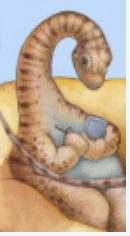
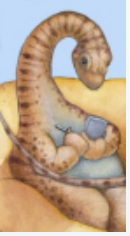
Chapter 16: Security



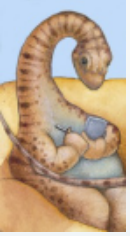
Chapter 15: Security

- The Security Problem
- Authentication
- Program Threats
- System Threats
- Securing Systems
- Intrusion Detection
- Encryption
- Windows NT



PROTECTION & SECURITY

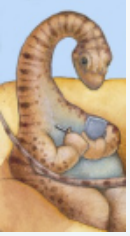
- **Are implemented to prevent *interference* with the use of files.**
- **Threats:- Protection & Security**
- **Protection**: is strictly **internal** problem. How do we provide **controlled access** to the programs and data stored in computer system.
- **Security:** on the other hand, deals with the **external threats**.
- includes firewalls, encryption techniques.
- We say our system is secure if its resources are used and accessed as intended under all circumstances.
- Computer resources must be guarded against unauthorized access, malicious destruction or alteration.
- Total security can never be achieved.



The Security Problem

- Security must consider external environment of the system, and protect it from:
  - unauthorized access.
  - malicious modification or destruction
  - Data unavailability.

- Security violation can be categorized as intentional or accidental.
- Easier to protect against accidental than intentional misuse.



Some common Terms

1. Threat: is the potential to security violation.
2. Attack: attempt to break security.

3. Hacker:

- A person with a strong interest in computers who enjoys learning and experimenting with them.

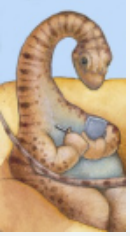
- Cracker/Intruder:

  Someone who breaks into computers.

  Crackers should not be confused with hackers.

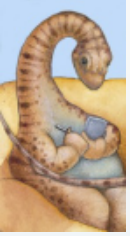
  The term cracker is usually connected to computer criminals.

  Some of their crimes include ID theft and session hijacking and intrusion in unauthorized areas.



Some security violations:

- Breach of **confidentiality**: Unauthorized reading of data. Theft of information
- Breach of **integrity**: Unauthorized modification of data.
- Breach of **availability**: Unauthorized destruction of data/ website defacement: A **website defacement** is an attack on a website that changes the visual appearance of the site or a webpage. These are typically the work of system crackers, who break into a web server and replace the hosted website with one of their own. SQL injections.
- Theft of service: unauthorized use of resources.
- **Denial of service**: Send invalid data to applications or network services, which cause abnormal termination or behavior of the applications or services.
- Flood a computer or the entire network with traffic until a shutdown occurs because of the overload.

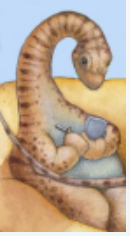


- Attackers use several standard methods in their attempts to breach security:

Masquerading: pretend to be someone else.

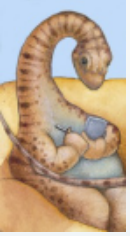
Replay attack: repeat of valid data transmission

Man in the middle attack: attacker sits in the data flow of communication. Masquerading as the sender to the receiver and vice versa.



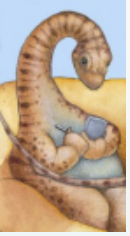
To protect our system, we must take **security measures at 4 levels**:

- Physical (site containing computer system must be physically secured).
- Human(using authorization/authentication mechanisms)
- Operating system(using firewalls)
- Network(using encryption-decryption techniques)(RSA, DES(DATA ENCRYPTION STANDARD,AES(ADVANCE ENCRYPTION STANDARD,MESSAGE DIGEST 5)



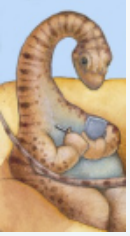
Authentication

- User identity most often established through *passwords.*
- Passwords must be kept secret.
  - Frequent change of passwords.
  - Use of “non-guessable” passwords.
  - Log all invalid access attempts.
- Passwords may also either be encrypted or allowed to be used only once.



