# Chapter 6

# Security

## Introduction

- ✓ Database security means the protection of data or information from accidental loss, unauthorized access, modification, destruction and unintended activities.
- ✓ Database security is about controlling access to information i.e. some information be available freely and other information be available to certain authorized people or groups.
- ✓ So data stored in database need to be protected from authorized access and from any kind of intentional or accidental corruption.

### Need of Database security

Database security is needed for a database due to the following reasons.

- ❖ Unauthorized disclose of information.
- ❖ Unauthorized modification or destruction of valuable information.
- ❖ Unauthorized use of service.
- ❖ Denial of service to the authorized users.

### Security and Integrity violations

The data stored in the database needs to be protected from unauthorized access, malicious destruction or alteration, and accidental introduction of inconsistency.

Misuse of the database can be categorized as being either intentional (malicious) or accidental.

Accidental loss of data consistency may result from:

- ✓ Crashes during transaction processing
- ✓ Anomalies due to concurrent access to the database
- ✓ Anomalies due to the distribution of data over several computers
- ✓ A logical error that violates the assumption that transactions preserve the database consistency constraints.

It is easier to protect accidental loss of data consistency than to protect against malicious access to the database. Among the forms of malicious access are the following:

- ✓ Unauthorized reading of data (theft of information)
- ✓ Unauthorized modification of data
- ✓ Unauthorized destruction of data

The term database **security usually refers to the security from malicious access, while integrity refer to the avoidance of accidental loss of consistency**. In practice dividing between the security and integrity is not always clear. We shall use the term security to refer security and integrity cases where distinction between these concept is not essential.

**To protect database we must take security measures at several levels**.

## 1. Physical level security

Physical-level security in a database refers to the measures taken to protect the physical infrastructure and resource.

It focuses on safeguarding the hardware, network infrastructure, and storage devices where the database resides.
It includes:

- ✓ Protection of equipment from floods, power failure etc.
- ✓ Protection of disk from theft, erase, physical damage etc.
- ✓ Protection of network and terminal cables.

## 2. Human level security

- ✓ Human-level security in a database refers to the security measures and practices implemented to address the potential risks and vulnerabilities associated with human users and their actions within the database environment.
- ✓ It focuses on minimizing the possibility of intentional or unintentional security breaches caused by human factors.

  Here are some key aspects of human-level security in a database:

  - ❖ Providing security training and awareness programs for database users
  - ❖ track and record user activities within the database
  - ❖ ensuring strong password policies (e.g., enforcing password complexity, regular password changes)

## 3. Operating system level security

- ✓ It refers to the security measures implemented by the underlying operating system to protect the data in database
- ✓ No matter how secure the database system is, weakness in operating system security may serve as a means of unauthorized access to the database.
- ✓ since almost all database systems allow remote access through terminals or networks, software level security within the operating system is important as physical security.

## 4. Network level security

- ✓ The database information must be protected from hackers and attack of viruses, leakages of data while being transferred from one computer to other in a network or internet
- ✓ Each site must be ensure that it is communicate with trusted sites (not intruders)

### 5. Database level security

- ✓ Database system users may be authorized to access only limited portion of the database.
- ✓ Here user may be allowed to issue queries without any modification.
- ✓ Also several views can be utilized as a form of security in the database because it can be used to hides the confidential columns from viewing and manipulation.

## Access control

- ✓ Access control mechanism enforces rules who can perform what operation or who can access which data.
- ✓ Alternatively, It is a security policy specifies who is authorized to do what

This access control mechanism must concern with three basic components.

### 1. Accessor (Subject)

- ✓ A subject is an active element in the security mechanism that operates on the object.
- ✓ A subject is a user who is given some right to access a data object.
- ✓ A subject may be a class of users or even an application program.
- ✓ To provide security to object, identification and authentication of accessor is required.
- ✓ The process of identification may be performed with the help of password, finger print or voice pattern etc.

