

Submission Policy: Submissions must be typed (not handwritten) and stapled hardcopies are to be turned in (no softcopies). Only two late submissions (max delay from due date is "two days") per student are acceptable.

1. **(True/False) (5 Pts)** Virtual private databases enforce security policies at the server-side, but not at the application side.
2. **(15 Pts)** Let "Family" be a table: Family(parent varchar2(30), childname varchar2(30)). The following VPD policy function is attached to this table.

```

Create function vpd_function (object_schema varchar2, object_name varchar2)
  Return varchar2
  As parent VARCHAR2(100);
Begin
  if ( SYS_CONTEXT('userenv', 'ISDBA') ) then
    return ' ';
  else
    user := SYS_CONTEXT('userenv', 'SESSION_USER');
    return 'parent = ' || user;
  end if;
End;
```

This policy specifies that a user can access all the rows in which his/her name is stored as the value of the attribute parent. The admin can access all the rows. You are submitting the following query to the database. Write the SQL query which is the result of the query rewriting process by the database server.

```
select * from Family;
```

3. Consider the table 'my_table' and the policy 'sec_function' specified in the class slides 5 and 6, respectively of Lecture 19. The attachment of the policy to this table is carried out as follows.


```

execute dbms_rls.add_policy (object_schema => 'Alice',
                             object_name => 'my_table',    policy_name => 'my_policy',
                             function_schema => 'Alice',
                             policy_function => 'sec_function',
                             statement_types => 'select, update, insert',
                             update_check => TRUE );
```

 - a. **(True/False) (5 Pts)** This policy would be enforced on all tables created from the schema 'Alice'.
 - b. **(5 Pts)** You are not referred to as a 'owner' in the table 'my_table'. Which of the following SQL statements can be executed by you on table "my_table"?
 - i. Select
 - ii. Update
 - iii. Insert
 - iv. None of the above
 - c. **(5 Pts)** Your name is referred to as an 'owner' in the table 'my_table'. Which of the SQL statements given in 3(b) can be executed by you on table "my_table"?
 - d. **(15 Pts)** If "update_check => TRUE" in this policy is removed, then what would be the answers for 3(a), 3(b), and 3(c)?
4. **(True/False) (5 Pts)** In the case of column-level VPD policies, the default behavior restricts the number of columns be returned by a query.
5. **(True/False) (5 Pts)** A VPD policy function f on a table can select that table within f.
6. **(True/False) (5 Pts)** For each tuple in a multi-level relation, the attributes of the primary key can have different access classes.
7. **(True/False) (5 Pts)** Polyinstantiation is used to prevent violation of data integrity.
8. **(True/False) (5 Pts)** Visible polyinstantiation due to a high user inserting a tuple that is already present with the same primary key prevents covert signaling channels.

9. **(True/False) (5 Pts)** In order to prevent polyinstantiation, some keys can be classified at the lowest possible class and some keys at the highest possible class when the domain of the primary keys is not partitioned.
10. **(10 Pts)** A file S is divided into four blocks S_1, S_2, S_3 and S_4 , and users may receive one or more of each of these blocks. Show how to compute the Merkle hash $MH(S)$ of S . [**Hint:** First build a binary tree with S_1 - S_4 as leaf nodes.]
11. **(10 Pts)** In question 10, let $MH(S)$ is signed with RSA by the owner O . A user has access to S_1 and S_3 . Show what information (other than S_1 and S_3), the user would need from the O in order to authenticate the integrity and origin of S_1 and S_3 .