# CT 2- Question Bank

**Unit 2 – 4 Marks**

## 1. Mention default users in Oracle and SQL server.

ORACLE default users, will be created at the time of ORACLE software installation

a. SYS (Super user will all DBA rights , can't be changed)
b. SYSTEM (With Minimal DBA rights
c. SCOTT (User without DBA rights)
d. SQL server default users, will be created at the time of SQL Server software installation
e. SA ( System Administrator , It is equivalent to SYS in Oracle and can't be changed)
f. BUILT-IN\Administrators ( Associated with the local administrators' group on the Windows server)

## 2. How to create user in Oracle?

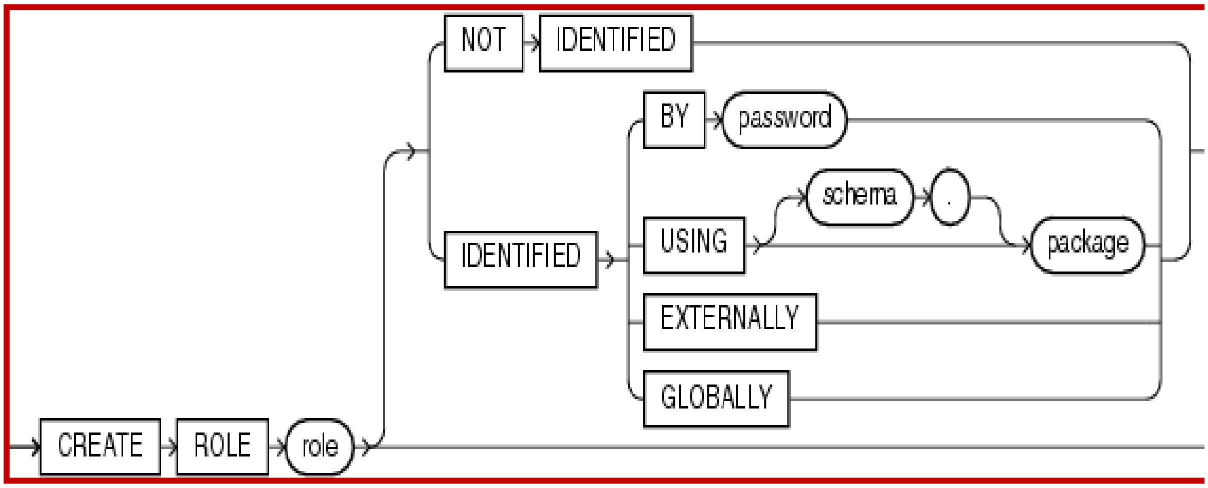
- Creating users is one of the main tasks you will perform as a database operator or DBA
- In most organization , this process is standardized , well documented, and surely managed
- The DBA had written a script to create a user for every developer working on the project
- This script granted privileges to read and write data to the database scheme
- Regardless of the database you use , creating the user is generally an easy task once a policy is documented and followed

## 3. List out the best practices for Administrators and Managers.

- Creating users is one of the main tasks you will perform as a database operator or DBA
- In most organization , this process is standardized , well documented, and surely managed
- The DBA had written a script to create a user for every developer working on the project

- This script granted privileges to read and write data to the database scheme
- Regardless of the database you use , creating the user is generally an easy task once a policy is documented and followed
- . Outline your business goals.
- A few example goals your business might have are:
- Improve decision-making
- Create/improve automations and processes
- Audience targeting/create a buyer profile
- Find customer buying habits/patterns
- Train sales and marketing teams on data use
- 2. Prioritize data protection and security.
- Focus on data quality.
- Reduce duplicate data
- Ensure your data is readily accessible to your team.
- Create a data recovery strategy.
- Use a quality data management software.

**4. Draw the diagram for creating role with ORACLE**



**5. Mention the two clauses in creating users in ORACLE.**

- When creating users in Oracle, two important clauses are:
- 1. **IDENTIFIED BY:** Specifies the password for the new user.
-   - Example: `CREATE USER username IDENTIFIED BY password;`

- 2. **DEFAULT TABLESPACE:** Specifies the default tablespace where the user's objects will be stored.

  - Example: `CREATE USER username IDENTIFIED BY password DEFAULT TABLESPACE users;`

6. Write about the following in SQL server
   I. Removing user II. Modifying user

## I. Removing a User in SQL Server

1. **Connect to the Database:**
   - Use `USE database_name;` to specify the database context.
2. **Execute the DROP USER Command:**
   - Remove the user with `DROP USER username;`.

