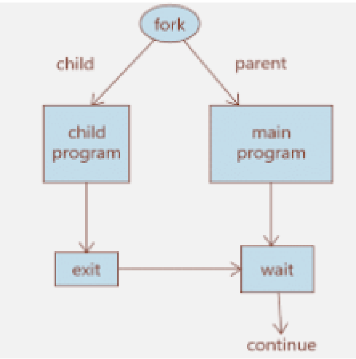
- ## What is Fork system call?

Fork system call is used for creating a new process, which is called ***child process***, which runs concurrently with the process that makes the fork() call (parent process). After a new child process is created, both processes will execute the next instruction following the fork() system call. A child process uses the same pc(program counter), same CPU registers, same open files which use in the parent proces.

```
   #include <stdio.h>
#include <sys/types.h>
#include <unistd.h>
int main()
{

    // make two process which run same
    // program after this instruction
    fork();

    printf("Hello world!\n");
    return 0;
   }
```



What is a semaphore?

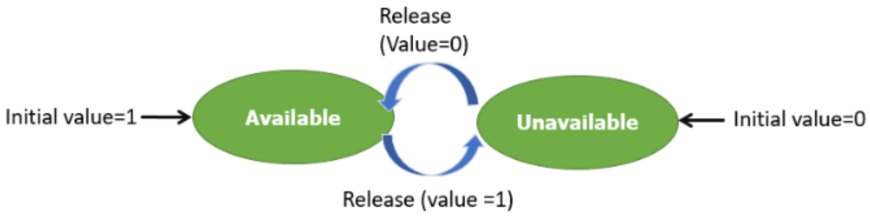
Semaphore was proposed by Dijkstra in 1965 which is a very significant technique to manage concurrent processes by using a simple integer value, which is known as a semaphore. A semaphore is simply an integer variable that is shared between threads. This variable is used to solve the critical section problem and to achieve process synchronization in the multiprocessing environment.
Semaphores are of two types:

1st**Binary Semaphore –**

This is also known as mutex lock. It can have only two values – 0 and 1. Its value is initialized to 1. It is used to implement the solution of critical section problems with multiple processes.

2nd**Counting Semaphore –**

Its value can range over an unrestricted domain. It is used to control access to a resource that has multiple instances.



Distinguish between hacker and cracker

Parameters	**Hackers**	**Crackers**
Definition	Hackers are good people who hack devices and systems with good intentions. They might hack a system for a specified purpose or for obtaining more knowledge out of it.	Crackers are people who hack a system by breaking into it and violating it with some bad intentions. They may hack a system remotely for stealing the contained data or for harming it permanently.
Skills and Knowledge	They have advanced knowledge of programming languages and computer OS. Hackers are very skilled and intelligent people.	These people may be skilled. But most of the time, they don’t even need extensive skills. Some crackers only have a knowledge of a few illegal tricks that help them in stealing data.

Role in an Organization	Hackers work with specific organizations to help them in protecting their information and important data. They mainly provide organizations with expertise in security and internet safety.	Crackers harm an organization. These are the people from whom hackers defend sensitive data and protect the organizations as a whole.
Ethics	These are ethical types of professionals.	These are illegal and unethical types of people who only focus on benefiting themselves with their hacking.
Data Security	They protect the data and never steal or damage it. Their only intention is to gain knowledge from the concerned data and information.	They usually steal, delete, corrupt, or compromise the data they find from a system's loopholes. Your data stays vulnerable in the hands of a cracker.
Use of Tools	Hackers use their own legal tools for checking network strength, establishing security, and protecting an organization from internet threats.	Crackers don't have any tools of their own. They make use of someone else's tools for performing illegal activities and harming/ compromising a system.
Network Strength	They help improve a network's strength.	They harm and deplete a network's strength.

What is cypher text?

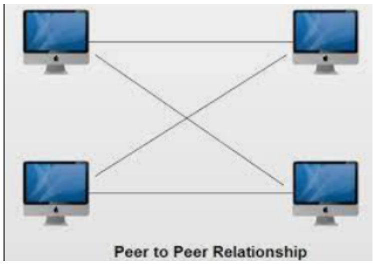
Ciphertext is encrypted text transformed from plaintext using an encryption algorithm. Ciphertext can't be read until it has been converted into plaintext (decrypted) with a key. The decryption cipher is an algorithm that transforms the ciphertext back into plaintext.

