**Key Terms – CH 6**

* **authentication** The process of confirming the identity of those individuals or applications that request access to a secure environment.
* **authorization** The process of ensuring that those individuals or applications that request access to an environment or an object within that environment have the permission to do so.
* **credential** A piece of information that is used to verify identity, such as a person’s username and password, an application’s secure ID, or a host’s network name and address.
* **database link** A link made between two databases that when created results in one logical data storage unit. Links are created in Oracle to apply common policies and to create associations between databases.
* **digital certificate** A password-protected and encrypted file that holds the identity of a user or object.
* **inference** A way that unauthorized users can obtain sensitive information by making assumptions based on the database’s reactions or query responses to nonsensitive queries.
* **Kerberos** An authentication protocol that was built by MIT to provide secure means for authentication using symmetric-key cryptology to verify the identity of a client to a server and a server to a client.
* **login**An object that is mapped to a user account within each database and is associated to users by the security identifier or SID.
* **Mixed Mode Authentication** A form of authentication that allows both Windows authentication and SQL Server authentication to be used. The database will accept both Windows and server logins.
* **principle of least privilege** A security standard by which each user added to a system is given the minimum set of privileges that he or she requires to conduct legitimate business within that system.
* **privilege** The ability to access a specific database resource or to perform a specific action within a database.
* **polyinstantiation** A strategy that allows the database to contain multiple instances of a record, all pointing to the same primary key, but contain and display different values to users of different security classifications.
* **role** A set of related privileges that are combined to provide a centralized unit from  which to manage similar users or objects of a database.
* **service ticket** A unique key that is used to validate a person’s identification (similar to a driver’s license), for the purpose of gaining access into a secured environment.
* **user profile** A set of rules that limits a user’s access to database resources, and can be used to set password restrictions as well.
* **Windows Authentication mode** A form of authentication that allows only Windows authentication to be used for accessing the database; those users logging in to the  database must have a Windows login to access it.