DATABASE SECURITY

Unit - 8

What is data security?

- Data security is the **protection of the data** from unauthorized users.
- Only the authorized users are allowed to access the data.
- Most of the **users are allowed to access a part of database** i.e., the data that is related to them or related to their department.
- Mostly, the DBA or head of department can access all the data in the database.
- Some users may be permitted only to retrieve data, whereas others are allowed to retrieve as well as to update data.

Security v/s Integrity

Security	Integrity
Data security deals with protection of data.	Data integrity deals with the validity of data.
Data security is making sure that only the people who should have access to the data are the only ones who can access the data.	Data integrity is making sure that the data is correct and not corrupt.
Data security avoids from unauthorized access of data.	Data integrity avoids from human errors, when data is entered.
Data security is implemented through user account (passwords).	Data integrity is implemented through constraints such as Primary key, Foreign key, Check constraints etc.

Authentication v/s Authorization

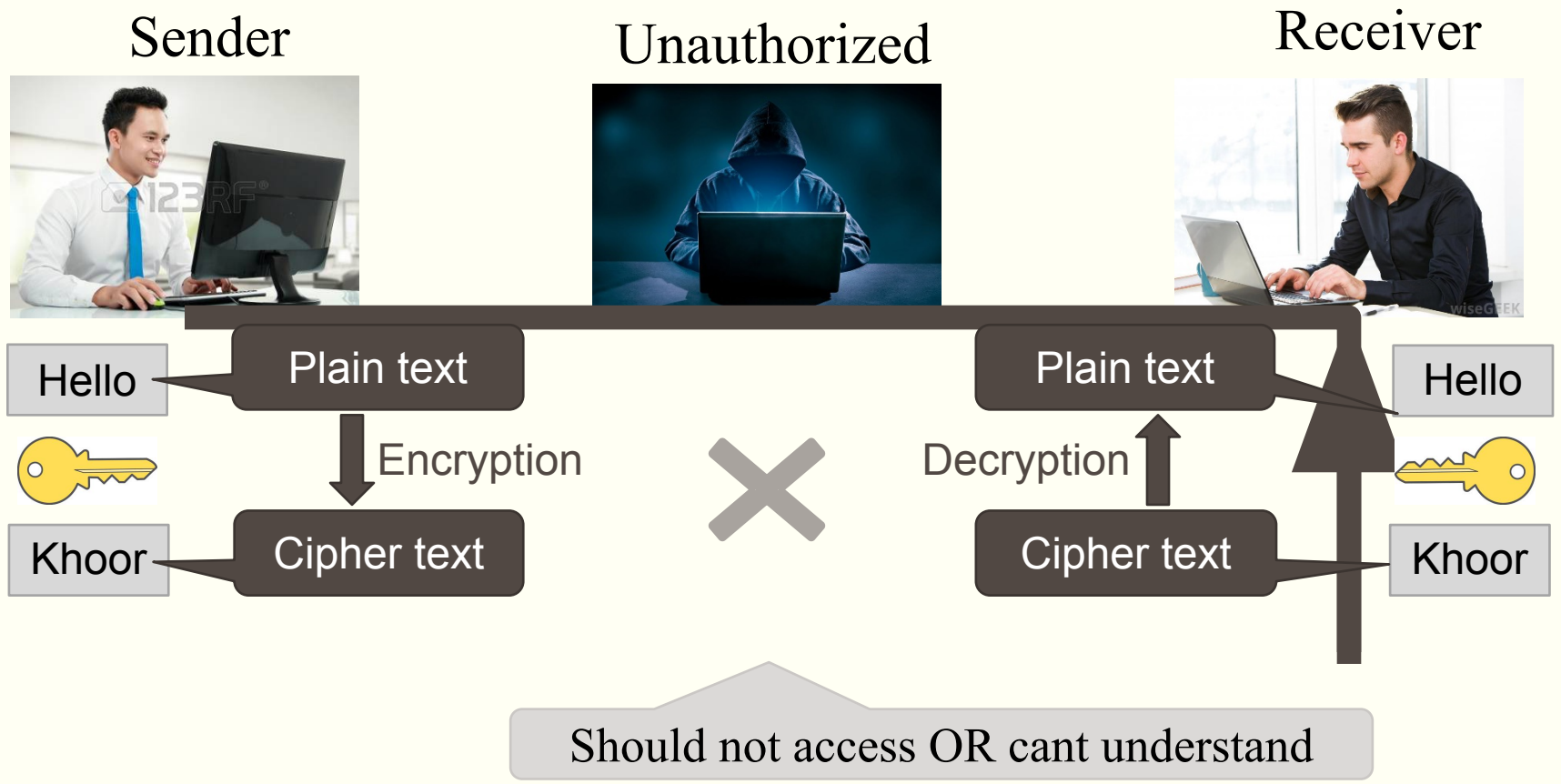
Authentication	Authorization
It is the process of validating a user on the credentials (username and password).	It is the process of verifying whether access is allowed or not.
Logging on to a PC or some website or app with username and password is authentication.	Accessing a file (data) from hard disk or some database is authorization.
It is the process of verifying who you are.	It is the process of verifying what you are authorized to do or not to do.
It is providing integrity control and security to the data.	It is protecting the data to ensure privacy and access control of data.

