Unit - 7

Database Security

Different Levels of Database Security

What is database security?

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. Database security means keeping sensitive information safe and prevent the loss of data. security of data-base is controlled by Database Administrator (DBA).

Database security protects the confidentiality, integrity and availability (CIA) of an organization's databases.

(1) Confidentiality : It means that only authorized individuals/systems can view sensitive or classified information. The data being sent over the network should not be accessed by unauthorized individuals. The attacker may try to capture the data using different tools available on the internet and gain access to our information. A primary way to avoid this is use encryption techniques to safeguard our data so that even if the attacker gain access to our data will not be able to decrypt it.

It prevents essential information from ~~reach~~ reaching the wrong people while making sure that the right people can get it.

(2) Integrity: Integrity refers to the methods for ensuring that data is real, accurate and safeguarded from unauthoriced user modification. It is the property that information has not be altered in an unauthoriced way, and that source of the information is genuine.
It also refers to the assurance that data ~~b~~ has not been tempered with and can thus be trusted. Integrity contributes to the dependability of data by ensuring that it is in the correct condition and free of any unauthorized changes.

(3) Availability: This means that the network should be readily available to its users. This applies systems and to data. To ensure availability, the network administrator should maintain hardware, make regular ~~upgrades~~ ~~upd~~ upgrades, have a plan for fail-over, and prevent bottlenecks in a network. It ensures that authoriced users ~~get~~ get consistent and timely access to resources when they are needed.
Systems, programs, and data are of little utility to a business and its customers if they are not available when authored users require them.

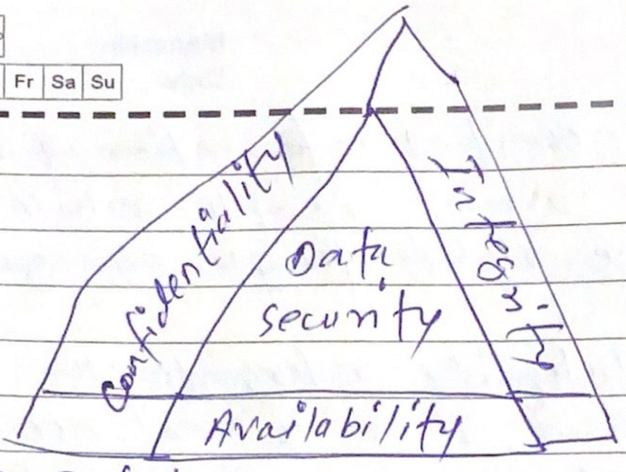


Fig: CIA Triad

Following are some of the most popular database security mechanisms used:

(1) Access Control:

The security mechanism of DBMS must include some provisions for restricting access to the database by unauthorized users. Access control is done by creating user accounts and to control login process by the DBMS. So, that database access of sensitive data is possible to those people (database users) who are allowed to access such data and to restrict access to unauthorized persons.

The database system must also keep the track of all operations performed by certain user throughout the entire login time.

Access control entails limiting unauthorized users' or roles access to the database and its objects, such as tables, views, and stored procedures.

(2) Authentication :

Database security that verifies the user's login information stored in the database is known as database authentication. The user can access the database if their login information matches what is in there. In other words, the user must authenticate before accessing your database. In other words authentication is the process of confirmation that whether the user login only according to the rights provided to him to perform the activities of database.

A particular user can login only upto his privilege but he can't access the other sensitive data.

