**4.1 Briefly define the difference between DAC and MAC.**

In a discretionary access control (DAC) system, the owner of a resource designates who can access it and to what level. In a mandatory access control (MAC) system, resources are given a label such (ie secret, top secret, etc) and users are given a clearance, and only users with an appropriate level of clearance may access a resource with a given label.

**4.3 List and define the three classes of subject in an access control system.**

The three classes of subject are owner, group, and world. The owner is the user in charge of a resource, often with many special privileges. Group access goes to a group of users with special privileges regarding a resource, though not necessarily as many as the owner. World access is for users who are capable of accessing the system the resource is in but don’t have any special access.

**4.5 What is an access right?**

An access right is the degree to which a subject is allowed to access an object.

**4.7 What is a protection domain?**

A protection domain is a group of objects that all share a common access right.

**4.9 List and define the four types of entities in a base model RBAC system.**

The four types of entity in a basic RBAC system are users, roles, permissions, and sessions. A user is anyone who has access to the systems covered by RBAC. A role is a particular set of functions or responsibilities that a user can have. Permissions are the level of access to resources that a role can have. A session is the relationship between a user and roles outlining what roles they have.

**4.11 In the NIST RBAC model, what is the difference between SSD and DSD?**

Static separation of duty (SSD) means that certain roles in a role based model are mutually exclusive such that a user with one role cannot have a certain other role ever. Dynamic separation of duty (DSD) is similar to static separation of duty, but the mutually exclusive roles is per session only.