Chapter 5 Security

5.1 Database Security

5.2 Need of Security

5.3 Security and integrity violation

5.4 Access control

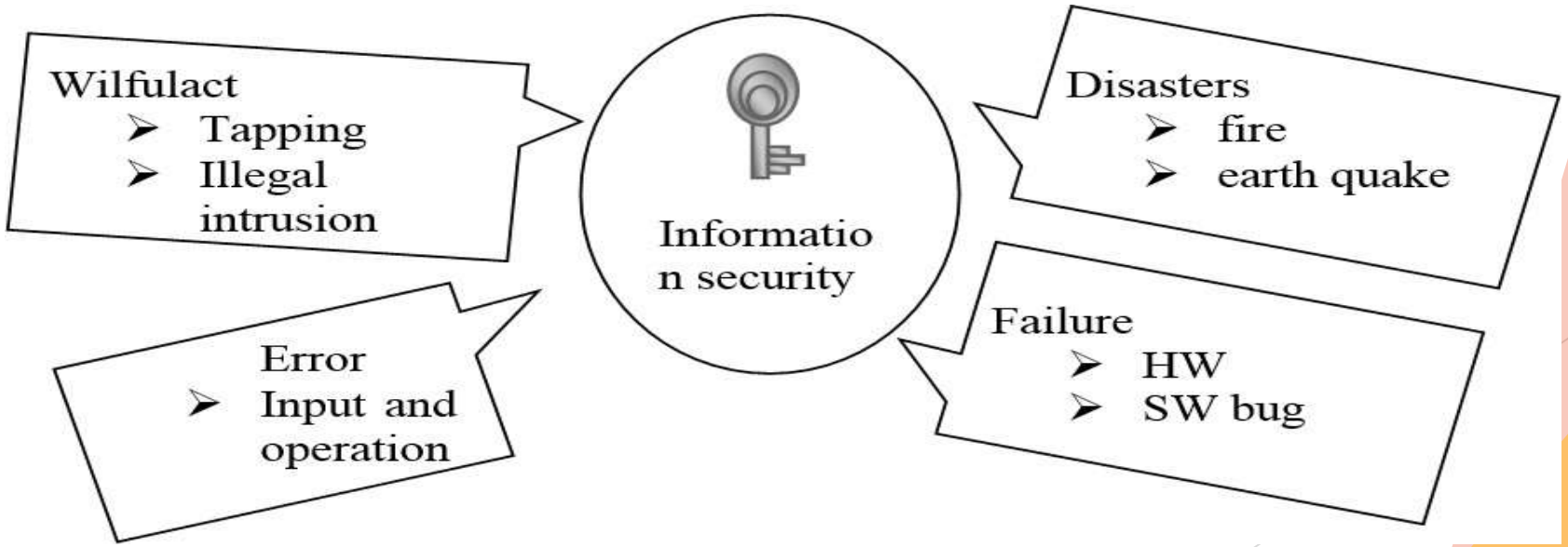
5.5 Authorization

5.5 Security and Views

5.7 Encryption and Decryption

5.1 Database Security

- Database security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.
- Security of data against intentional or unintentional threats.



5.1 Database Security

- Designing and implementing a secure database involves achieving the following objectives:
  - **Confidentiality:** Prevent the disclosure or leak of sensitive information from unauthorized people, resources, and processes.
  - **Integrity:** The protection of system information or processes from intentional or accidental modification.
  - **Availability:** The assurance that systems and data are accessible by authorized users when needed.
  - **Authentication:** Making sure the data is from where it is supposed to be from.

5.1 Database Security : Security attacks

- **Interruption**
  - This is an **attack on availability**.
  - **Example:** Cutting of a communication line or the disabling of the file management system.