Substitution ciphers. Replace bits, characters, or character blocks in plaintext with alternate bits, characters or character blocks to produce ciphertext. A substitution cipher may be monoalphabetic or polyalphabetic:

- **Permutation ciphers.** In this cipher, the positions held by plaintext are shifted to a regular system so that the ciphertext constitutes a permutation of the plaintext.
- **Polygraphic ciphers.** Substituting one letter for another letter, a polygraphic cipher performs substitutions with two or more groups of letters. This masks the frequency distribution of letters, making frequency analysis attacks much more difficult.

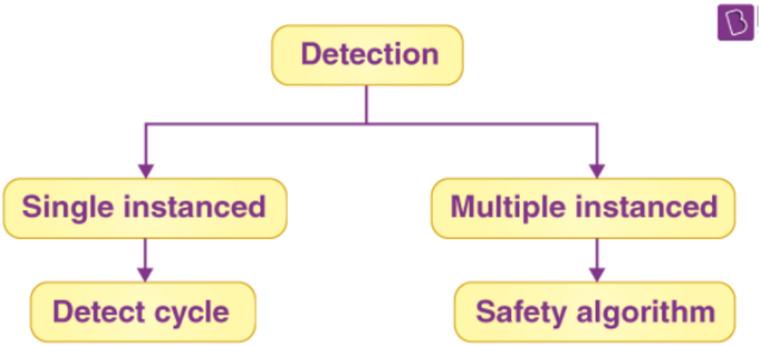
What is a peer to peer network?

A peer-to-peer network is a simple network of computers. It first came into existence in the late 1970s. Here each computer acts as a node for file sharing within the formed network. Here each node acts as a server and thus there is no central server in the network. This allows the sharing of a huge amount of data. The tasks are equally divided amongst the nodes. Each node connected in the network shares an equal workload. For the network to stop working, all the nodes need to individually stop working. This is because each node works independently.



When does the deadlock occur? Explain deadlock detection and recovery detail.

A deadlock is **a situation in which two computer programs sharing the same resource are effectively preventing each other from accessing the resource, resulting in both programs ceasing to function**. The earliest computer operating systems ran only one program at a time.



If a cycle forms in a system with single instanced resource types, there will undoubtedly be a deadlock. Detecting a cycle, on the other hand, is insufficient in a graph of the multiple instanced resource type. By turning the resource allocation graph into the allocation matrix as well as the request matrix, we must apply the safety algorithm to the system.

Deadlock Recovery :
A traditional operating system such as Windows doesn't deal with deadlock recovery as it is a time and space-consuming process. Real-time operating systems use Deadlock recovery.

1st**Killing the process –**

Killing all the processes involved in the deadlock. Killing process one by one. After killing each process check for deadlock again keep repeating the process till the system recovers from deadlock. Killing all the processes one by one helps a system to break circular wait condition.

2nd**Resource Preemption –**

Resources are preempted from the processes involved in the deadlock, preempted resources are allocated to other processes so that there is a possibility of recovering the system from deadlock. In this case, the system goes into starvation.

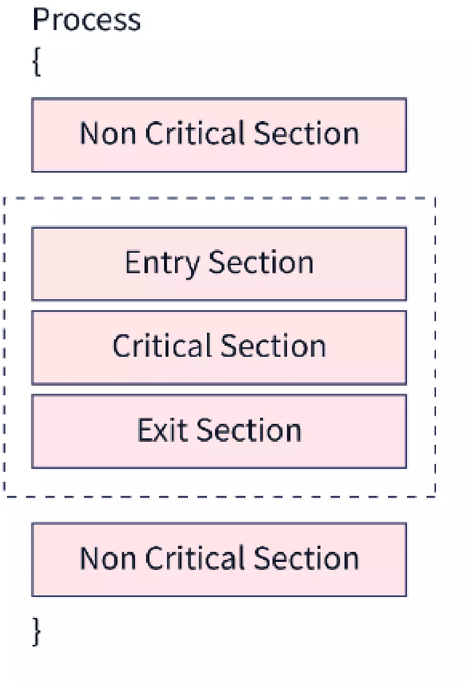
- What is critical section problem? Explain any one problem with solution.

Critical Section refers to the segment of code or the program which tries to access or modify the value of the variables in a shared resource.

The section above the critical section is called the **Entry Section**. The process that is entering the critical section must pass the entry section.

The section below the critical section is called the **Exit Section**.

The section below the exit section is called the **Reminder Section** and this section has the remaining code that is left after execution.