## II. Modifying a User in SQL Server

1. **Connect to the Database:**
   - Use `USE database_name;` to specify the database context.
2. **Execute the ALTER USER Command:**
   - Modify user attributes such as default schema or username:
     - Change default schema: `ALTER USER username WITH DEFAULT_SCHEMA = schema_name;`
     - Rename user: `ALTER USER username WITH NAME = new_username;`

-

7. Mention the different types of users in handling the Database.

 **Database Administrators (DBAs):**

- Responsible for overall management and maintenance of the database system.
- Perform tasks such as installation, configuration, backup, recovery, and security management.

 **Developers:**

- Design and develop database applications.
- Write and optimize SQL queries, stored procedures, and functions.

 **End Users:**

- Use the database applications to perform specific tasks related to their role.
- Interact with the database through user interfaces or reporting tools.

▯ **Data Analysts:**

- Analyze data stored in the database to generate reports and insights.
- Use tools like SQL, data visualization software, and statistical analysis tools.

▯ **Security Administrators:**

- Focus on managing database security.
- Implement access controls, monitor database activity, and ensure compliance with security policies.

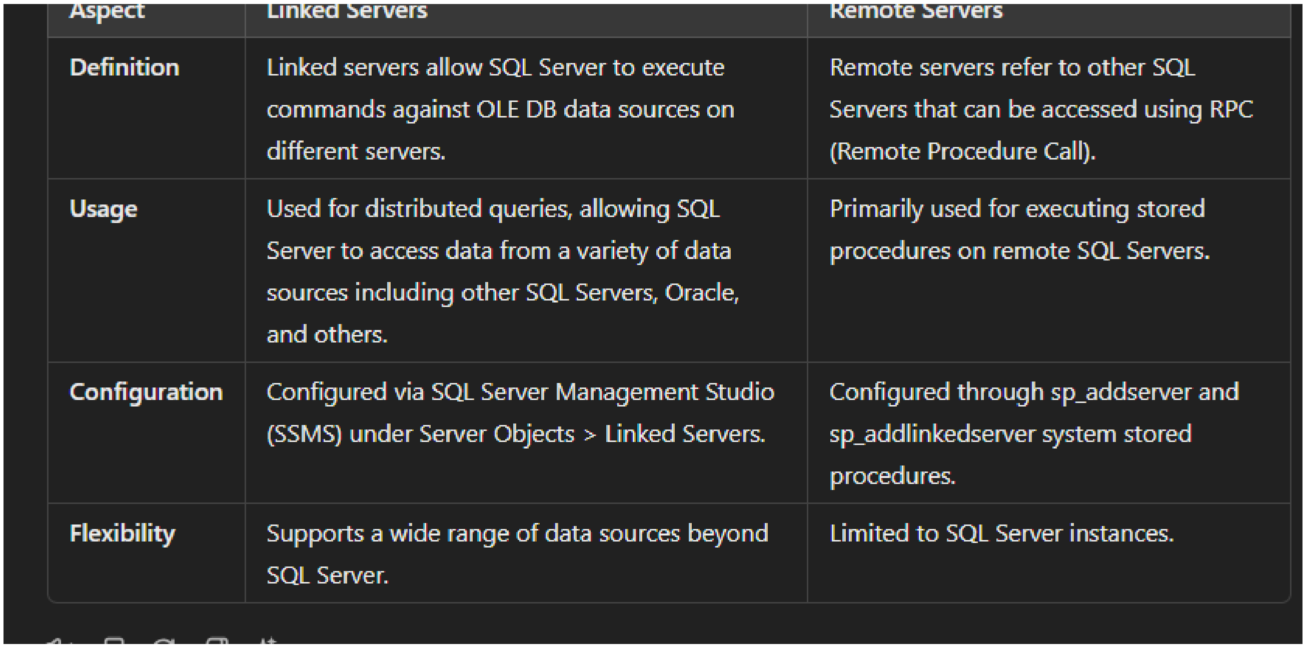
▯ **Application Administrators:**

- Manage and support specific database applications.
- Ensure the application runs smoothly and troubleshoot any issues related to database access.

▯ **Backup Operators:**

- Responsible for managing database backups and restorations.
- Ensure data integrity and availability through regular backup schedules.