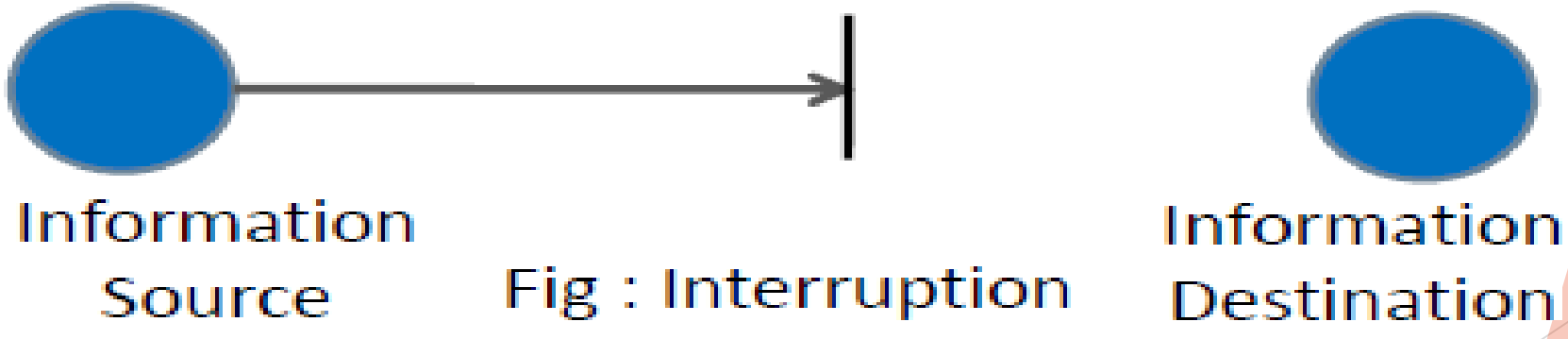


Fig : Interruption

5.1 Database Security : Security attacks

- **Interception**
  - This is an **attack on confidentiality**.
  - **Example:** Wiretapping to capture data in a network and unauthorized copying of files or programs.

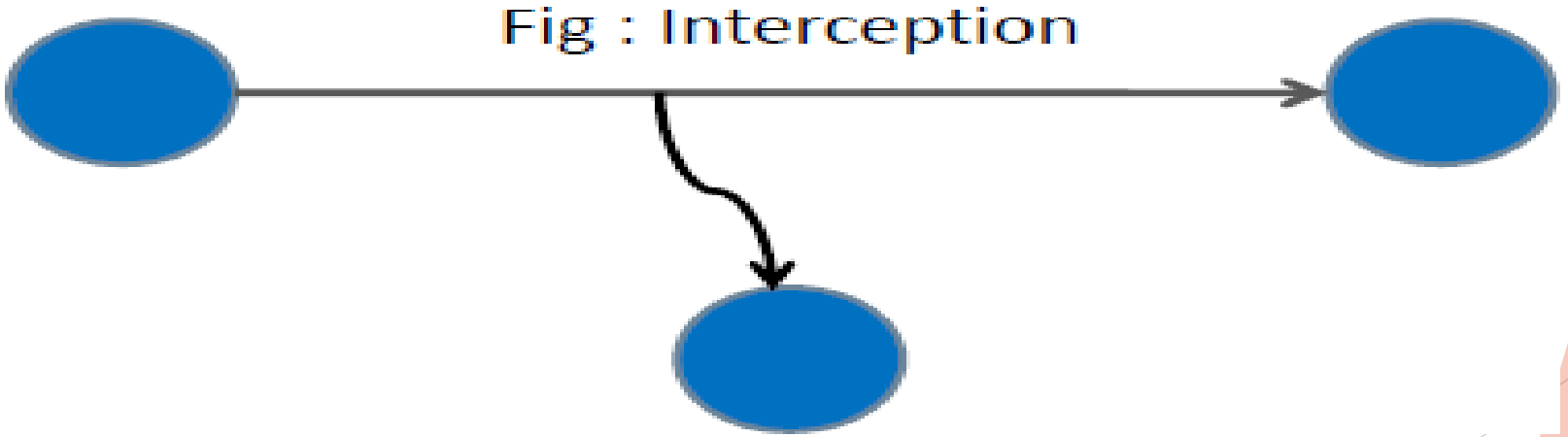


Fig : Interception

5.1 Database Security : Security attacks

- **Modification**
  - This is an **attack on integrity**.
  - **Example:** Changing values in a data or modifying the content of message being transmitted.