The **critical section problem** is to make sure that only one process should be in a critical section at a time. When a process is in the critical section, no other processes are allowed to enter the critical section. This solves the race condition.

Example of Critical Section Problem

Suppose P1 is a process and the Critical Section is assigned to the P1. Now, if P2 is requesting to enter into the critical section to perform some task, then P2 needs to be a wait because P1 is already using the critical section. When P1 leaves the Critical Section, then the Operating System can assign the Critical Section to the process P2.

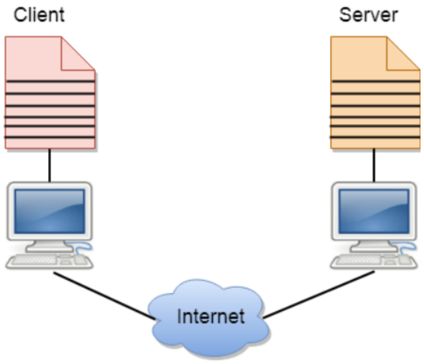
Pseudocode of Critical Section Problem

```
do
{
Entry in the Critical Section
    Critical Section
Exit from the Critical Section
    Remainder Section
}
while(True);
```

- Explain with the help of diagram functionality of client server network.

  A client-server network is the medium through which clients access resources and services from a central computer, via either a local area network (LAN) or a wide-area network (WAN), such as the Internet. A unique server called a daemon may be employed for the sole purpose of awaiting client requests, at which point the network connection is initiated until the client request has been fulfilled.

Network traffic is categorized as client-to-server (north-south traffic) or server-to-server (east-west traffic). Popular network services include e-mail, file sharing, printing, and the World Wide Web.



Benefits of Client-Server Computing

There are numerous advantages of the client server architecture model:

- A single server hosting all the required data in a single place facilitates easy protection of data and management of user authorization and authentication.
- Resources such as network segments, servers, and computers can be added to a client-server network without any significant interruptions.
- Data can be accessed efficiently without requiring clients and the server to be in close proximity.
- All nodes in the client-server system are independent, requesting data only from the server, which facilitates easy upgrades, replacements, and relocation of the nodes.
- Data that is transferred through client-server protocols are platform-agnostic.

Elaborate the concept of system threat with the help of example.

System threats refers to misuse of system services and network connections to put user in trouble. System threats can be used to launch program threats on a complete network called as program attack. System threats creates such an environment that operating system resources/ user files are misused. Following is the list of some well-known system threats.

-
- **Worm** − Worm is a process which can choked down a system performance by using system resources to extreme levels. A Worm process generates its multiple copies where each copy

uses system resources, prevents all other processes to get required resources. Worms processes can even shut down an entire network.

- **Port Scanning** − Port scanning is a mechanism or means by which a hacker can detects system vulnerabilities to make an attack on the system.
- **Denial of Service** − Denial of service attacks normally prevents user to make legitimate use of the system. For example, a user may not be able to use internet if denial of service attacks browser's content settings.

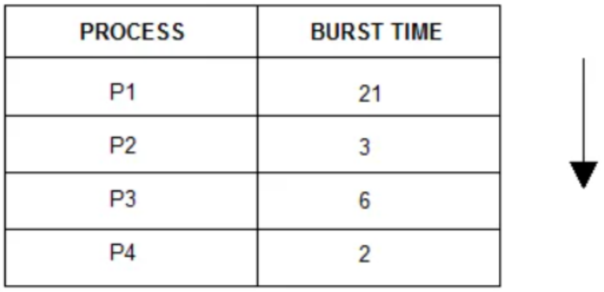
Which of the following scheduling algorithms could result in starvation? Explain in detail?

a. First-come, first-served
b. Shortest job first
c. Round robin
d. Priority

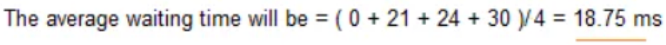
Types of Process Scheduling Algorithms

The different types of process scheduling algorithms are as follows −

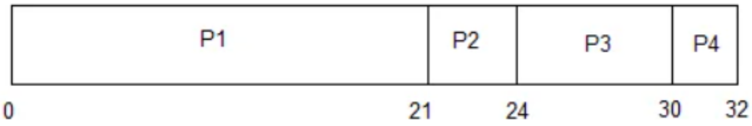
FCFS As the name goes, jobs are executed on a **first come first serve basis. It's a simple algorithm based on FIFO that's first in first out. It is pre-emptive and non pre-emptive and its performance is poor based on its average waiting time.**



