**Goals of Protection in Operating System**

Various goals of protection in the operating system are as follows:

1. The policies define how processes access the computer system's resources, such as the CPU, memory, software, and even the operating system. It is the responsibility of both the operating system designer and the app programmer. Although, these policies are modified at any time.
2. Protection is a technique for protecting data and processes from harmful or intentional infiltration. It contains protection policies either established by itself, set by management or imposed individually by programmers to ensure that their programs are protected to the greatest extent possible.
3. It also provides a multiprogramming OS with the security that its users expect when sharing common space such as files or directories.

**Protection in OS**

When multiple users access resources of the operating system like CPU, memory, and disk data then securing or protecting data from other processes or external unauthorized access is a critical task. Security mechanisms are to be used to provide better protection for the data. Access to the file system containing user information can be given to a single or group of users. Based on the access privileges given to the user, he/she can use the resources to perform read, write, or execute operations.

In terms of multi-user environments, user groups should predefine the protective measures so that multiple users can access a logical space that shares some files or directories. Protection should be given for common threats that occur in the operating system like viruses, worms, Trojan horses, or any malware activities.

Below are the points listed on the importance of adding protection to the operating system −

* Applying security factors could protect the data, resources, process, or program files from illegal access.
* Access permissions configured to each of the files in the memory of the OS could restrict read, write, and execute access to unauthorized users.
* Allows safe sharing of logical and physical address spaces to access multiple processes of the shared memory by several users.
* Security policies defined by the owner of the system or administrator of the organization provide measures to protect data from harmful attacks.

**Domain of Protection in OS**

The computer system can be viewed as a collection of objects and processes in terms of hardware (printers, disk drives, CPU, memory space) or Software (files, semaphores, etc.) used by OS. These objects and processes are to be protected from illegal access. Access rights are defined as the domain present in each computer system that has two default parameters such as subject or object (whom to grant access) and operation (what operations are allowed) for users.

Consider an example of two domains which has two objects to a file (John: read; Bob: write, execute) this implies John can only read the file whereas Bob can perform write and execute operations. These operations of read, write, and execute can also be shared by the object in different domains and these permissions can be given by the owner of the file. Other file operations include open, close, and delete which are defined during the access permission process.

**Association**

Each process switches from one domain to another based on the permission or access rights specified to it. The association between process and domain can be either in static or dynamic type.

In the static approach, the domain has a fixed set of resources for its lifetime and it cannot be changed instantly when needed whereas in dynamic, processes can switch dynamically from one domain to another or create a new domain ID.

Consider an example of a domain in the Unix Operating system that has a User Id and Group Id which has access rights to perform read, write, and execute operations. So, when processes have the same Uid and Gid will have the same group of objects and permissions. Other scenarios would be switching from the user part to kernel space during a system call.

**Authentication methods**

Authentication is the technique of verifying the user identity compared with the authorized list of users and providing access to the resources of the system. These verification process can be possible in the following ways −

* Providing strong passwords to confidential data or matching with correct username and password combination. One time password option can be configured that sends a random password each time when the user request for accessing the resources.
* These passwords created for authentication purposes can be protected from hackers using an encryption algorithm to encrypt the password that is sent through the network.
* Applying encryption and decryption methods using cryptographic functions where keys are used at the sender side for encryption and the same keys are to be decoded at the other end to gain access to the data, here high-end encryption algorithm has to be used with a maximum number of keys to provide an extra layer of authentication to prevent man in the middle attack.
* Fingerprints, retina scans, multi-factor authentication, using cards, etc. are practical approaches to protect data against illegal access.

## Access Matrix

The Access Matrix is a security model for a computer system's protection state. It is described as a matrix. An access matrix is used to specify the permissions of each process running in the domain for each object. The rows of the matrix represent domains, whereas the columns represent objects. Every matrix cell reflects a set of access rights granted to domain processes, i.e., each entry **(i, j)** describes the set of operations that a domain **Di** process may invoke on object **Oj.**

There are various methods of implementing the access matrix in the operating system. These methods are as follows:

1. **Global Table**
2. **Access Lists for Objects**
3. **Capability Lists for Domains**
4. **Lock-Key Mechanism**

### **Global Table**

It is the most basic access matrix implementation. A set of ordered triples **<domain, object, rights-set>** is maintained in a file. When an operation **M** has been performed on an object Oj within domain Di, the table is searched for a triple **<Di, Oj, Rk>.** The operation can proceed if this triple is located; otherwise, an exception (or error) condition has arrived. This implementation has various drawbacks. The table is generally large and cannot be stored in the main memory, so additional input and output are required.