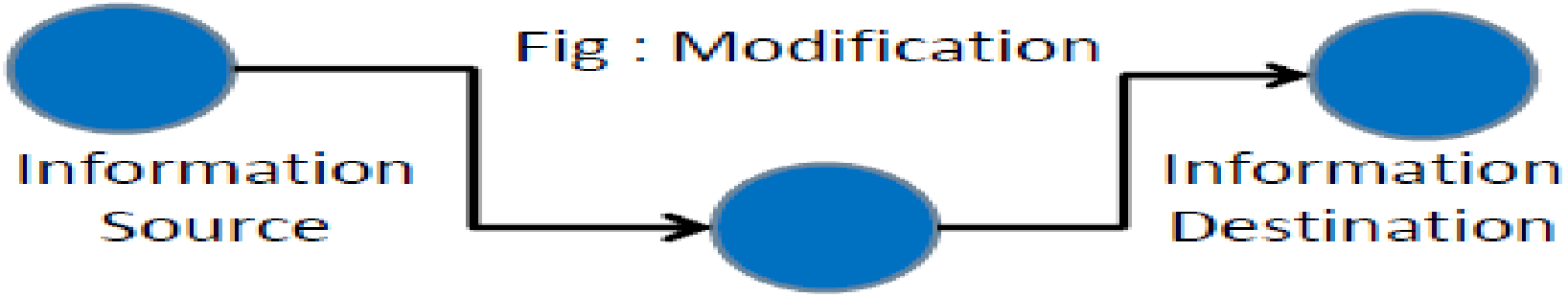


Fig : Modification

5.1 Database Security : Security attacks

- **Fabrication**
  - This is an **attack on authenticity**.
  - **Example:** Insertion of fake messages in a network.