PROCESS	BURST TIME
P1	21
P2	3
P3	6
P4	2

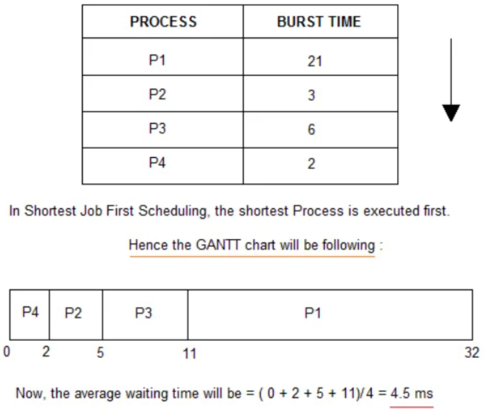


The average waiting time will be = (0 + 21 + 24 + 30)/4 = 18.75 ms



SJF

It is also known as the **shortest job first or shortest job next. It is a pre-emptive and non pre-emptive type algorithm that is easy to implement in batch systems and is best in minimising the waiting time**



PROCESS	BURST TIME
P1	21
P2	3
P3	6
P4	2

In Shortest Job First Scheduling, the shortest Process is executed first.

Hence the GANTT chart will be following :

P4	P2	P3	P1

0 2 5 11 32

Now, the average waiting time will be = (0 + 2 + 5 + 11)/4 = 4.5 ms

Round Robin It is pre-emptive scheduling algorithm in which each process is given a fix time called quantum to execute. In this time one process is allowed to execute for a quantum and then pre-empts and then other process is executed. In this way there is context switching between processes to save states of these pre-empted processes.

Priority Scheduling

It is a non pre-emptive Algorithm that works in batch systems and in this each process is given a priority and the process with highest priority is executed first and others are executed according to priorities which can lead to starvation for those processes.

Algorithms leading to Starvation

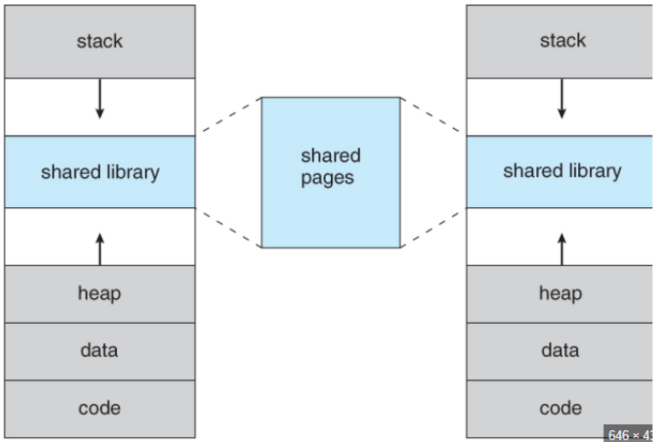
Now in SJF, if longer processes come, then they have to wait for longer times and hence this suffers from starvation. In round robin, there is no chance of starvation as each process is given quanta for execution or fixed time to execute.

In priority scheduling the longer processes with low priority keep in waiting and hence priority scheduling undergoes starvation as only high priority processes execute fast and low ones remain waiting.

In FCFS there is no chance of starvation in both the cases of longer or shorter processes. Eventually, every process gets to execute without waiting on a first come first serve basis.

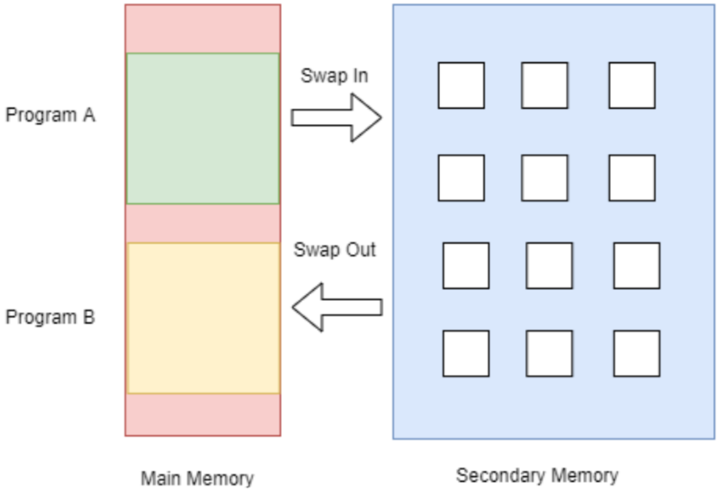
Explain the concept of virtual memory along with demand paging.