### 2. 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.

**Object can be classified as**

**Data:** These are prime candidates for protection. Data object may be file, record, table etc.

**Access Path:** Access path to be followed for accessing a particular data item or service is an important object by itself in any security mechanism.

**Schema:** The database schema is another object for protection. Since schema declaration defines access right to different data object, anyone having access to schema declaration can eventually attain access right to different data items also. This is highest level of security.

**Views:** The views may involve read only facility of the data items and no modification will be permitted for one class of users while other call of user might be able to update view also.

**Communication Object:** In a distributed database environment, some communication protocols have to be maintained for reliable communication of environment. The communication protocol may include necessary information for the identification and authentication of the sender and receiver.

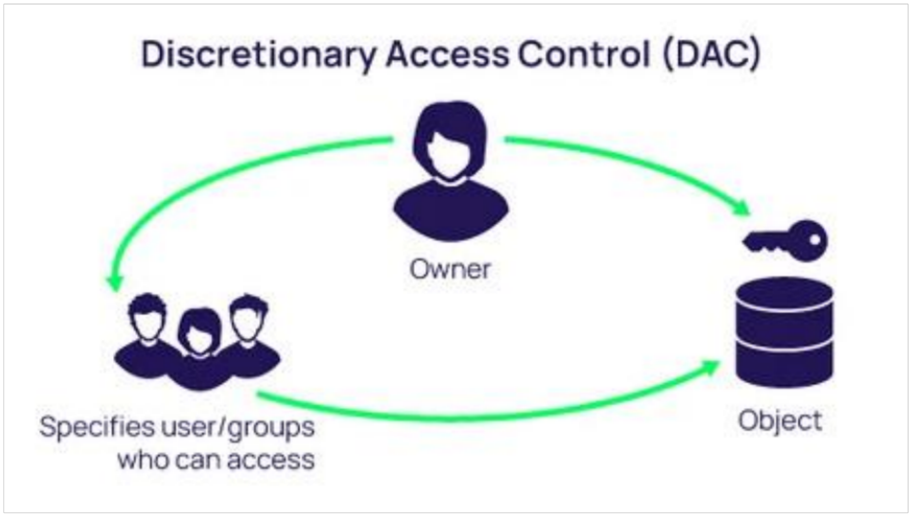
## 3.Types of Access Control

Once an object is created, the owner may grant the following rights to object to the other authorized users. Read, insert, delete, update, run, create and destroy.

There are following types of access control:

### 1. Discretionary Access Control (DAC)

- ✓ Discretionary Access Control (DAC) allows each user to control access to their own data.
- ✓ An individual user (object owner) can set an access control mechanism to allow or deny to access the object.
- ✓ This model is called Discretionary because the control of access is based on the discretion of the owner.
- ✓ Each resource object on a DAC based system has an Access Control List (ACL) associated with it. An ACL contains a list of users and groups to which the user has permitted access together with the level of access for each user or group. For example, User A may provide read-only access on one of their files to User B, read and write access on the same file to User C and full control to any user belonging to Group.


Discretionary Access Control (DAC)
Owner
Specifies user/groups who can access
Object

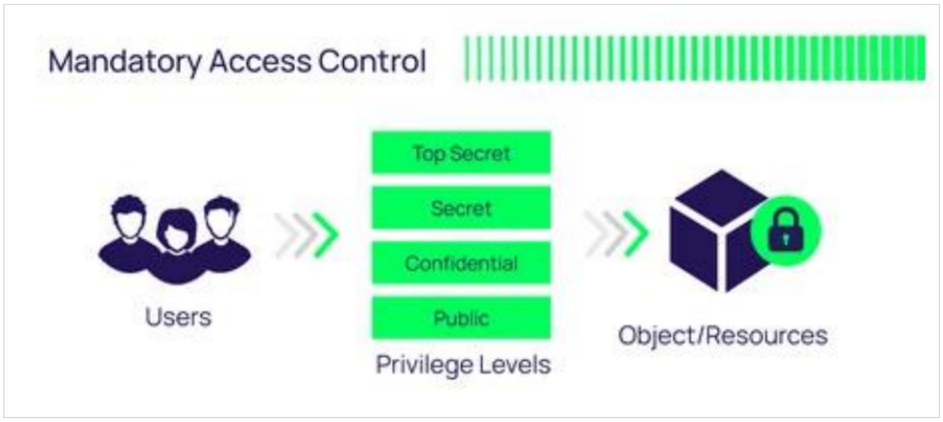
## 2. Mandatory Access Control(MAC)