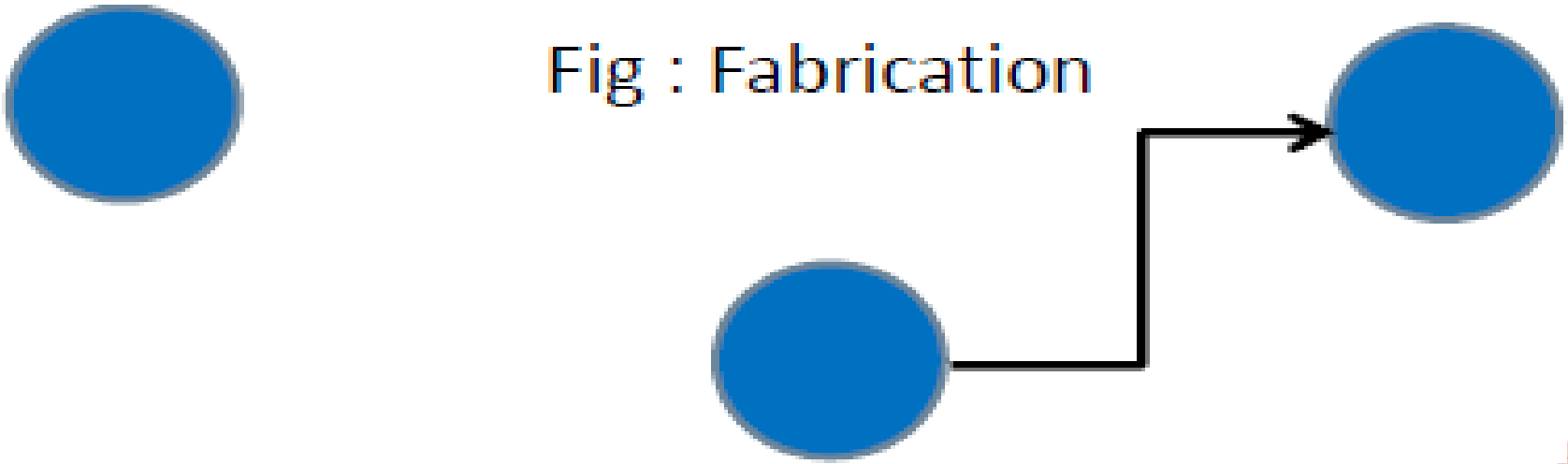


Fig : Fabrication

5.2 Need of Database Security

- Security considerations will apply not only to the data stored in an organization's database:
- A breach of security may impact other aspects of the system, which may ultimately affect the database structure.
- As a result, database security encompasses hardware parts, software parts, human resources, and data.

5.2 Need of Database Security

- Security is an important concern in database management because the information stored in a database is a very valuable and, at times, quite sensitive commodity.
- As a result, data in a database management system must be protected from abuse and illegal access and updates.
- Although most security breaches are caused by hackers, in reality, insiders account for 80% of data loss.
- The extent to which an incident, such as a data breach, can harm our company is determined by several factors.

5.2 Need of Database Security

- How much harm a data breach inflicts on your enterprise depends on a number of consequences or factors:
  - **Compromised intellectual property:** Your intellectual property—trade secrets, inventions, proprietary practices—may be critical to your ability to maintain a competitive advantage in your market. If that intellectual property is stolen or exposed, your competitive advantage may be difficult or impossible to maintain or recover.

5.2 Need of Database Security

- **Damage to brand reputation:** Customers or partners may be unwilling to buy your products or services (or do business with your company) if they don't feel they can trust you to protect your data or theirs.
- **Business continuity (or lack thereof):** Some business cannot continue to operate until a breach is resolved**.**
- **Costs of repairing breaches and notifying customers:** In addition to the cost of communicating a breach to customer, a breached organization must pay for forensic and investigative activities, crisis management, triage, repair of the affected systems, and more.

5.3 Control Methods of Database Security

- Security of database is controlled by DBA.
- **Database Security and the DBA**
  - The database administrator (DBA) is the central authority for managing a database system.
  - The DBA's responsibilities include granting privileges to users who need to use the system and classifying users and data in accordance with the policy of the organization.
  - The DBA has a DBA account in the DBMS, sometimes called **a system or superuser account**, which provides powerful capabilities that are not made available to regular database accounts and users.

5.3 Control Methods of Database Security

Database Security and the DBA

- DBA- privileged commands include commands for granting and revoking privileges to individual accounts, users, or user groups and for performing the following types of actions:
  - **Account creation.** This action creates a new account and password for a user or a group of users to enable access to the DBMS.
  - **Privilege granting.** This action permits the DBA to grant certain privileges to certain accounts.
  - **Privilege revocation.** This action permits the DBA to revoke (cancel) certain privileges that were previously given to certain accounts.
  - **Security level assignment.** This action consists of assigning user accounts to the appropriate security clearance level.

5.3 Control Methods of Database Security

- Following are the control measures :
  - Access Control
  - Authentication
  - Authorization
  - Integrity Control
  - Views
  - Encryption
  - Backup and Recovery

5.3 Control Methods of Database Security

Access Control

- Database access control is a method of allowing access to company's sensitive data only to those people (database users) who are allowed to access such data and to restrict access to unauthorized persons.
- It includes two main components: **authentication and authorization.**

5.3 Control Methods of Database Security

Access Control

- Preventing unauthorized persons from accessing the system itself, either to obtain information or to make malicious changes in a portion of the database.
- The security mechanism of a DBMS must include provisions for restricting access to the database system as a whole.
- This function, called **access control**, is handled by **creating user accounts and passwords to control the login process** by the DBMS.

