Chapter: 6 Security (3hrs)

Database security refers to the collective measures used to protect and secure a database or database management software from illegitimate use and malicious threats and attacks.
In other words, the protection of data or information from accidental loss, unauthorized access, modification, destruction and unintended activities can be termed as database security.

Needs of Security in Database

1. ***Protection from improper access***- only authorized users should be granted access to objects of DBMS. This control should be applied on smaller objects (record, attribute, value).
2. ***Protection from inference*** - inference of confidential information from available data should be avoided. This regards mainly statistical DBMSs.
3. ***Database integrity*** - partially is ensured with system controls of DBMS (atomic transactions) and various back-up and recovery procedures and partially with security procedures.
4. ***Operational data integrity*** - logical consistence of data during concurrent transactions (concurrency manager), serializability and isolation of transactions (locking techniques).
5. ***Semantic data integrity*** - ensuring that attribute values are in allowed ranges. This is ensured with integrity constraints.
6. ***Accountability and auditing*** - there should be possibility to log all data accesses.
7. ***User authentication*** - there should be unambiguous identification of each DBMS user. This is basis for all authorization mechanisms.
8. ***Management and protection of sensitive data*** - access should be granted only to narrow round of users.
9. ***Multilevel security*** - data may be classified according to their sensitivity. Access granting should then depend on that classification.
10. ***Confinement (subject isolation)*** - there is necessity to isolate subjects to avoid uncontrolled data flow between programs (memory channels, covert channels).

Security and integrity violations

Database security refers to the protection of data against unauthorized access or corruption and is necessary to ensure data integrity. Similarly, data integrity is a desired result of database security, but the term data integrity refers only to the validity and accuracy of data rather than the act of protecting data.

Q. What is the difference between security & integrity?

Security risks to database systems include, for example:

- Unauthorized or unintended activity or misuse by authorized database users, database administrators, or network/systems managers, or by unauthorized users or hackers (e.g. inappropriate access to sensitive data, metadata or functions within databases, or inappropriate changes to the database programs, structures or security configurations);

- Malware infections causing incidents such as unauthorized access, leakage or disclosure of personal or proprietary data, deletion of or damage to the data or programs, interruption or denial of authorized access to the database, attacks on other systems and the unanticipated failure of database services;
- Overloads, performance constraints and capacity issues resulting in the inability of authorized users to use databases as intended;
- Physical damage to database servers caused by computer room fires or floods, overheating, lightning, accidental liquid spills, static discharge, electronic breakdowns/equipment failures and obsolescence;
- Design flaws and programming bugs in databases and the associated programs and systems, creating various security vulnerabilities (e.g. unauthorized privilege escalation), data loss/corruption, performance degradation etc.;
- Data corruption and/or loss caused by the entry of invalid data or commands, mistakes in database or system administration processes, sabotage/criminal damage etc.

Security Levels /Security at different levels

To protect a database, we must take security measures at different levels.

1. Database System: Since some users may modify data while some may only query, it is the job of the system to enforce authorization rules.
2. Operating System: No matter how secure the database system is, the operating system may serve as another means of unauthorized access.
3. Network System: Since most databases allow remote access, hardware and software security is crucial.
4. Physical System: Sites with computer systems must be physically secured against entry by intruders or terrorists.
5. Human: Users must be authorized carefully to reduce the chance of a user giving access to an intruder.

Authorization

→ Authorization is a security mechanism used to determine user/client privileges or access levels related to system resources, including computer programs, files, services, data and application features.

→ Authorization explains that what you can do and is handled through the DBMS unless external security procedures are available.

→ Database management system allows DBA to give different access rights to the users as per their requirements.

→ In basic Authorization, we can use any one form or combination of the following basic forms of authorizations:

i. *Resource authorization*: Authorization to access any system resource. e.g. sharing of database, printer etc.

ii. *Alternation Authorization*: Authorization to add attributes or delete attributes from relations

iii. *Drop Authorization*: Authorization to drop a relation.

- When the **SQL standard authorization** mode is enabled, object owners can use the GRANT and REVOKE SQL statements to set the user privileges for specific database objects or for specific SQL actions. They can also use roles to administer privileges.

Granting of privileges:

An authorized user may pass on this authorization to other users. This process is called as granting of privileges.

Syntax: GRANT <privilege list>

ON<relation name or view name>

TO<user/role list>

Example: GRANT select

ON Emp_Salary

TO U1, U2 and U3;

Revoking of privileges:

We can reject the privileges given to particular user with help of revoke statement.

Syntax: REVOKE <privilege list>

ON<relation name or view name>

FROM <user/role list>[restrict/cascade]

Example: Revoke select

ON Emp_Salary

FROM U1, U2, U3;

Authentication

Authorization is the process to confirm what you are authorized to perform but Authentication confirms who you are. So the primary goal of authentication system is to allow access to the legal system users and deny access to unauthorized access. The most widely used authentication techniques are:

i. Password Based Authentication

ii. Artifact Based Authentication: It includes machine readable batches and electronics cards. E.g. ATM

iii. Biometric Technique: unique characteristics of individuals. E.g. finger print, voice recognition, etc.