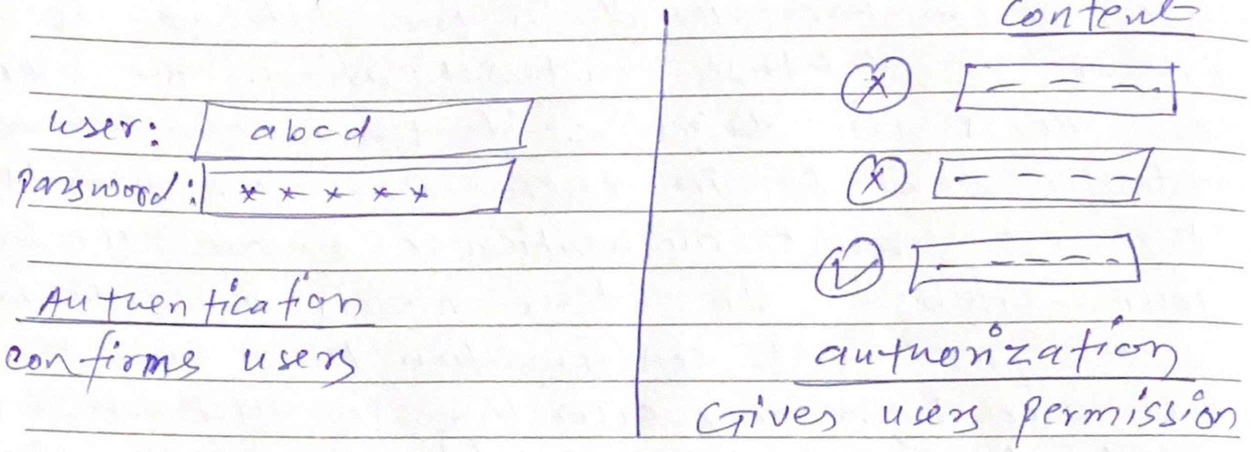
~~By using~~ E.g : Password, Biometric etc.

(3) Authorization :

Authorization is basically identifying ang giving users access to the resources. In DBMS, authorization manager provides access to the user depending upon the roles. It is a way to check if the user has ~~per~~ permission to use a resource or not.

*) Authorization is the process of giving permission to access the resources.

*) It is usually done once the user is successfully authenticated.



(4) Non-Repudiation:

Non-repudiation, initially a legal idea, now extends its significance to computing, information security, and communication. In ensures that any institution involved cann't reject the transmission or reception of a message, utilizing encryption, digital signature, or approval of information. Furthermore, it prevents the denial of the legitimacy of one's signature on a document. This Concept plays an important role in encouraging trust and accountability in various domains, uderlining its widespread adoption in today's digital world.

Non-repudiation ensures proof of where data Comes from, its ~~guiness~~ guineness, and it hasn't been altered. It Confirsms who sent the information and varifies the identity of the recipient. Both parties can't deny that the communication or was handled in this way. This aspect of security is crucial for maintaining trust and reliability in various process.

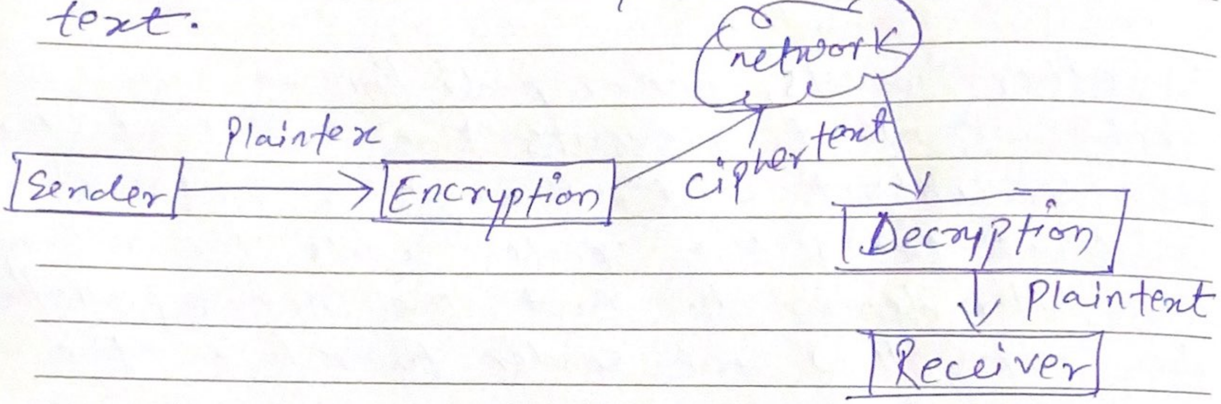
In other words, non-repudiation is a mechanism that prevents the denial of the message content sent through a network. In some cases the sender sends the message and later denies it. But the non-repudiation does not allow the sender to refuse the receiver.