5.3 Control Methods of Database Security

Access Control

- In practice, there are two major approaches to data security.
  - **Discretionary control:** In this type of security, a user will have different access rights, also known as **privileges on individual items**. Obviously, there are various limitations in terms of rights that different users have on various objects.
  - For example, in a system for which the discretionary control is used, a user may be able to access object X of the database, but cannot access object Y, while user B can access object Y, but cannot access object X. Discretionary control schemes are very flexible. We can combine rights and assign to users and objects according to our needs.

5.3 Control Methods of Database Security

Access Control

- In practice, there are two major approaches to data security.
  - **Mandatory control:** In this case, each data object is associated with a certain classification level and each user is given a certain permission level. A given data object can then be accessed only by users with the appropriate permission. Mandatory schemes are hierarchic in nature and are hence more rigid than discretionary ones.

5.3 Control Methods of Database Security

Authentication

- Authentication is the process by which users are identified by the DBMS and prove their identity to access the database.
- User and group identity validation is achieved through security facilities located outside of the DBMS that is,
- they are performed as part of the operating system or using a third-party security facility, such as Kerberos or Lightweight Directory Access Protocol (LDAP).

5.3 Control Methods of Database Security

Authentication

- Authentication of a user requires two elements: a user ID and an authentication token.
- The user ID allows the security component to identify the user and by supplying the correct authentication token (a password known only by the user and the security component), the user identity is verified.
- After successful authentication of a user, the authenticated user ID is mapped to an authorization ID.

5.3 Control Methods of Database Security

Authentication

- Usually, authentication by a server entails the use of a user name and password. Other ways to authenticate can be through cards, retina scans, voice recognition, and fingerprints.
- Authentication does not determine what tasks the individual can do or what files the individual can see. Authentication merely identifies and verifies who the person or system is.

5.3 Control Methods of Database Security

Authorization

- After a user is authenticated, it is necessary to determine whether that user is authorized to access certain data or resources.
- Authorization is the process of granting privileges, which allows a subject to have legitimate access to a system or an object in a system.
- The definition of authorization contains the terms subject and object.
- The subject refers to a user or program and the term object addresses a table, a view, an application, procedure or any other object that can be created in the system

5.3 Control Methods of Database Security

Authorization

- Authorization control can be implemented by software elements and it can regulate both systems and objects to which a user has access and what a user can do with them.
- A user may have several forms of authorization on parts of the database.
  - Read authorization
  - Insert authorization
  - Update authorization
  - Delete authorization

5.3 Control Methods of Database Security

Authorization

- A user may be assigned all, none or combination of these types of authorization.
- A user may be granted to modify the database schema:
  - Index authorization allows the creation and deletion of indexes
  - Resource authorization allows the creation of new relations
  - Alteration authorization allows the addition or deletion of attributes in a relation
  - Drop authorization allows the deletion of relations

5.3 Control Methods of Database Security

Security and Integrity Violation

- Data integrity in the database is the correctness, consistency and completeness of data.
- Data integrity is enforced using the following three integrity constraints:
  - **Entity Integrity** - This is related to the concept of primary keys. All tables should have their own primary keys which should uniquely identify a row and not be NULL.
  - **Referential Integrity** - This is related to the concept of foreign keys. A foreign key is a key of a relation that is referred in another relation.
  - **Domain Integrity** - This means that there should be a defined domain for all the columns in a database.

5.3 Control Methods of Database Security

Security and Integrity Violation

- Integrity violations can occur when an attacker attempts to change sensitive data without proper authorization.
- An example of an integrity violation is when an attacker obtains permission to write to sensitive data and then changes or deletes it.
- The owner of the data might not detect such a change until it is too late, perhaps when the change has already resulted in tangible loss.
- Because of the difficulty of detecting changes and the possible cascading consequences of late detection, many businesses treat integrity violations as the most serious threat to their business.

5.3 Control Methods of Database Security

Integrity Control

- The aim of integrity control is to protect data from unauthorized use and update, by restricting the values that may be held and the operations that can be performed on data.
- Integrity controls may also trigger the execution of some procedure, such as placing an entry in a log that records what users have done what with which data. There are more forms of integrity controls.