## 8. Compare Linked Servers and Remote Server.



| Aspect | Linked Servers | Remote Servers |
|---|---|---|
| **Definition** | Linked servers allow SQL Server to execute commands against OLE DB data sources on different servers. | Remote servers refer to other SQL Servers that can be accessed using RPC (Remote Procedure Call). |
| **Usage** | Used for distributed queries, allowing SQL Server to access data from a variety of data sources including other SQL Servers, Oracle, and others. | Primarily used for executing stored procedures on remote SQL Servers. |
| **Configuration** | Configured via SQL Server Management Studio (SSMS) under Server Objects > Linked Servers. | Configured through sp_addserver and sp_addlinkedserver system stored procedures. |
| **Flexibility** | Supports a wide range of data sources beyond SQL Server. | Limited to SQL Server instances. |

## 9. Write short notes the Password Policies in ORACLE.

- Password policy is a set of guidelines that enhances the robustness of the password and reduces the likelihood of its being broken

- Importance of Password Policies
  - The frontline defence of your account is your password.
  - If your password is weak, the hacker can break in, destroy your data, and violate your sense of security .

For this specific reason, most of the companies invest considerable resources to strengthen authentication by adopting technological measures that protect their assets

## 10.Brief about the creation of a SQL server User.

Creating a user in SQL Server involves a few key steps. Here's a brief guide in four points:

1. **Connect to SQL Server:**

   - Use SQL Server Management Studio (SSMS) or another SQL interface to connect to the SQL Server instance.

2. **Create a Login:**

   - Create a server-level login, which can be either SQL Server authenticated or Windows authenticated.

   - Example:

```sql
CREATE LOGIN login_name WITH PASSWORD = 'password';
```

3. **Create a Database User:**

   - Map the login to a database user within a specific database.

   - Example:

```sql
USE database_name;
CREATE USER user_name FOR LOGIN login_name;
```

4. **Assign Roles and Permissions:**

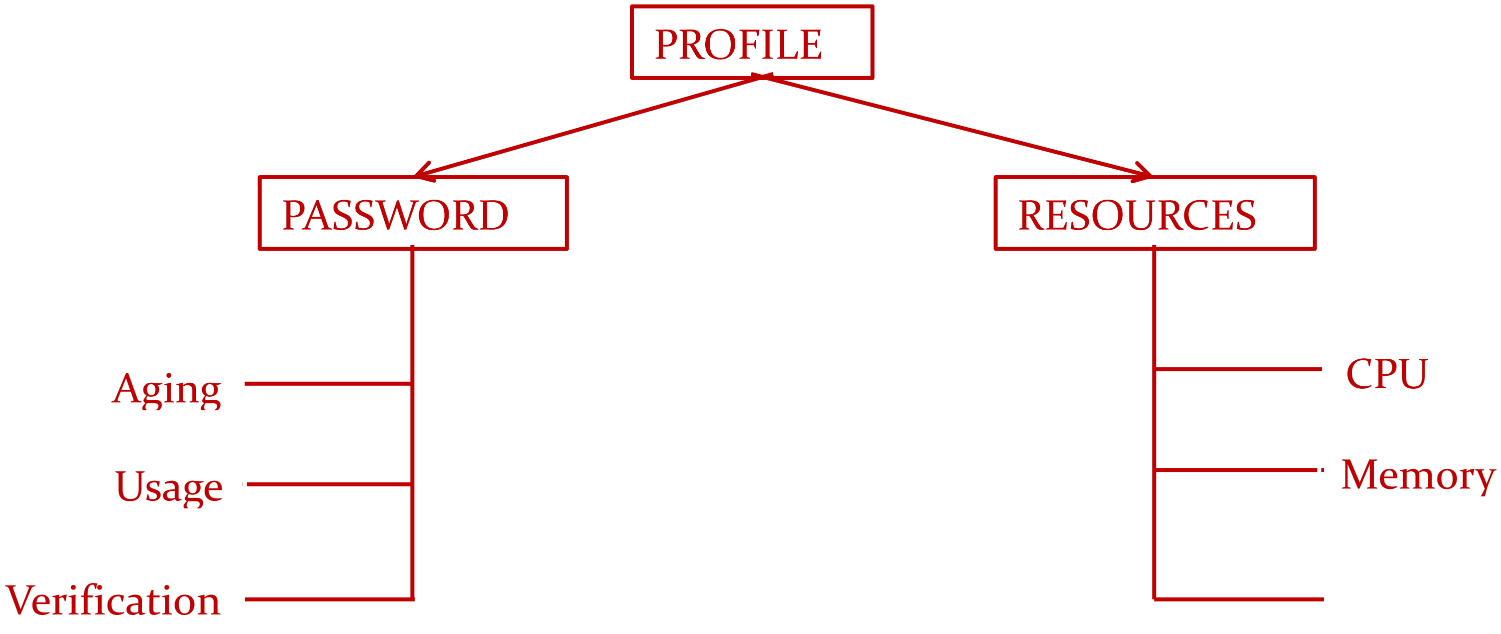
- Grant necessary roles and permissions to the user to perform specific tasks.
- Example:

```sql
ALTER ROLE db_datareader ADD MEMBER user_name;
```