Mandatory Access Control (MAC) is the strictest of all levels of control. All access to resource objects is strictly controlled by the operating system based on system administrator configured settings. It is not possible under MAC enforcement for users to change the access control of a resource.

Mandatory Access Control begins with security labels assigned to all resource objects on the system. These security labels contain two pieces of information - a classification (top secret, confidential,public etc) and a category (which is essentially an indication of the management level, department etc. to which the object is available).

Similarly, each user account on the system also has classification and category properties from the same set of properties applied to the resource objects.
When a user attempts to access a resource under Mandatory Access Control the operating system checks the user's classification and categories and compares them to the properties of the object's security label.

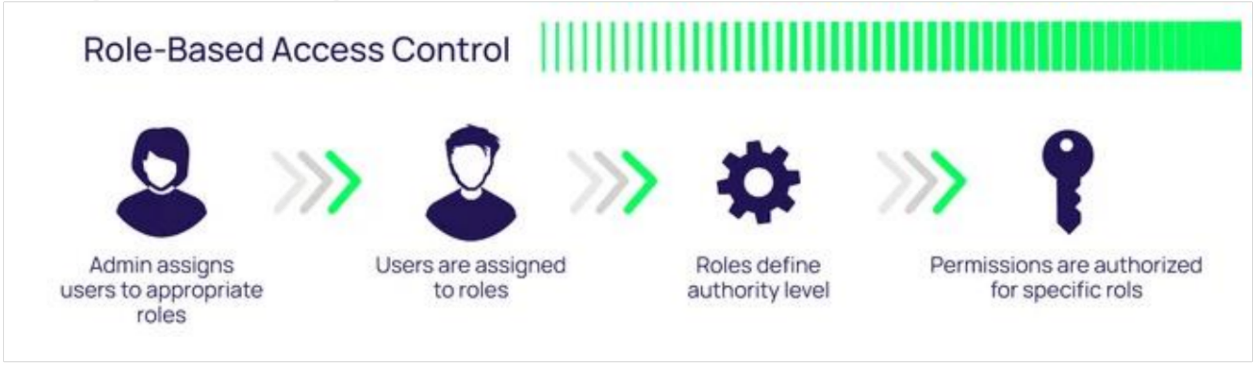
If the user's credentials match the MAC security label properties of the object access is allowed. It is important to note that both the classification and categories must match.
A user with top secret classification, for example, cannot access a resource if they are not also a member of one of the required categories for that object.



## 3. Role Based Access Control(RBAC)

Role Based Access Control assigns permissions to particular roles in an organization. Users are then assigned to that particular role. For example, an accountant in a company will be assigned to the Accountant role, gaining access to all the resources permitted for all accountants on the system. Similarly, a software engineer might be assigned to the developer role.

Roles differ from groups in that while users may belong to multiple groups, a user under RBAC may only be assigned a single role in an organization. Additionally, there is no way to provide individual users additional permissions over and above those available for their role. The accountant described above gets the same permissions as all other accountants, nothing more and nothing less.


Role-Based Access Control
Admin assigns users to appropriate roles
Users are assigned to roles
Roles define authority level
Permissions are authorized for specific rols

## Authorization

- ✓ Authorization is a security mechanism used to determine user/client privilege or access level related to system resources.
- ✓ In multiuser database system, a system administrator defines for the system which users are allowed access to the system and what privilege of use.
- ✓ During authorization system verifies authenticated users access role and either grant or revoke resource access.