### **Access Lists for Objects**

Every access matrix column may be used as a single object's access list. It is possible to delete the blank entries. For each object, the resulting list contains ordered pairs **<domain, rights-set>** that define all domains for that object and a nonempty set of access rights.

We may start by checking the default set and then find the access list. If the item is found, we enable the action; if it isn't, we verify the default set. If M is in the default set, we grant access. Access is denied if this is not the case, and an extraordinary scenario arises.

### **Capability Lists for Domains**

A domain's capability list is a collection of objects and the actions that can be done on them. A capacity is a name or address that is used to define an object. If you want to perform operation M on object **Oj,** the process runs operation M, specifying the capability for object **Oj.** The simple possession of the capability implies that access is allowed.

In most cases, capabilities are separated from other data in one of two ways. Every object has a tag to indicate its type as capability data. Alternatively, a program's address space can be divided into two portions. The programs may access one portion, including the program's normal instructions and data. The other portion is a capability list that is only accessed by the operating system.

### **Lock-Key Mechanism**

It is a compromise between the access lists and the capability lists. Each object has a list of locks, which are special bit patterns. On the other hand, each domain has a set of keys that are special bit patterns. A domain-based process could only access an object if a domain has a key that satisfies one of the locks on the object. The process is not allowed to modify its keys.

**OTP: One-time Password**

OTP stands for One Time Password. It is a 4 or 6 digit code which is also known as a one-time pin or dynamic password. It is a type of security password that is valid only for a single-use or transaction and on a single computer, mobile device, etc., which is used for the transaction.

OTP provides an extra layer of security while using your debit cards, credit cards for online transactions such as mobile recharge, online shopping, paying bills, etc. It is sent by your bank to your registered mobile number during the transaction just before the last step.

The code is meant to be used only once and within the given time frame that may be around 3 minutes. If you don't use this code within the given time limits, it will expire, and you have to click the "resend the OTP" option. Furthermore, OTP is generated randomly, so on one can guess it and it becomes invalid after it has been used once, so can't be used again.

It provides more security than static passwords such as login or transaction password, which remains the same for multiple login sessions and transactions. Even if someone has your bank account details, login id, and password, he would not able to use your account as the OTP will come to your mobile and without that, the fraud can't complete the transaction.

There are mainly two types of threats that occur. These are as follows:

### **Program threats**

The operating system's processes and kernel carry out the specified task as directed. Program Threats occur when a user program causes these processes to do malicious operations. The common example of a program threat is that when a program is installed on a computer, it could store and transfer user credentials to a hacker. There are various program threats. Some of them are as follows:

**1.Virus**

A virus may replicate itself on the system. Viruses are extremely dangerous and can modify/delete user files as well as crash computers. A virus is a little piece of code that is implemented on the system program. As the user interacts with the program, the virus becomes embedded in other files and programs, potentially rendering the system inoperable.

**2. Trojan Horse**

This type of application captures user login credentials. It stores them to transfer them to a malicious user who can then log in to the computer and access system resources.

**3. Logic Bomb**

A logic bomb is a situation in which software only misbehaves when particular criteria are met; otherwise, it functions normally.

**4. Trap Door**

A trap door is when a program that is supposed to work as expected has a security weakness in its code that allows it to do illegal actions without the user's knowledge.

### **System Threats**

System threats are described as the misuse of system services and network connections to cause user problems. These threats may be used to trigger the program threats over an entire network, known as program attacks. System threats make an environment in which OS resources and user files may be misused. There are various system threats. Some of them are as follows:

**1. Port Scanning**

It is a method by which the cracker determines the system's vulnerabilities for an attack. It is a fully automated process that includes connecting to a specific port via TCP/IP. To protect the attacker's identity, port scanning attacks are launched through Zombie Systems, which previously independent systems now serve their owners while being utilized for such terrible purposes.

**2. Worm**

The worm is a process that can choke a system's performance by exhausting all system resources. A Worm process makes several clones, each consuming system resources and preventing all other processes from getting essential resources. Worm processes can even bring a network to a halt.

**3. Denial of Service**

Denial of service attacks usually prevents users from legitimately using the system. For example, if a denial-of-service attack is executed against the browser's content settings, a user may be unable to access the internet.

# **Cryptography Definition**

Nowadays, computing systems play a significant role in every aspect of human activity. Every marketing, software, banking, healthcare, and education application uses this computing technology. However, you might be curious about how businesses protect their data and maintain the privacy of their banking activities.