12 Marks

**1)Elaborate on the creation of Profiles in ORACLE.**

- ✓ Creating Profiles in ORACLE
- ✓ A profile in ORACLE helps define two elements of Security
- ✓ Restrictions on Resources
- ✓ Implementation of password policy
- ✓ The following figure shows the two aspects of a profile in ORACLE



**Defining and Using Profiles…**

- ✓ In this syntax:
  - First, specify the name of the profile that you want to create.
  - Second, specify the LIMIT on either database resources or password
- ✓ Resource Parameters
  - SESSIONS_PER_USER – specify the number of concurrent sessions

that a user can have when connecting to the Oracle database.

- CPU_PER_SESSION – specify the CPU time limit for a user session, represented in hundredth of seconds.
- CPU_PER_CALL – specify the CPU time limit for a call such as a parse, execute, or fetch, expressed in hundredths of seconds.
- CONNECT_TIME – specify the total elapsed time limit for a user session, expressed in minutes.
- IDLE_TIME – specify the number of minutes allowed periods of continuous inactive time during a user session. Note that the long-running queries and other operations will not subject to this limit.
- LOGICAL_READS_PER_SESSION – specify the allowed number of data blocks read in a user session, including blocks read from both memory and disk.
- LOGICAL_READS_PER_CALL – specify the allowed number of data blocks read for a call to process a SQL statement.
- PRIVATE_SGA – specify the amount of private memory space that a session can allocate in the shared pool of the system global area (SGA).
- COMPOSITE_LIMIT – specify the total resource cost for a session, expressed in service units. The total service units are calculated as a weighted sum of of CPU_PER_SESSION CONNECT_TIME, LOGICAL_READS_PER_SESSION, and PRIVATE_SGA.

✓ Password_parameters

- You use the following clauses to set the limits for password parameters:
- FAILED_LOGIN_ATTEMPTS – Specify the number of consecutive failed login attempts before the user is locked. The default is 10 times.
- PASSWORD_LIFE_TIME – specify the number of days that a user can use the same password for authentication. The default value is 180 days.
- PASSWORD_REUSE_TIME – specify the number of days before a user can reuse a password.
- PASSWORD_REUSE_MAX – specify the number of password changes required before the current password can be reused. Note that you must set values for both PASSWORD_REUSE_TIME and PASSWORD_REUSE_MAX parameters make these parameters take effect.
- PASSWORD_LOCK_TIME – specify the number of days that Oracle will lock an account after a specified number of a consecutive failed login. The default is 1 day if you omit this clause.

    - PASSWORD_GRACE_TIME – specify the number of days after the grace period starts during which a warning is issued and login is allowed. The default is 7 days when you omit this clause.
- Note that to create a new profile, your user needs to have the CREATE PROFILE system privilege.

**2)Define a Database Link. Discuss the different ways of creating the Database Links. Explain the different methods of creating a Database Link.**

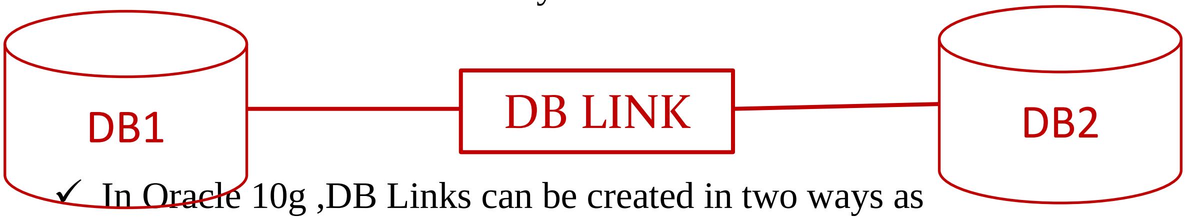
- It is a connection from one DB to another DB
- The linked DBs can be like
    - Both be ORACLE10g
    - Both be SQL Server
    - Mix of ORACLE10g and SQL Server
- A DB link enables a user to perform Data Manipulation Language (DML) or any other valid SQL statements on a DB.
- The following figure gives the architecture of DB Link
- In Oracle 10g ,DB Links can be created in two ways as