Differences between Authentication and Authorization

Basis for comparison	*Authentication*	*Authorization*
Basic	Checks the person's identity to grant access to the system.	Checks the person's privileges or permissions to access the resources.
Includes process of	Verifying user credentials	Validating the user permissions
Order of the process	Authentication is performed at the very first step	Authorization is usually performed after authentication.
User's point of view	It determines whether user is what he claims to be.	It determines what user can and cannot access.
Example	In the online banking applications, the identity of the person is first determined with the help of the user ID and password.	In a multi-user system, the administrator decides what privileges or access rights do each user have.

Access Control

Access control is the mechanism that enforce rules about who can perform what operation or who can access which data. This access control mechanism must concern with three basic components.

i. *Accesor (Subject):* A subject is a user who is given some right to access a data object.

ii. *Object to be accessed*: An object is something that needs protection. A typical object in a database environment could be a unit of data that need to be protected.

iii. *Types of Access Control*: Once an object is created, the owner may grant the following rights to object to the other authorized user's .Read, run, modify, delete, insert, create and destroy.

- ***Discretionary Access Control (DAC)*:** DAC is a kind of access control system that holds the owner responsible for deciding people making way into a premise or unit. This model utilizes some of the most widely-popular operating systems including Windows etc. A typical example of this system is Access Control Lists (ACLs).

- ***Mandatory Access Control (MAC***): The MAC system doesn't permit owners to have a say in the entities having access in a unit or facility. Typically, this classifies all users and entities and provides label which permits them to pass through the security and gain entry. These labels establish security guidelines and permit subjects to gain access. MAC is more commonly utilized in military-based organizations that place high emphasis on confidentiality and classification of data.

Cryptography

Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages. *Applications of cryptography* include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.

Cryptanalysis is the study of how to crack encryption algorithms or their implementations.

Encryption: Encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot.

Properties of good encryption technique:

i. It is relatively simple for authorized user to encrypt or decrypt data.
ii. It depends not on secrecy of algorithm but rather on secrecy of encryption key.
iii. Its encryption key is extremely difficult for intruder to determine.

Decryption: Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form.

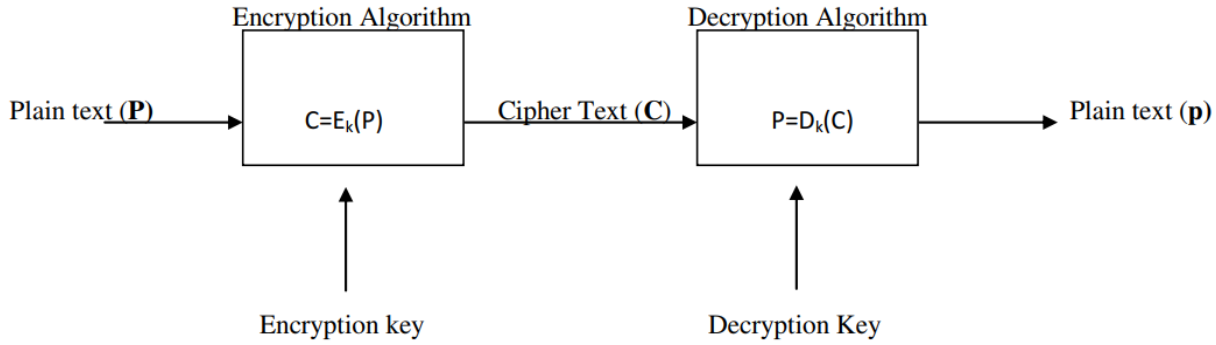


Figure: General Model of Cryptography System

Two types of cryptosystem in use:

i. Private Key Cryptosystem

- It is also called symmetric key cryptosystem.
- It is based on symmetric key algorithm i.e. both encryption and decryption techniques uses the same key.
- The key used for encrypt and decrypt must only be know by the sender and receiver i.e. key must be private hence called as private key cryptography.
- Disadvantage: Prior to message or data transfer, the sender & receiver must agree on cryptographic key. Often this step involves the exchange of key which is potentially troublesome and not secure.

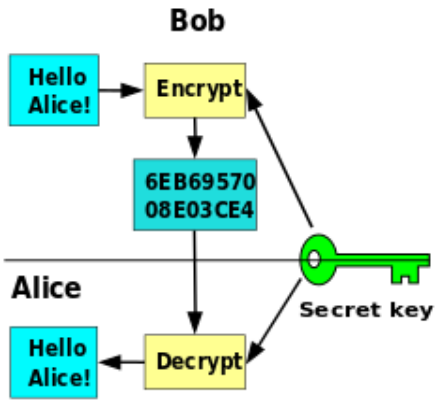


Fig. Private Key Cryptography

ii. Public Key Cryptosystem

- It is also called asymmetric key.
- It is based on asymmetric key algorithm i.e. encryption and decryption techniques uses the different key.
- In this system every user has two keys know as public key and private key. It is also called as asymmetric cryptography because the two keys are not identical.
- In public key encryption, encryption uses public key and decryption is performed using private key.

