Database Integrity, Security and Recovery

- Database integrity
- Database security
- Database recovery

Database Integrity

- Database integrity – refers to correct processing of a database such as applying the appropriate business rules when performing a database operations
- Means that data stored in a database are accurate

Database Integrity

- Several ways to ensure data integrity:
  - Domain integrity
  - Entity integrity constraint
  - Referential integrity
  - Business rules
  - Database consistency

Database Integrity

- Domain integrity
  - Means entries in a field or column from the same domain
  - Validation rules can be applied to trap errors
- Entity integrity constraint
  - Each row in a relation must be unique
  - Primary key shows the uniqueness of a rows, cannot be NULL (called entity integrity constraint)
- Referential integrity
  - Means that if a table has a foreign key, then a rows of the key must be exist in the referenced table

Database Integrity

- Business rules
  - Relationship between entities define the business rules
- Database consistency
  - Must be consistent before and after a transaction
  - All database integrity constraints are satisfied

Database Security

- All data must be protected from all types of threats
  - Accidental threats – caused by accidents such as operator carelessness, power failure, disk crashes and fire.
  - Intentional – caused by human, to exploit weaknesses in the system for personal gain. Such as unauthorized access to database

Database Security

- Security measures
  - Views/subschemas
  - Authorization rules
  - Authentication
  - Encryption
  - User-defined procedures

Database Security

- Views/subschemas
  - Different user has a different views.
  - Corresponds to a subset of the database presented to the user
- Authorization rules
  - To restrict access to data and operations
- Authentications
  - Using a specific device to detect personal characteristic

Database Security

- Encryption
  - Used to protect highly confidential or sensitive data
  - Coding or scrambling data to unintelligible form
  - Data must be decrypt before the receiver read it
- User-defined procedures
  - Users write their own procedures to protect data

Database Recovery

- Several approaches to recover from system failures
  - Backup failure – makes a copies of the database
  - Journalizing facilities – used to store the audit trails of transactions and database changes
  - Checkpoint facilities – will refuse to accept any new transaction
  - Recovery manager – restore the database correctly after a failure has occured

Database Recovery

- Types of database failure
  - Aborted transaction – to correct the errors, the system must roll back by undoing the steps for the transaction
  - Incorrect data – updating a database correctly but with uncorrect data
  - System failure – power failure, disk crashed
  - Database destruction – part of database may be destroyed