Thus ,Authorization includes:

- ✓ Permitting only certain users to access process or alter data.
- ✓ Applying different limitations on user access or actions .Here limitations placed on users can apply to object such as tables, rows etc.

A user may have several form of authorization on parts of database.

- ✓ Authorization to read data
- ✓ Authorization to insert new data
- ✓ Authorization to update data
- ✓ Authorization to delete data

Each of these type of authorization is called privilege. A database user may be assigned all, none, or combination of these types of privileges on specified parts of database such as relation or views. In addition to authorization data, users may be granted database schema, allowing them to create modify or drop relations. The ultimate form of authority is that given to DBA (Database Administrator)DBA may authorize new users, reconstructed the database etc.

## Granting and Revoking of Privileges

- The SQL standard includes the privileges select, insert, update, and delete. The privilege **all privileges** can be used as a short form for all the allowable privileges.
- A user who creates a new relation is given all privileges on that relation automatically.
- The SQL data-definition language includes commands to grant and revoke privileges.

### Grant statement

The grant statement is used to confer authorization.

The basic form of this statement is:

```
grant <privilege list>
on <relation name or view name>
to <user>;
```

The privilege list allows the granting of several privileges in one command

- **select authorization**

- The select authorization on a relation is required to read tuples in the relation.

  The following grant statement grants database users Amit and Satoshi select authorization on the department relation:

  **Example:**
  grant select on department to Amit, Satoshi;

  This allows those users to run queries on the department relation

- **update authorization**

- The update authorization on a relation allows a user to update any tuple in the relation.
- The update authorization may be given either on all attributes of the relation or on only some.
- If update authorization is included in a grant statement, the list of attributes on which update authorization is to be granted optionally appears in parentheses immediately after the update keyword.
- If the list of attributes is omitted, the update privilege will be granted on all attributes of the relation.

  This grant statement gives users Amit and Satoshi update authorization on the budget attribute of the department relation:

  **Example:**
  grant update (budget) on department to Amit, Satoshi;

- ❖ **insert authorization**

The insert authorization on a relation allows a user to insert tuples into the relation. The insert privilege may also specify a list of attributes; any inserts to the relation must specify only these attributes, and the system either gives each of the remaining attributes default values (if a default is defined for the attribute) or sets them to null

**Example:**
grant insert on department to Amit, Satoshi;

grant insert(dept_name,building) on department to Amit, Satoshi;

- ❖ **delete authorization**

The delete authorization on a relation allows a user to delete tuples from a relation

grant delete on department to Ram,Hari;

## Revoke statement

To revoke an authorization use revoke statement.

revoke<privilege list> on <relation or view>  from<user>

**Example:**
revoke select on department from Amit, Satoshi;

revoke update (budget) on department from Amit, Satoshi;

## 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 users.

The most widely used authentication techniques are:

**1) Password based authentication:** A password is a secret word or string of characters used for user authentication to prove identity to a resource, which should be kept secret from those are not allowed access. It is not much reliable than other authentication system because if a weak password is chosen then it can be easily guessed.

### 2) Artifact based authentication

It includes machine-readable batches and electronic cards. These cards consist of magnetic strip, which represents the unique identification number. Card reader may be installed in or near the terminal and users are required to supply artifact for authentication. This form of authentication is common in ATMs in bank. Some companies also provide cards to their employee for authentication.

### 3) Biometric Technique

In this technique, the major groups of authentication mechanism are based on the unique characteristic of each user. This falls into two basic categories.

- **Physiological characteristics:** characteristics such as finger prints, facial characteristics, retina characteristics etc.
- **Behavioral characteristics:** characteristics such as voice pattern, signature pattern etc.

## Security and views

The concept of views is a means of providing a user with a “personalized “model of a database. A view can hide data that user does not need to see. The ability of views to hide data serves both to simplify usage of system and to enhance security.

In SQL, a view is a virtual table based on the result-set of an SQL statement.

- A view contains rows and columns, just like a real table.
- The fields in a view are fields from one or more real tables in the database.
- Through a view, users can query and modify only the data they can see. The rest of the database is neither visible nor accessible.