5.3 Control Methods of Database Security

Integrity Control

- **Assertions** are also powerful constraints that enforce some desirable database conditions.
- They are checked automatically by the DBMS when transactions are run involving tables or fields on which assertion exists.
- If the assertion fails, the DBMS will generate an error message.

5.3 Control Methods of Database Security

Integrity Control

- For security purposes one can use triggers as well.
- Triggers consist of blocks of procedural code that are stored in a database and which run only in response to an INSERT, UPDATE or DELETE command.
- A trigger, which includes an event, condition, and action, may be more complex than an assertion.
- It may prohibit inappropriate actions, it may cause special handling procedures to be executed, or it may cause a row to be written to a log file in order to store important information about the user and transactions made to sensitive data.

5.3 Control Methods of Database Security

Integrity Control

- For security purposes one can use triggers as well.
- Triggers consist of blocks of procedural code that are stored in a database and which run only in response to an INSERT, UPDATE or DELETE command.
- A trigger, which includes an event, condition, and action, may be more complex than an assertion.
- It may prohibit inappropriate actions, it may cause special handling procedures to be executed, or it may cause a row to be written to a log file in order to store important information about the user and transactions made to sensitive data.

5.3 Control Methods of Database Security

Views

- Views allow the database to be conceptually divided into pieces in ways that allow sensitive data to be hidden from unauthorized users.
- In the relational model, views provide a powerful mechanism for specifying data-dependent authorizations for data retrieval.
- Views allow a user to see information while hiding any information that the user should not be given access to.
- A view is the dynamic result of one or more relational operations that apply to one or more base tables to produce another table.

5.3 Control Methods of Database Security

Views

- A view is always based on the current data in the base tables from which it is built.
- The advantage of a view is that it can be built to present only the data to which the user requires access and prevent the viewing of other data that may be private or confidential.
- A user may be granted the right to access the view but not to access the base tables upon which the view is based.

5.3 Control Methods of Database Security

Views

- Through a view, users can query and modify only the data they can see.
- The rest of the database is neither visible nor accessible.
- Permission to access the view must be explicitly granted or revoked, regardless of the permissions on the view's underlying tables.
- If the view and underlying tables are owned by the same owner, no permissions need to be given on the underlying tables.
- Data in an underlying table that is not included in the view is hidden from users who are authorized to access the view but not the underlying table

5.3 Control Methods of Database Security

Views

- By defining different views and selectively granting permissions on them, a user (or any combination of users) can be restricted to different subsets of data. Access can be restricted to:
  - A subset of the rows of a base table (a value-dependent subset). **For example,** you might define a view that contains only the rows for business and psychology books to keep information about other types of books hidden from some users.
  - A subset of the columns of a base table (a value-independent subset). **For example**, you might define a view that contains all the rows of the titles table, but omits the price and advance columns, since this information is sensitive.

5.3 Control Methods of Database Security

Encryption

- Encryption is the process of encoding data by a particular algorithm, which makes it impossible for a program to read data without the decryption key.
- Usually encryption protects data transmitted through communication lines.
- An unauthorized user who tries to access this encoded data will face difficulty in decoding it, but authorized users are given decoding keys to decode data.

5.3 Control Methods of Database Security

Cryptography

- Cryptography in Greek means **"Secret Writing".**
- It is a Science and Art of transforming message by which it make them secure and immune to attack.
- Cipher refers to different categories of algorithm (encryption & decryption algorithm) in Cryptography.
- The secret key is also input to the algorithm.