1. Public – Which makes the database links accessible by every user in DB

2.Private – Which gives the ownership of the database to a user

The DB is not accessible by any other user unless the user has

been access by the owner



- In Oracle 10g ,DB Links can be created in two ways as

1. Public – Which makes the database links accessible by every user in DB

2.Private – Which gives the ownership of the database to a user

The DB is not accessible by any other user unless the user has

been access by the owner

Authentication Methods

- Authentication methods for connecting ORACLE10g DB using DB link mechanism.

- ✓ There are three types of authentication methods when creating a DB link.
- ✓ Authentication Method 1: CURRENT USER
    - ▪ This authentication method orders ORACLE10g to use the current user credentials for authentication to the DB to which the user is trying to link.
- ✓ Authentication Method 2: FIXED USER

This authentication method orders ORACLE10g to use the user password provided in this clause for authentication to the DB to which the user is trying to link.

- ✓ Authentication Method 3: CONNECT USER

This authentication method orders ORACLE10g to use credentials of the connected user who has an existing account in the database to which the user is trying to link.

3)With Neat Sketch, Explain about the different steps to be followed for creating an ORACLE log User.

**4)Explain about Granting and Revoking the privileges in SQL Server with suitable query.**

**SQL GRANT Command**

SQL GRANT is a command used to provide access or privileges on the database objects to the users.

- ✓ The Syntax for the GRANT command is:

GRANT privilege_name ON object_name TO {user_name |PUBLIC |role_name} [WITH GRANT OPTION];

- ✓ *privilege_name* is the access right or privilege granted to the user. Some of the access rights are ALL, EXECUTE, and SELECT.
- ✓ *object_name* is the name of an database object like TABLE, VIEW, STORED PROC and SEQUENCE.
- ✓ *user_name* is the name of the user to whom an access right is being granted.
- ✓ *PUBLIC* is used to grant access rights to all users.
- ✓ *ROLES* are a set of privileges grouped together.
- ✓ *WITH GRANT OPTION* - allows a user to grant access rights to other users.

Eaxmple :

```
SQL > Grant select on emp to bmnantha;
Grant succeeded
```

The schema owner of emp object gave select privilege to user bmnantha

SQL REVOKE Command:

The REVOKE command removes user access rights or privileges to the database objects.

- The Syntax for the REVOKE command is:

```
REVOKE privilege_name ON object_name
FROM {user_name |PUBLIC |role_name}
```

- Example :

```
SQL > Revoke select on emp from bmnantha;
Revoke succeeded
```

The schema owner of emp object get back the  select privilege to user bmnantha

Privileges in SQL Server

Database Privileges – Statement permissions

- CREATE TABLE
- CREATE VIEW
- CREATE PROCEDURE
- CREATE FUNCTION
- CREATE DEFAULT
- CREATE ROLE
- BACKUP DATABASE
- BACKUP LOG

Privileges in SQL Server

Server Privileges

- Sysadmin – Can perform any function within the system
- Serveradmin – Can perform certain server-level functions.
- Setupadmin – Can manage linked servers and startup procedures
- Securityadmin – Can manage logons, change passwords
- Processadmin – Can manage processes running
- Dbcreator – Create, Alter and Drop Databases
- Diskadmin – Can manage the disk files for the server and database
- Bulkadmin – Can insert bulk insert operations

## Unit 3 – 4 Marks

1. **Why the encryption process is important in Database Security?**

   **Data Encryption**

✓ Encryption is a security method in which information is encoded in such a way that only authorized user can read it.

✓ It uses encryption algorithm to generate ciphertext that can only be read if decrypted.

✓ Types of Encryption

✓ There are two types of encryptions schemes as listed below:

  - Symmetric Key encryption
  - Public Key encryption

2. **Write the short notes on column level VPD.**

   Column level Security with SQL Server

✓ Column level permissions provide a more granular level of security for data in your database. You do not need to execute a separate GRANT or DENY statements for each column; just name them all in a query:

```
GRANT SELECT ON data1.table (column1, column2) TO user1;
GO
DENY SELECT ON data1.table (column3) TO user1;
GO
```

✓ If you execute a DENY statement at table level to a column for a user, and after that you execute a GRANT statement on the same column, the DENY permission is removed and the user can have access to that column. Similarly, if you execute GRANT and then DENY, the DENY permission will be in force.