A view is created with the CREATE VIEW statement.

**Syntax**

```
CREATE VIEW view_name AS

SELECT column1, column2, ...

FROM table_name

WHERE condition;
```

**Benefits of using views**

**Data Security:** Views can be used to enforce data security by limiting the access to sensitive information. By creating views that only expose certain columns or rows, we can control what data users can see and ensure that confidential or restricted information remains hidden.

borrower (customer-name, loan-number)

loan (loan-number, branch-name, amount)

Suppose a bank clerk needs to know the names of the customers of each branch but it is not authorized a specific loan information.

**Approach:** Deny direct access to the loan relation but grant access to the view cust_loan which consists of only the names of customers and the branches at which they have a loan.

The cust_loan view is defined in SQL as follows

```
CREATE VIEW cust_loan AS
SELECT  borrwer.customer_name,loan.branch_name
FROM borrower ,loan
WHERE borrower.loan_numer=loan.loan_number;
```

## How views differs from relation?

| **Relation (table)** | **views** |
|---|---|
| A relation is used to organize data in the form rows and columns and displayed them in structured format. | views are treated as virtual /logical table used to view or manipulate parts of the table. |
| It is a physical entity that means data is actually stored in the relation. | A view is virtual entity which means data is not actually stored in table. |
| It occupies space in the system. | A view does not occupy physical space on the system. |
| It is an independent data object. | It depends on the table(relation) .we cannot create a view without using table. |
| In the table, we can maintain relationships using a primary and foreign key. | The view contains complex multiple tables joins |
| It generates  a fast result. | View generates a slow result because it renders the table every time we query it. |
| **syntax:**<br>CREATE TABLE table_name (<br>column1 datatype,<br>column2 datatype,<br>column3 datatype,<br>....<br>); | **syntax:**<br>CREATE VIEW view_name AS<br>SELECT column_name_1, column_name_2,...<br>FROM table_name<br>WHERE condition; |
| Example:<br>Let us consider the following relation<br>**EMPLOYEE(Emp_No ,Name ,Skill ,Sal_Rate ,Address)**<br><br>Now, it can be created as :<br>**Create table EMPLOYEE**<br>**(Emp_No int PRIMARY KEY,**<br>**Name varchar (30),**<br>**Skill varchar (30),**<br>**Sal_Rate decimal (10, 2),**<br>**Address varchar (30));** | Example:<br>Let us consider the following relation<br>**EMPLOYEE(Emp_No ,Name ,Skill ,Sal_Rate ,Address)**<br><br>For a very personal or confidential matter, every user is not permitted to see the Sal_Rate of an EMPLOYEE.<br>For such users, DBA can create a view, for example, EMP_VIEW defined as:<br>**Create view EMP_VIEW as**<br>**SELECT Emp_No, Name, Skill, Address**<br>**From EMPLOYEE;** |

# Encryption and decryption

## Encryption

Encryption is a process which transforms the original information into an unrecognizable form. This new form of the message is entirely different from the original message. That's why a hacker is not able to read the data as senders use an encryption algorithm. Encryption is usually done using key algorithms.

In database encryption is used to store data in secure way so that even if data is acquired by unauthorized users the data will not be accessible without decryption key.