5.3 Control Methods of Database Security

Cryptography

- The exact substitutions and transformations performed by the algorithm depend on the key.
- The traditional ciphers are character oriented but the modern one is the bit-oriented.
  - Original message or data that is fed into the algorithm as input => **Plaintext**
  - An Encryption algorithm transforms + Secret Key => **Plaintext to Ciphertext**
  - Decryption algorithm transforms + Secret Key => **Ciphertext to Plaintext**

5.3 Control Methods of Database Security

Cryptography

- There are two types of cryptography :
  - **Private Key cryptography**

    - Single Key or Symmetric Key
  - **Public Key cryptography**

    -Two key or Asymmetric Key

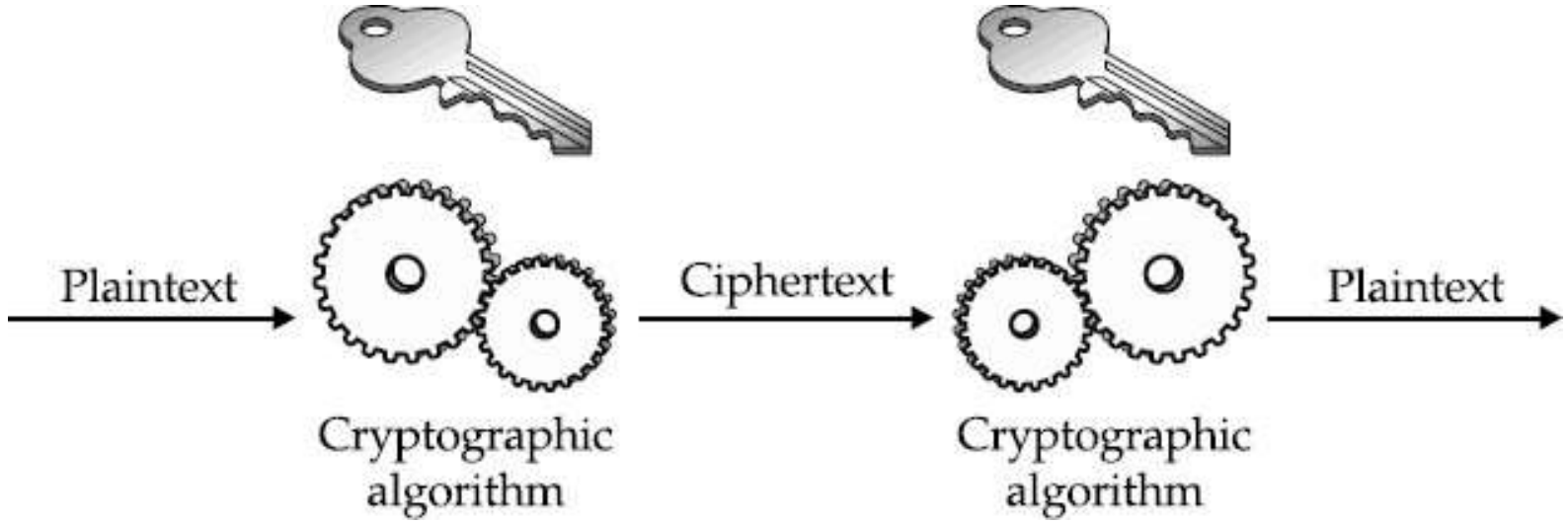
5.3 Control Methods of Database Security

Private Key Cryptography

- In the private key encryption method, the same key is used by the sender (for encryption) and the receiver (for decryption).
- Thus, the key is shared. This method requires maximum number of keys in the internet as individual requires a secrete key.