What is audit trail (audit log)?

- An audit trail (audit log) is a **record which will be generated for each and every transactions**.
- It will **keep certain information** about the transaction.
- An audit trail (audit log) records
  - **Who** (user or the application program and a transaction number)
  - **When** (date and time)
  - From **Where** (location of the user and/or terminal)
  - **What** (identification of the data affected, as well as a before-and-after image of that portion of the database that was affected by the update operation)

What is data encryption?

- Encryption is a **security method in which information is encoded in such a way that only authorized user can read (understand) it**.
- It **uses encryption algorithm to generate cipher text that can only be read if decrypted**.



What is data encryption?

- Data encryption is the **process of encoding (translating) a message or information** in such a way that only authorized persons can access it and those who are not authorized cannot.
- Encryption is the **process of translating plaintext data (plaintext) into something that appears to be meaningless (cipher text)**.
- Decryption is the **process of converting cipher text back to plaintext**.
- Types of Encryption
  - Symmetric key encryption / Private key encryption
  - Asymmetric key encryption / Public key encryption

Types of Encryption

- Symmetric key encryption
  - Encryption and decryption **keys are the same**.
  - The **same key is used by the sender to encrypt the data**, and again **by the receiver to decrypt the data**.
  - Symmetric key encryption is **fast in execution**.

- Asymmetric key encryption
  - Encryption and decryption **keys are the different** (Public Key and Private Key).
  - **Messages are encrypted by sender with one key (Public Key)** and **can be decrypted by receiver only by the other key (Private Key)**.
  - Asymmetric key encryption is **slow in execution due to the high computational burden**.

Access control methods of data security

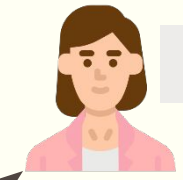
- There are three different methods of data access control:
  1. Discretionary access control (DAC)
  2. Mandatory access control (MAC)
  3. Role based access control (RBAC)

Discretionary access control

- In discretionary access control (DAC), the **owner of the object specifies (decides) which subjects (user) can access the object**.
- In this method a **single user can have different rights on different objects**, as well as **different user can have different rights on the same objects**.

Student

- **Read (Partial rights)**
- **Partial table (Only 1 tuple)**



HOD

- **Read and Write (Full rights)**
- **On entire table (3 tuples)**

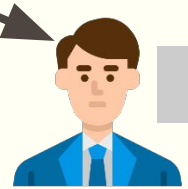
Student

RollNo	Name	Branch	Sem	SPI	BL
101	Raju	CE	3	6	1
101	Mitesh	CE	5	9	0
102	Jay	CE	3	8	0