Virtual Memory is a storage mechanism which offers user an illusion of having a very big main memory. It is done by treating a part of secondary memory as the main memory. In Virtual memory, the user can store processes with a bigger size than the available main memory. Therefore, instead of loading one long process in the main memory, the OS loads the various parts of more than one process in the main memory.



The demand paging system is similar to the swapping paging system in that processes are mostly stored in the main memory (usually on the hard disk). As a result, demand paging is a procedure that addresses the problem above just by shifting pages on demand. Lazy swapper is another name for this (It never swaps the page into the memory unless it is needed).

A pager is a kind of swapper that deals with the individual pages of a process.
Demand Paging is a method in which a page is only brought into main memory when the CPU requests it. At first, just those pages are loaded directly required by the operation. Pages that are never accessed are thus never loaded into physical memory.



Advantages of Demand Paging

Here are the following advantages of demand paging in the operating system, such as:

- It increases the degree of multiprogramming as many processes can be present in the main memory simultaneously.
- There is a more efficient use of memory as processes having a size more than the size of the main memory can also be executed using this mechanism because we are not loading the whole page at a time.
- We have to the right for scaling of ***virtual memory***.
- If any program is larger than physical memory, it helps run this program without compaction.
- Partition management is simpler.
- It is more useful in ***a time-sharing system***.
- It has no limitations on the level of ***multi-programming***.
- Discards external fragmentation.
- Easy to swap all pages.

Explain DDOs? Explain the difference between DDOS and DOS attack.

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.
DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices.

How does a DDoS attack work?

These networks consist of computers and other devices (such as IoT devices)which have been infected with malware, allowing them to be controlled remotely by an attacker. These individual devices are referred to as bots (or zombies), and a group of bots is called a botnet. Once a botnet has been established, the attacker is able to direct an attack by sending remote instructions to each bot.

How to identify a DDoS attack

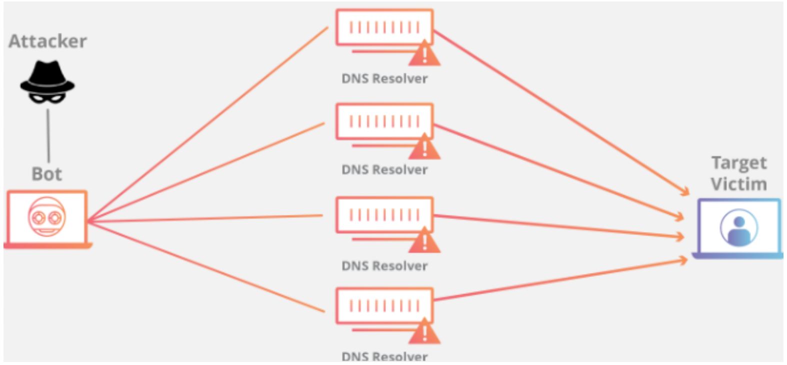
The most obvious symptom of a DDoS attack is a site or service suddenly becoming slow or unavailable. But since a number of causes — such a legitimate spike in traffic — can create similar performance issues, further investigation is usually required. Traffic analytics tools can help you spot some of these telltale signs of a DDoS attack:

- Suspicious amounts of traffic originating from a single IP address or IP range

- A flood of traffic from users who share a single behavioral profile, such as device type, geolocation, or web browser version

- An unexplained surge in requests to a single page or endpoint

- Odd traffic patterns such as spikes at odd hours of the day or patterns that appear to be unnatural (e.g. a spike every 10 minutes)



DOS	DDOS
DOS Stands for Denial of service attack.	DDOS Stands for Distributed Denial of service attack.
In Dos attack single system targets the victim system.	In DDoS multiple systems attacks the victims system..
Victim PC is loaded from the packet of data sent from a single location.	Victim PC is loaded from the packet of data sent from Multiple location.
Dos attack is slower as compared to DDoS.	DDoS attack is faster than Dos Attack.
Can be blocked easily as only one system is used.	It is difficult to block this attack as multiple devices are sending packets and attacking from multiple locations.
In DOS Attack only single device is used with DOS Attack tools.	In DDoS attack,The volumeBots are used to attack at the same time.
DOS Attacks are Easy to trace.	DDOS Attacks are Difficult to trace