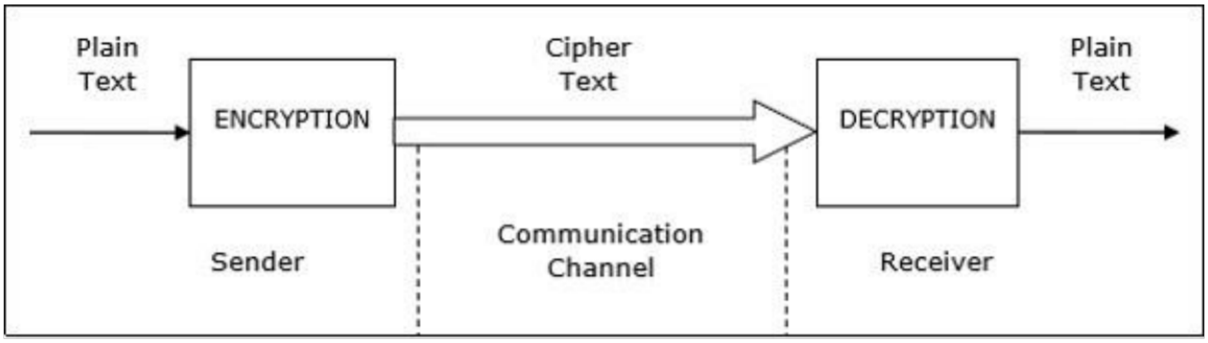
## Decryption

- ✓ Decryption is a process of converting encoded/encrypted data in a form that is readable and understood by a human or a computer.
- ✓ In symmetric key encryption, the encryption key is also used to decrypt.
- ✓ In asymmetric key encryption, two different keys public and private key are used to encrypt and decrypt data.
- ✓ If decryption key is extremely difficult for intruder to determine even if intruder has encrypted data.
- ✓ In asymmetric key encryption, its difficult to infer private key even if public key is available.

# Cryptography

- ✓ Cryptography is the science of encoding information before sending via unreliable communication paths so that only an authorized receiver can decode and use it.
- ✓ The coded message is called cipher text and the original message is called plain text. The process of converting plain text to cipher text by the sender is called encoding or encryption.
- ✓ The process of converting cipher text to plain text by the receiver is called decoding or decryption.

The entire procedure of communicating using cryptography can be illustrated through the following diagram



Modern cryptography concerns with:

- **Confidentiality** - Information cannot be understood by anyone
- **Integrity** - Information cannot be altered.
- **Non-repudiation** - Sender cannot deny his/her intentions in the transmission of the information at a later stage
- **Authentication** - Sender and receiver can confirm each

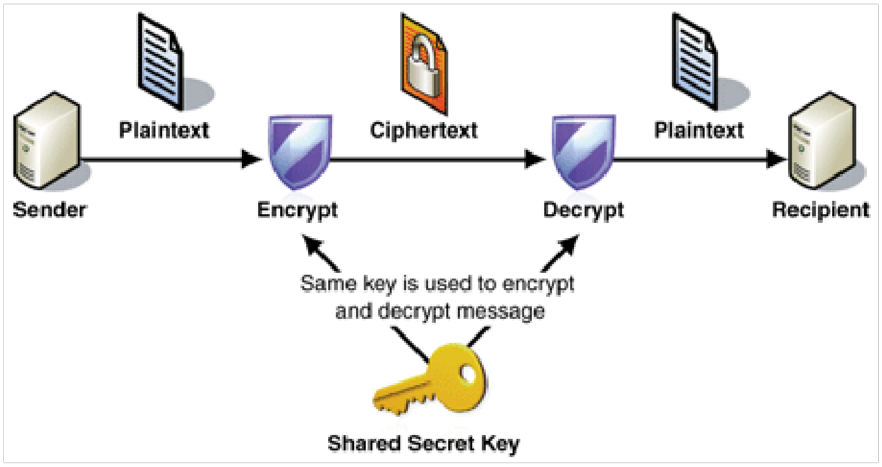
Cryptography is used in many applications like banking transactions cards, computer passwords, and e- commerce transactions.

Three types of cryptographic techniques used in general.

1. Symmetric-key cryptography
2. Asymmetric-key cryptography

## 1. Symmetric-key Cryptography (private key cryptography)

- ✓ Both the sender and receiver share a single key.
- ✓ The sender uses this key to encrypt plaintext and send the cipher text to the receiver.
- ✓ On the other side the receiver applies the same key to decrypt the message and recover the plain text.
  Some of the encryption algorithms that use symmetric key are, Advanced Encryption Standard (AES),Data Encryption Standard (DES) etc.

