4.

（1）用户身份鉴别：系统提供的最外层安全保护措施，通过由用户名和用户标识号组成的用户标识进行判定，包括静态口令识别，动态口令识别，智能卡识别等。

（2）存取控制：定义用户权限，并将用户权限登记到数据字典中，用户发出存取数据库操作请求，DBMS通过查看数据库字典进行合法权限检查，包括自主存取控制，强制存取控制。

（3）视图：视图能够对机密数据提供安全保护，将机密数据对无权用户进行隐藏。

（4）审计:通过建立审计日志，将用户对数据库的所有操作记录在上面，审计员利用审计日志，监控数据库中的各种行为来发现非法存取及潜在威胁。

（5）数据加密：根据一定的算法将原始数据（明文）变换成不可直接识别的格式（密文），包括存储加密，传输加密。

6.

（1）

GRANT ALL PRIVILEGES

ON TABLE 学生，班级

TO U1

WITH GRANT OPTION;

（2）

GRANT SELECT,UPDATE(家庭地址)

ON TABLE 学生

TO U2;

（3）

GRANT SELECT

ON TABLE 班级

TO PUBLIC;

（4）

GRANT SELECT,UPDATE

ON TABLE 学生

TO R1;

（5）

GRANT R1

TO U1

WITH ADMIN OPTION;

7.

(1)

GRANT SELECT

ON 职工，部门

TO 王明;

(2)

GRANT INSERE,DELETE

ON 职工，部门

TO 李勇;

(3)

GRANT SELECT

ON 职工

WITH USER（）=NAME

TO PUBLIC；

(4)

GRANT SELECT，UPDATE(工资)

ON 职工表

TO 刘星；

(5)

GRANT ALTER TABLE

ON 职工，部门

TO 张新;

(6)

GRANT ALL PRIVILICES

ON 职工，部门

TO 周平

WITH GRANT OPTION;

(7)

GRANT