### 3)Briefly explain about the different Application Types

□ **Mainframe Applications:** Centralized applications running on large, powerful mainframe computers, primarily used for critical business operations and processing large volumes of data.

□ **Client/Server Applications:** Distributed applications where the server hosts resources and services, and the client accesses and uses those resources over a network.

- **Web Applications:** Applications that run on a web server and are accessed through a web browser via the internet or an intranet.
- **Data Warehouse Applications:** Systems designed for analytical processing and reporting, aggregating data from various sources into a central repository to support business intelligence activities.

## 4)Briefly explain the architecture of Virtual Private Databases.

- Policy Enforcement Point (PEP):

This is the core component of the VPD architecture. It intercepts SQL statements issued by users or applications to the database.

- Security Policies:

These define the rules for restricting access to rows and columns based on specific conditions such as user roles, user attributes, or SQL conditions.

- Context and Label Security:

VPD uses context and label security to determine which rows or columns a user can access. Context can be based on session information, while label security can be based on data classifications.

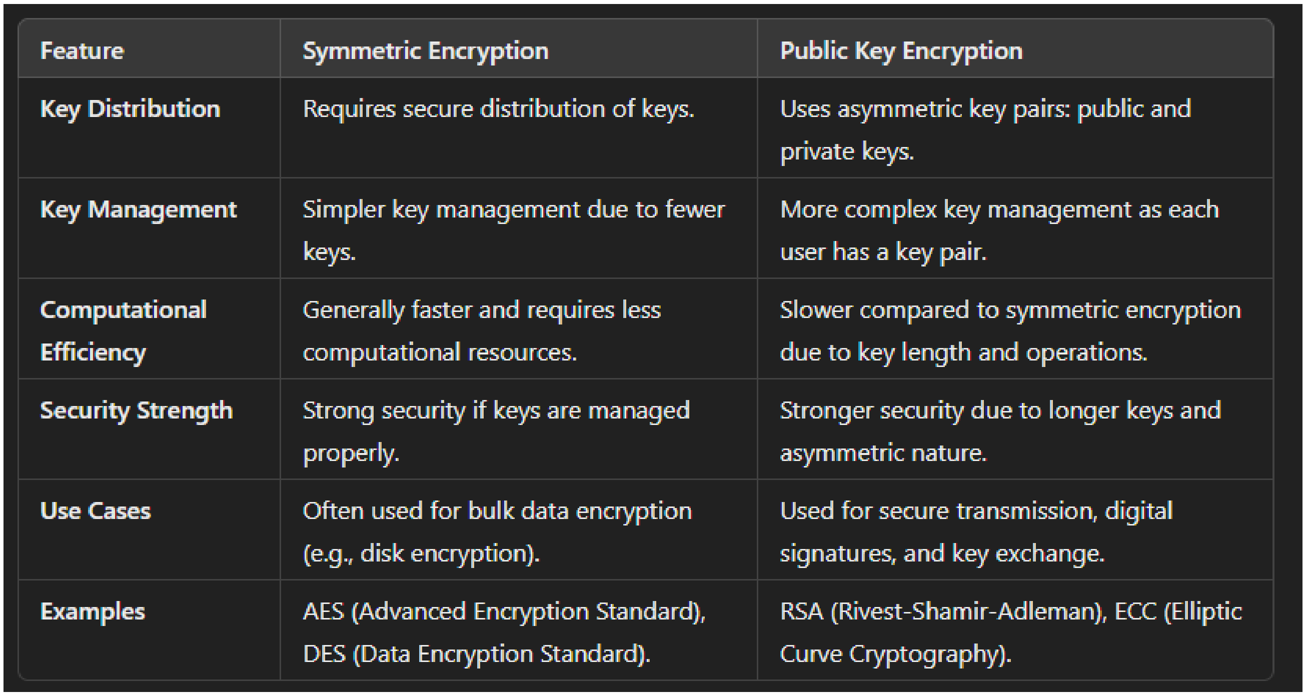
- Predicate Functions:

These are user-defined functions that evaluate the security policies defined for the database. They are used to dynamically append WHERE clauses to SQL queries to enforce access control.

- Fine-Grained Access Control:

VPD provides fine-grained access control, allowing administrators to specify detailed conditions for accessing data. This ensures that users only see the data they are authorized to access.