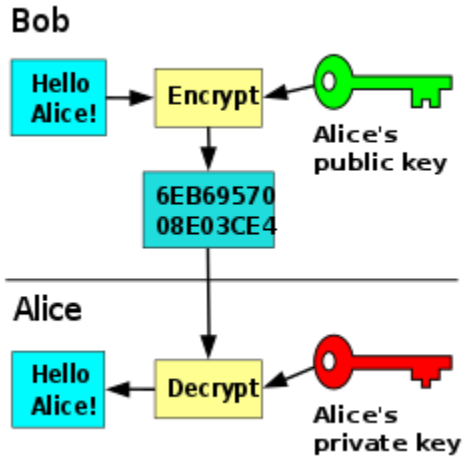
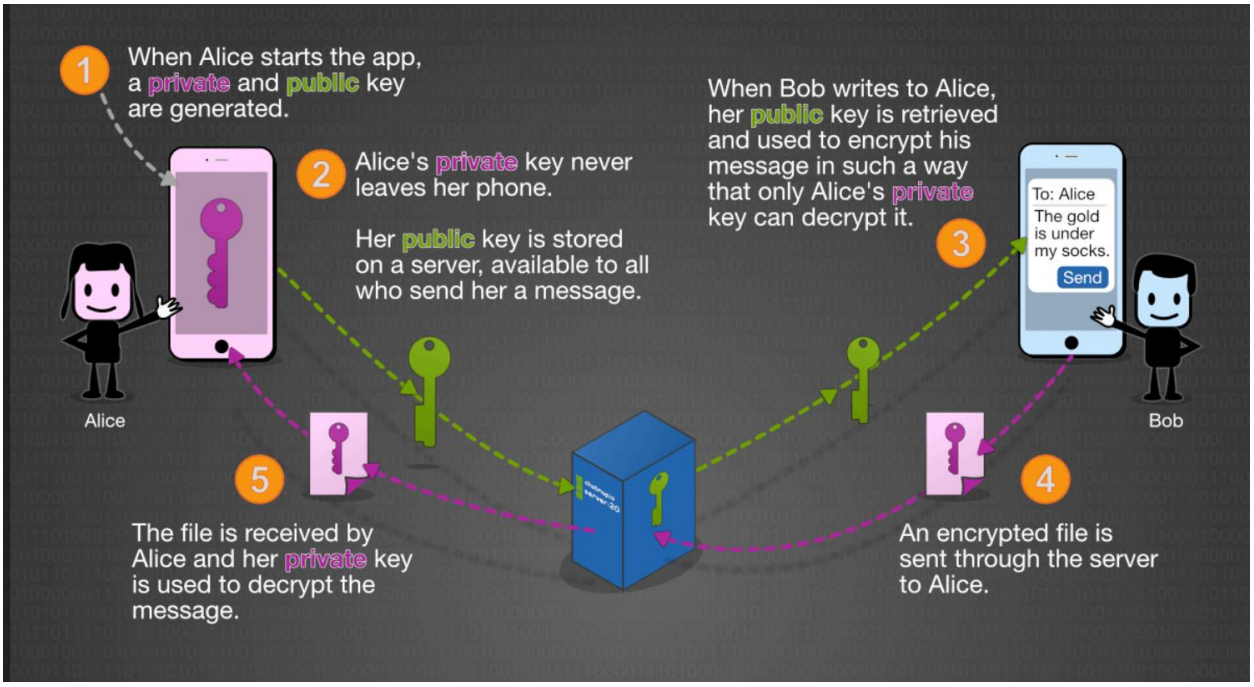


Fig. Public Key Cryptography



Views in SQL

- A view is a virtual table based on the result-set of an SQL statement.
- Views are used for security purpose in databases, views restricts the user from viewing certain column and rows means by using view we can apply the restriction on accessing the particular rows and columns for specific user.
- To create the view, we can select the fields from one or more tables present in the database.
- A view can either have specific rows based on certain condition or all the rows of a table.

SQL CREATE A VIEW

Syntax:

```
CREATE VIEW view_name AS
SELECT column1, column2, ...
FROM table_name
WHERE condition;
```

id	name	mobile_number	username	password
1	Ronaldo	9801234568	ronaldo_007	Football66
2	Messi	9812234768	messi_10	Messi112
3	Pogba	9801245678	pogba_06	Pogba111
4	hazard	9711245679	hazard_7	hazard21
5	degea	9712245899	degea_01	degea11

Table name: social_info

Example:

1. Create a view named social_media_view & display name, username from the table.

Answer: create view social_media_view as select name, username
from social_info;
*select * from social_media_view*;

2. Create a view named view_try & display username from the table.

Answer: create view view_try as select username
from social_info;

SQL Dropping a View

Syntax: DROP VIEW view_name;

Example: DROP VIEW social_media_view;

QUESTIONS

1. Why security is needed in database? How security can be granted using view explain? **OR,** how does a view differ with relation? Explain the role of view in security.
2. Is it necessary to manage security at OS level if security in database level is already done? Explain private key cryptosystem.
3. What is cryptanalysis? Explain private & public key cryptosystem.
4. Differentiate between authorization & authentication.