The burden of proving the identity comes on the receiver.
The receiver must be able to prove that the received message has come from a specific sender.

(5) Encryption and Decryption:
Encryption is the process of converting normal message (plaintext) into meaningless message (ciphertext). whereas decryption is the process of converting meaningless message (ciphertext) into its original form (plaintext).

Encryption is the process which takes place at senders end. Its major task is to convert the plain text into cipher text.

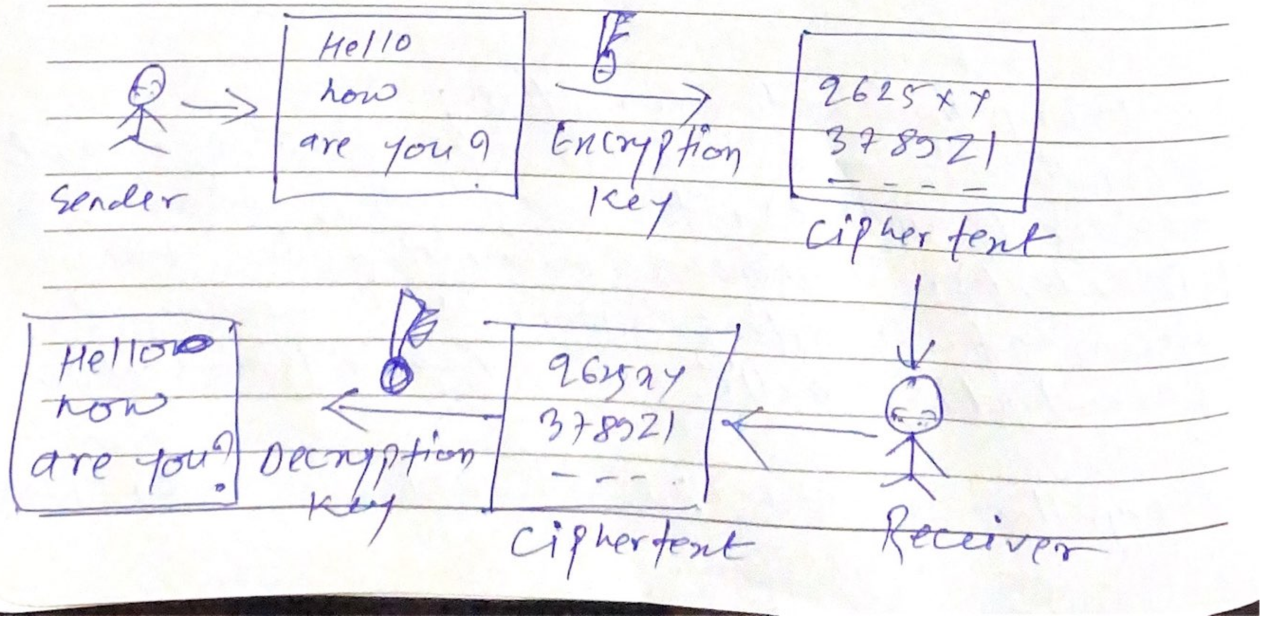
Decryption is the process which take place at receiver's end. while its main task is to convert the cipher text into plain text.



(*) The same algorithm with the same key is used to the encryption-decryption process.

(*) Any message can be encrypted with either secret ~~ke~~ key or public key.

(*) The encrypted message can be decrypted with either secret key or private key.


Hello
how
are you?
Sender
Encryption
Key
2625x7
378921
cipher text
Hello
how
are you?
Decryption
key
9625x7
378921
Ciphertext
Receiver