## 5)Compare Symmetric and public key encryptions schemes.



| Feature | Symmetric Encryption | Public Key Encryption |
|---|---|---|
| **Key Distribution** | Requires secure distribution of keys. | Uses asymmetric key pairs: public and private keys. |
| **Key Management** | Simpler key management due to fewer keys. | More complex key management as each user has a key pair. |
| **Computational Efficiency** | Generally faster and requires less computational resources. | Slower compared to symmetric encryption due to key length and operations. |
| **Security Strength** | Strong security if keys are managed properly. | Stronger security due to longer keys and asymmetric nature. |
| **Use Cases** | Often used for bulk data encryption (e.g., disk encryption). | Used for secure transmission, digital signatures, and key exchange. |
| **Examples** | AES (Advanced Encryption Standard), DES (Data Encryption Standard). | RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography). |

## 6)Write short notes on Client / Server architecture.

client/Server architecture in database security refers to a model where database systems are structured into two primary components: the client, which initiates requests for data or operations, and the server, which manages and provides access to the database. Here are some key points:

1. **Client Responsibilities**:
   - Initiates database requests such as querying data, inserting, updating, or deleting records.
   - Provides user interface and application logic for interacting with the database.
   - May perform initial data processing before sending queries to the server.
2. **Server Responsibilities**:
   - Stores and manages the actual database and its data.
   - Receives requests from clients, processes them, and returns results.
   - Manages concurrency control, transactions, and ensures data integrity and security.

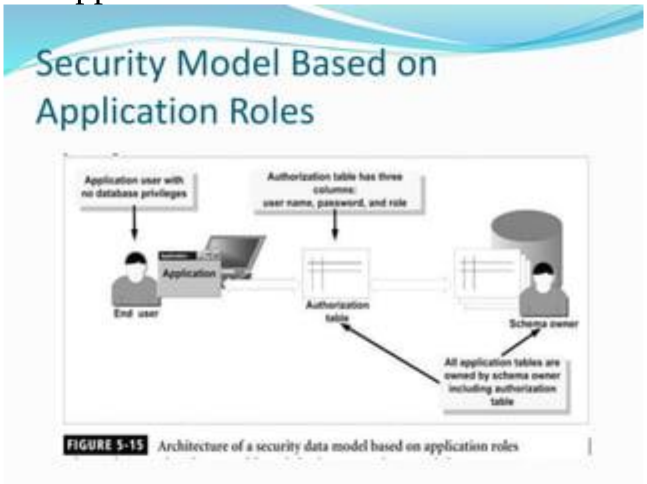
**Communication**:

- ✓ Clients and servers communicate typically over a network using standard protocols (e.g., TCP/IP).
- ✓ Requests from clients are structured in a format understandable by the server (e.g., SQL queries).
- ✓ Responses from the server contain requested data or acknowledge successful operations.

**12 Marks**

1. **Explain the architecture of security data model based on Application roles.**
   **Security Model based on Application Roles**

- ✓ When considering this security model , keeps this point in mind
  - This model is primitive and does not allow the flexibility required to make changes necessary for security
  - Privileges are limited to any combination  like read, add, read / update / admin and so on
  - The following list presents characteristics of this security model
  - Isolating the application security from the database
  - Only one role is assigned to an application user
  - This lowers the risk of database violations
  - Passwords must be securely encrypted
  - The application must use a real database  user to log on and connect to the application database



Security Model Based on Application Roles

Application user with no database privileges
Authorization table has three columns: user name, password, and role
Application
End user
Authorization table
Schema owner
All application tables are owned by schema owner including authorization table

FIGURE 5-15 Architecture of a security data model based on application roles

Security model based on Application Roles and Functions

- ✓ It is a combination of both the role and function security model
- ✓ Depends on the application to authenticate the application users
- ✓ The application authenticates users by maintaining all end users in a table with their encrypted passwords
- ✓ Applications are divided into functions and roles are assigned to functions that are in turn assigned to users.
- ✓ This model is highly flexible in implementing application security.

