMARY KEY(sigla);  CREATE TABLE GRUPOS(   materia CHAR(4) NOT NULL,   numero NUMBER(2) NOT NULL,   capacidad NUMBER(2) NOT NULL,   inscritos NUMBER(2) NOT NULL; ALTER TABLE GRUPOS ADD CONSTRAINT PK_GRUPOS   PRIMARY KEY (materia,numero); ALTER TABLE GRUPOS ADD CONSTRAINT FK_GRUPOS_MATERIAS   FOREIGN KEY(materia) REFERENCES MATERIAS(sigla);</pre>	<pre>CREATE TABLE ESTUDIANTES(   codigo NUMBER(7) NOT NULL,   nombres VARCHAR(50) NOT NULL; ALTER TABLE ESTUDIANTES ADD CONSTRAINT PK_ESTUDIANTES   PRIMARY KEY(codigo);  CREATE TABLE INSCRIPCIONES(   materia CHAR(4) NOT NULL,   numero NUMBER(2) NOT NULL,   estudiante NUMBER(7) NOT NULL); ALTER TABLE INSCRIPCIONES ADD CONSTRAINT PK_INSCRIPCIONES   PRIMARY KEY(materia,estudiante); ALTER TABLE INSCRIPCIONES ADD CONSTRAINT FK_INSCRIPCIONES_ESTUDIANTES   FOREIGN KEY(estudiante) REFERENCES ESTUDIANTES(codigo); ALTER TABLE INSCRIPCIONES ADD CONSTRAINT FK_INSCRIPCIONES_GRUPOS   FOREIGN KEY(materia,numero) REFERENCES GRUPOS(materia, numero);</pre>
---	--

CREATE OR REPLACE

PROCEDURE INSCRIBIR(xEstudiante IN NUMBER, xMateria IN CHAR, xNumero IN NUMBER) IS

xInscritos NUMBER(2);

xCapacidad NUMBER(2);

BEGIN

SELECT inscritos, capacidad INTO xInscritos, xCapacidad  
 FROM GRUPOS

WHERE materia=xMateria AND numero=xNumero;

IF (xInscritos < xCapacidad) THEN

INSERT INTO INSCRIPCIONES(materia,numero,estudiante) <-2

VALUES (xMateria,xNumero,xEstudiante);

UPDATE GRUPOS SET <-3

inscritos=inscritos+1

WHERE materia=xMateria AND numero=xNumero;

END IF;

END INSCRIBIR;

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

## 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 los posibles resultados de ejecución correcta de los procesos de inscripción de estos dos estudiantes? Expliquen su respuesta.

### Problemas/Soluciones

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

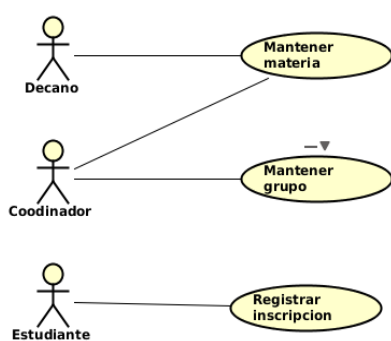
1. Si el nivel de aislamiento de las transacciones es READ UNCOMMITTED : Lectura no confirmada (sin bloqueos) ¿cómo se comportan? ¿es correcto? ¿ilustra algún problema clásico?
2. Si el nivel de aislamiento de las transacciones es REPEATABLE READ : Lectura repetible : (Bloqueo exclusivo para actualizar y compartido para leer) ¿cómo se comportan? ¿es correcto? ¿ilustra algún problema clásico?
3. Si en el caso 2. se adiciona el mecanismo de control de bloqueo mortal, ¿cómo se comportan? ¿es correcto?

MBDA 01 tiene 20 cupos y ya están inscritos 19 estudiantes  
Los estudiantes existen y no se han inscrito a MBDA.

	TA. INSCRIBIR 8754623 MBDA 01	TB. INSCRIBIR 4859632 MBDA 01
t1	1	-
t2	-	1
t3	2	-
t4	-	2
t5	3	-
t6	-	3
t7	-	-

## 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.



- Los decanos y coordinadores pueden adicionar y modificar materias. El único dato que se permite modificar es el nombre. El decano es el único responsable eliminar materias.
- El coordinadores pueden crear los grupos asociados a las materias. El único dato que pueden modificar es la capacidad, respetando los estudiantes ya inscritos. Los grupos se pueden eliminar si no tienen inscripciones.
- Los estudiantes pueden inscribir las materias que desean cursar. Los inscripciones se pueden eliminar pero no modificar.
- El decano puede consultar una síntesis de las inscripciones: sigla, grupo, inscritos y disponibles. Esta consulta únicamente está disponible el primer día de la semana de 8:00 a 5:00.
- Todos los actores pueden consultar los datos de las materias.

## CIFRADO

- 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.
- Considerando que el método de cifrar de la ESCUELA es de sustitución (por el carácter siguiente en la tabla ASCII<sup>1</sup>) 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 (**C**ifrado-**D**escifrado, **E**scuela-**N**acional)
  - 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?

**DATE** "Supongamos que A y B son dos usuarios que desean comunicarse entre sí usando un esquema de cifrado de clave pública. Entonces A y B publicarán un algoritmo de cifrado (incluyendo en cada caso la clave de cifrado correspondiente) pero por supuesto, mantendrán el algoritmo de descifrado y la clave en secreto (incluso entre sí). Hagamos que los algoritmos de cifrado sean CA y CB (para cifrar mensajes que serán enviados a A y B, respectivamente) y hagamos que los algoritmos de descifrado correspondientes sean DA y DB, respectivamente. CA y DA son inversos entre sí, al igual que CB y DB. Ahora supongamos que A desea enviar a B un fragmento de texto plano P. En lugar de calcular CB (P) y transmitir el resultado, A aplica primero a P el algoritmo de descifrado DA y luego cifra el resultado y lo transmite como el texto cifrado TC= CB ( DA ( T ) )  
Al recibir C, el usuario B aplica el algoritmo de descifrado DB y luego el algoritmo de cifrado CA produciendo el resultado final T: CA ( DB ( TC ) ) = T  
Ahora B sabe que el mensaje en efecto proviene de A, ya que CA producirá T sólo si el algoritmo DA fue utilizado en el proceso de cifrado y ese algoritmo sólo lo conoce a A.

```

-----
CA ( DB ( CB ( DA ( T ) ) ) )
CA ( DA ( T ) ) /* ya que DB y CB se cancelan */
T /* ya que CA y DA se cancelan */

```