5.3 Control Methods of Database Security

Private Key Cryptography



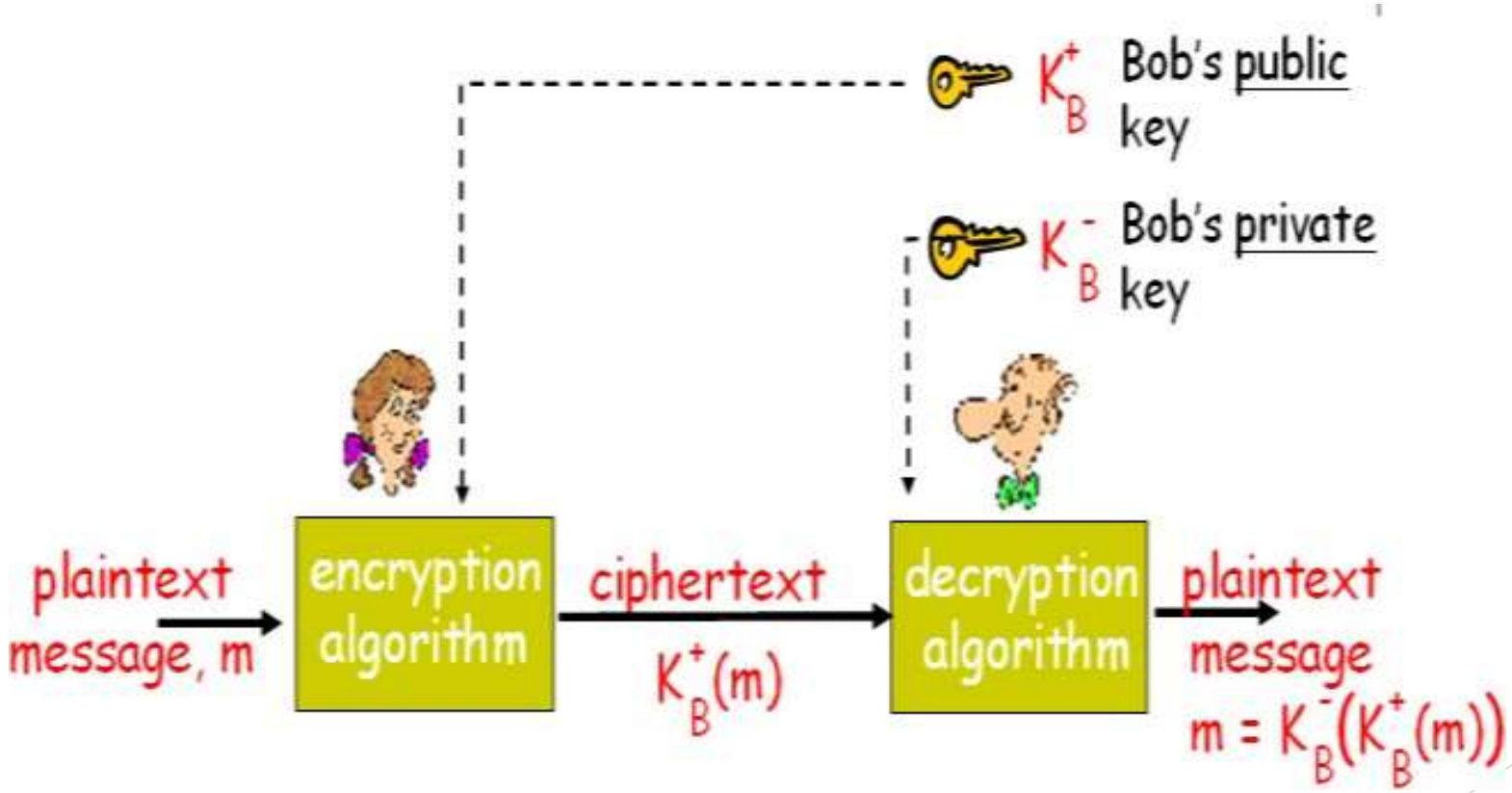
5.3 Control Methods of Database Security

Public Key Cryptography

- To remove the limitation of private key, the asymmetric or public key encryption method is come in existence in which a public key and a private key is used.
- The private key is kept by the receiver and the public key is announced to the public by the same receiver to encrypt all the sending data for him by the general public or anyone.

5.3 Control Methods of Database Security

Public Key Cryptography



Database Security

** Assignment*

- Backup and Recovery
- Difference Between Encryption and Decryption
- Private vs Public Cryptography
- Challenges and Threats in Database Security

This is the end of the lecture!
I hope you enjoyed it.
Thank You