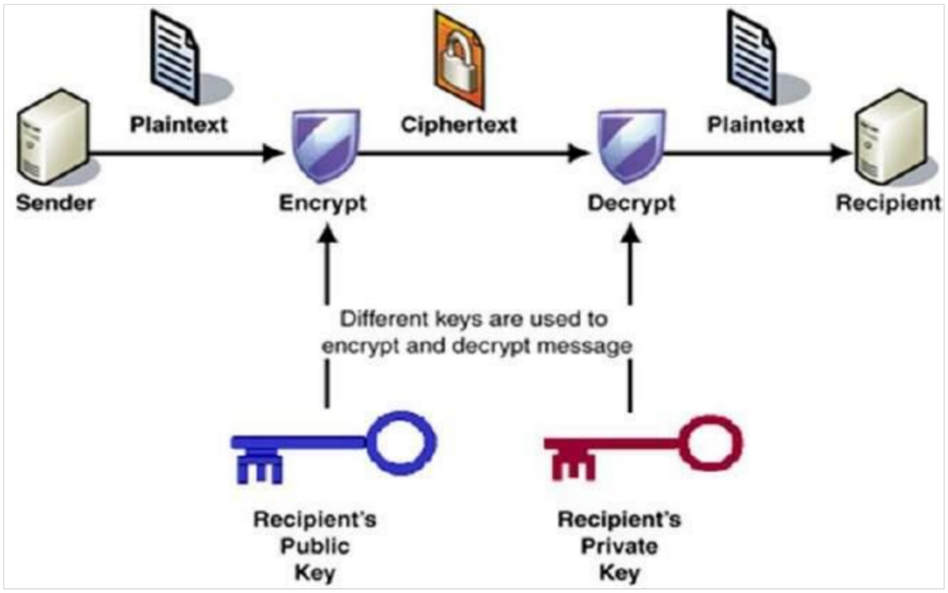


**Disadvantages of symmetric key cryptography**

- ✓ Each pair of users require a unique secret key**.**
- ✓ If N people in the world wants to use this technique, then there needs to be N(N-1) / 2 secret keys.
- ✓ Security is less as only one key is used for both encryption and decryption purpose.

## 2. Asymmetric-key Cryptography (Public-Key Cryptography)

- ✓ In Public-Key Cryptography two related keys (public and private key) are used.
- ✓ Public key may be freely distributed, while its paired private key, remains a secret.
- ✓ The public key is used for encryption and for decryption private key is used.
- ✓ some algorithms for asymmetric –key cryptography are are Diffie-Hellman, El Gamal, DSA and RSA.



The process for the above image is as follows:

Step 1: sender uses recipient's public key to encrypt the message
Step 2: The encrypted message is sent to recipient
Step 3: recipient uses own private key to decrypt the message

## Difference between Symmetric and Asymmetric key Encryption

| **Symmetric key Encryption** | **Asymmetric key Encryption** |
|---|---|
| It only requires a single key for both encryption and decryption. | It requires two keys, a public key and a private key, one to encrypt and the other one to decrypt. |
| The encryption process is very fast. | The encryption process is slow. |
| In symmetric key encryption, resource utilization is low as compared to asymmetric key encryption. | In asymmetric key encryption, resource utilization is high. |
| Security is less as only one key is used for both encryption and decryption purpose. | It is more secure as two keys are used here- one for encryption and the other for decryption |
| The Mathematical Representation is as follows-<br>P = D (K, E(K, P))<br><br>where K –> encryption and decryption key<br>P –> plain text<br>D –> Decryption<br>E(K, P) –> Encryption of plain text using K | The Mathematical Representation is as follows-<br>P = D(Kd, E (Ke,P))<br>where Ke –> encryption key<br><br>Kd –> decryption key<br>D –> Decryption<br>E(Ke, P) –> Encryption of plain text using encryption key Ke. P –> plain text |
| It is used when a large amount of data is required to transfer. | It is used to transfer small amounts of data. |
| Examples: 3DES, AES and DES | Examples: Diffie-Hellman, El Gamal, DSA and RSA |