"Cryptography" is the answer to each of these questions. In today's connected world, sensitive information must be protected, which is why cryptography has influenced the current information age.

Additionally, Gmail data is secured using cryptography and is transmitted throughout Google data centers in an encrypted manner. Cryptography is therefore regarded as the essential component for protecting shared information.

## Cryptography

Cryptography uses codes to protect data and communications so only the intended receivers can decode and understand them. Consequently, restricting access to information from outside parties.

"Crypto" indicates "hidden," and "graphy" indicates "writing," respectively. The techniques used in cryptography to secure data are based on mathematical principles and a set of rule-based calculations known as algorithms to modify signals in a way that makes them challenging to decode.

These algorithms generate cryptographic keys, create digital signatures, safeguard data privacy, enable online browsing on the Internet, and ensure the confidentiality of private transactions like credit and debit card payments.

Currently used cryptography techniques can potentially be irreversible, ensuring the message's security forever. The requirement for data to be safeguarded more securely than ever before has led to the development of more complex cryptography methods. Most early cryptographic ciphers and algorithms have been cracked, making them ineffective for data security.

It would sometimes take years or even decades to figure out the meaning of a single message, even though it is possible to interpret today's algorithms. Thus, the competition to develop newer and more powerful cryptographic techniques continues.

## What is The Purpose of Cryptography?

Cryptography aims to keep data and messages private and inaccessible to possible threats or bad actors. It frequently works invisibly to encrypt and decrypt the data you send through email, social media, applications, and website interactions.

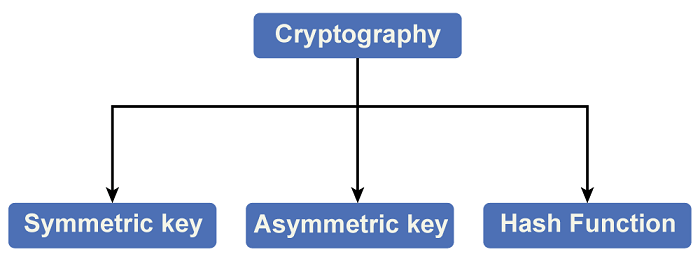
There are several uses for symmetric cryptography, including:

* Payment applications and card transactions
* Random number generation
* Verify the sender's signature to be sure they are who they claim they are

There are several uses for asymmetric cryptography, including:

* Email messages
* SIM card authentication
* Web security
* Exchange of private keys

## Types of Cryptography



There are three main types of cryptography:

**Symmetric key Cryptography:**With the encryption technique, the sender and the recipient use the same shared key to encrypt and decrypt messages.Although symmetric key systems are quicker and easier to use, they have the drawback of requiring a secure key exchange between the sender and the receiver. Data Encryption System (DES) is the most widely used symmetric key encryption method.

**Hash Functions:** In this algorithm, no key is used. The plain text is used to produce a hash value that has a fixed length, making it challenging to retrieve the plain text's information. Hash functions are widely used by operating systems to encrypt passwords.

**Asymmetric Key Cryptography:**This approach uses a set of keys to encrypt and decrypt data. Public keys are used for encryption, whereas private keys are used for decryption.

The Public Key and Private Key are different from one another. Even if everyone knows the public key, only the intended recipient may decode the message since only he can access the private key.

In the age of computers, cryptography is frequently associated with converting plain text into cipher text, which is text that the intended recipient can only decode. This process is known as encryption. The process of converting encrypted text into plain text is called decryption.

## Features of Cryptography

Cryptography has the following features:

* **Confidentiality:** The only person who can access information is the one it is intended for, which is the primary feature of cryptography.
* **Integrity:** Information cannot be altered while it is being stored or sent from the sender to the intended destination without the recipient spotting the addition of new information in Cryptography.
* **Non-repudiation:**The creator/sender of a message cannot deny his intent to send information at a future point.
* **Authentication:**The identities of the sender and the recipient have been confirmed. Furthermore, the information's source and final destination are confirmed.
* **Availability:**It also ensures that the required information is available to authorized users at the appropriate time.
* **Key Management:** The creation, distribution, storage, and alteration of cryptographic keys take place in this process.
* **Algorithm:** Mathematical formulae are used in cryptography to encrypt and decrypt messages.
* **Digital Signatures:**A signature that can be applied to messages to protect the message's authenticity and sender identification.

## Encryption and Decryption

Cryptography involves two phases at its most fundamental level: **Encryption and Decryption**.

Encryption uses a cipher to encrypt and transform the plaintext into ciphertext. On the other hand, decryption transforms the ciphertext into plaintext by employing the same cipher.