- **Read (Partial rights)**
- **Partial table (2 or 1 tuples)**

Faculty

- **Read and Write (Full rights)**
- **Partial table (2 or 1 tuples)**



Coordinator

Discretionary access control

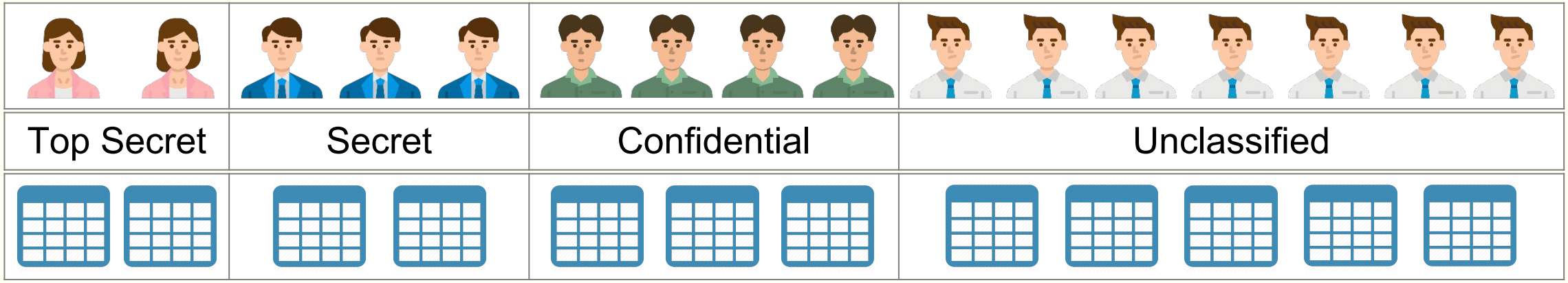
- SQL support discretionary access control through the **GRANT** and **REVOKE** commands.

- **GRANT**
  - This command **gives rights to user** for an object.
  - Syntax:- GRANT privilege ON object TO user [WITH GRANT OPTION]

- **REVOKE**
  - This command **takes back rights** from user for an object.
  - Syntax:- REVOKE privilege ON object FROM user {RESTRICT/CASCADE}

Mandatory access control

- In this method individual user cannot get rights.
- But **all the users as well as all the objects are classified into different categories**.



- Each **user is assigned a clearance level** and each **object is assigned a security level**.
- A **user can access object of particular security level only if he has proper clearance level**.
- The DBMS (system) determines whether the given user can read or write a given object based on some rules.
- This rule makes sure that sensitive data can never be passed to a user without necessary clearance.

Mandatory access control

- Mandatory access control technique for multi-level security uses four components:
  - Subjects:- Such as users, accounts, programs etc.
  - Objects:- Such as relation (table), tuples (records), attribute (column), view etc.
  - Clearance level:- Such as top secret (TS), secret (S), confidential (C), Unclassified (U). Each subject is classified into one of these four classes.
  - Security level:- Such as top secret (TS), secret (S), confidential (C), Unclassified (U). Each object is classified into one of these four classes.
- In the above system **TS>S>C>U**, where **TS>S means class TS object is more sensitive than class S object**.
- A user can access data by following two rules
  - Security property:-
    - Security property states that a **subject at a given security level may not read an object at a higher security level**.
  - Star (*) security property:-
    - Star (*) property states that a **subject at a given security level may not write to any object at a lower security level**.

Role based access control (RBAC) rules

- It restricts database access **based on a person's role within an organization**. The roles in RBAC refer to the levels of access that employees have to the network.
- Employees are only **allowed to access the information necessary to effectively perform their job duties**.
- **Access can be based** on several factors, such as **authority, responsibility, and job competency**.
- In addition, access to computer resources can be limited to specific tasks such as the ability to view, create, or modify a file.
- Lower-level employees usually do not have access to sensitive data if they do not need it to fulfil their responsibilities.
- Using RBAC will help in securing your company’s sensitive data and important applications.

Intrusion detection

- An Intrusion Detection System (IDS) is a system or **software application that monitors network traffic or system for suspicious activity or policy violations and issues alerts when such activity is discovered**.
- It is a software application that scans a network or a system for harmful activity or policy breaching.
- Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system.
- A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.

SQL injection

- SQL injection, also known as SQLI, is a common **attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed**.
- This information may include any number of items, including sensitive company data, user lists or private customer details.
- A successful attack may result in the unauthorized viewing of user lists, the deletion of entire tables, gaining administrative rights to a database, all of which are highly detrimental to a business.

Questions asked in GTU

1. Explain Authorization and access control in brief.
2. What is the difference between data security and data integrity?
3. What is constraint? Explain types of constraints.

Thank
You…!!