2. **Discuss the different steps involved in the Virtual Private Network (VPD) setup with suitable syntax.**

   VPD (Virtual Private Database) is shared database schema containing data that belongs to many users , and each user can view or manipulate the data the user owns

- ✓ Not every database system offers a mechanism to implement VPD with out VIEW objects.
- ✓ ORACLE offered VPD in several versions before the release of 10G
- ✓ ORACLE uses two other names to refer VPDs
  - ▪ Row Level Security (RLS)
  - ▪ Fine Grain Access (FGA)

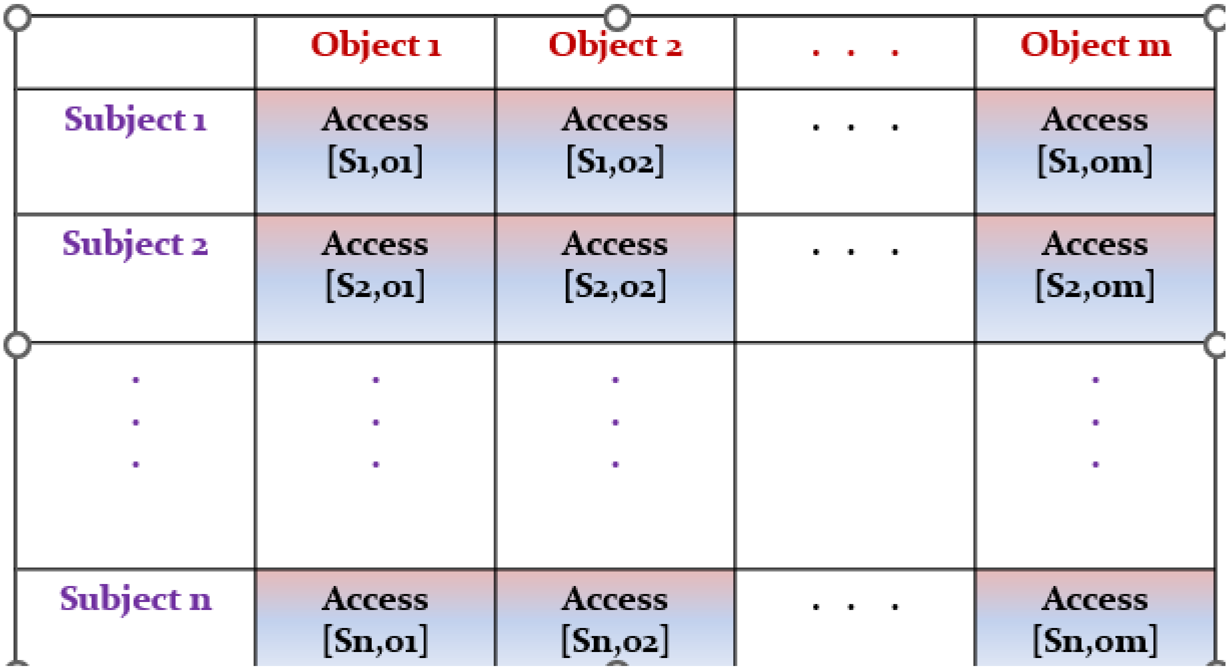
**Security model based on Application Roles and Functions**

- ✓ It is a combination of both the role and function security model
- ✓ Depends on the application to authenticate the application users
- ✓ The application authenticates users by maintaining all end users in a table with their encrypted passwords
- ✓ Applications are divided into functions and roles are assigned to functions that are in turn assigned to users.
- ✓ This model is highly flexible in implementing application security.

3. **What are the two types of security models? Explain in detail with suitable example for each type.**

   There are two security models

   a. Access Matrix Model
   b. Access Modes Model



| | Object 1 | Object 2 | . . . | Object m |
|---|---|---|---|---|
| Subject 1 | Access [S1,o1] | Access [S1,o2] | . . . | Access [S1,om] |
| Subject 2 | Access [S2,o1] | Access [S2,o2] | . . . | Access [S2,om] |
| ⋮ | ⋮ | ⋮ | | ⋮ |
| Subject n | Access [Sn,o1] | Access [Sn,o2] | . . . | Access [Sn,om] |

Access Modes Model

- ✓ This model based on the Take-Grant models
- ✓ It uses both subject and object
- ✓ Object is the main security entity
- ✓ Access mode indicates that the subject can perform any task or not
- ✓ There are two modes
  - ▪ Static Modes
  - ▪ Dynamic Modes
- ✓ Mainframe applications
- ✓ Client / Server Applications
- ✓ Web Applications
- ✓ Data warehouse applications

4. Discuss, how to create Security policies in VPD and write PL/ SQL using oracle to test if VPD is working correctly?
5. Give the importance of password policies. Explain in detail about the design and implementation of password policies.