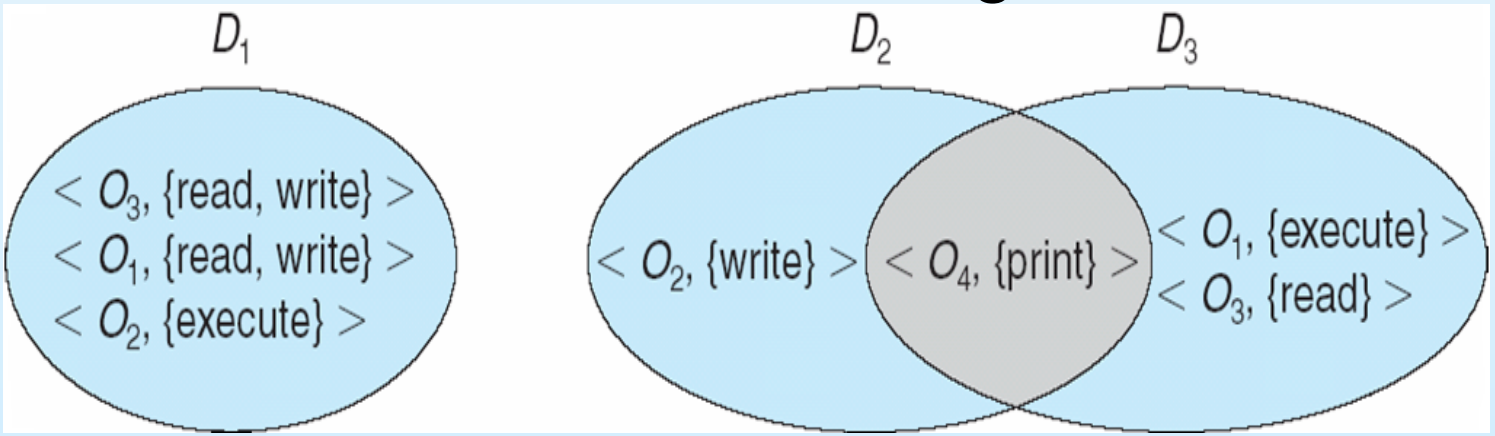
ACCESS MATRIX

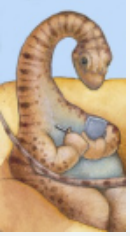
- **Access Matrix** is used to specify the resources a process may access.
- Protection Domain-Domain can be user, process, procedure



Domain Structure

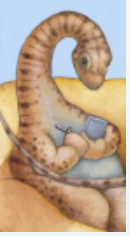
- Access-right = <*object-name*, *rights-set*> where *rights-set* is a subset of all valid operations that can be performed on the object
- Domain = set of access-rights





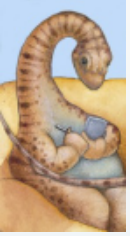
Access Matrix

- Used for the implementation of Protection Model.
- Rows represent domains
- Columns represent objects
- *Access(i, j)* is the set of operations that a process executing in $Domain_i$ can invoke on $Object_j$



Access Matrix

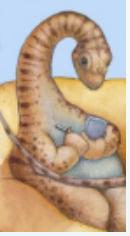
object / domain	F_1	F_2	F_3	printer
D_1	read		read	
D_2				print
D_3		read	execute	
D_4	read write		read write	



Types of Threats

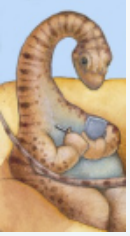
Program Threats

- When any prog.created by a user is used by another user then misuse of that prog.may occur.Examples:-Trojan Horses,Trap doors, stack buffer overflow.
- **Malware(malicious software):** software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system Types of malware can include computer viruses, worms, Trojan horses and spyware.
- **A back door** is a means of access to a computer program that bypasses security mechanisms. A programmer may sometimes install a back door so that the program can be accessed for troubleshooting or other purposes. However, attackers often use back doors that they detect or install themselves, as part of an exploit. In some cases, a worm is designed to take advantage of a back door created by an earlier attack.



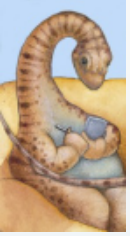
Trojan horse

- A **Trojan horse**, or **Trojan**, is software that appears to perform a desirable function for the user, but (perhaps in addition to the expected function) steals information or harms the system.
- It is a program that sit ideally and transmits all user information to the attacker.
- It is attached to your browser and when user fills his username or password for any website, it records everything and passes to attacker.

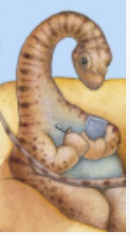


Spyware

- **Spyware** is a type of malware that can be installed on computers, and which collects small pieces of information about users without their knowledge.
- The presence of spyware is typically hidden from the user, and can be difficult to detect.
- Sometimes, however, spywares such as key loggers are installed by the owner of a shared, corporate, or public computer on purpose in order to secretly monitor other users.
- While the term *spyware* suggests software that secretly monitors the user's computing. Spyware programs can collect various types of personal information, such as Internet surfing habits and sites that have been visited, but can also interfere with user control of the computer in other ways, such as installing additional software and redirecting Web browser activity.
- Spyware is known to change computer settings, resulting in slow connection speeds, different home pages, and/or loss of Internet connection or functionality of other programs.

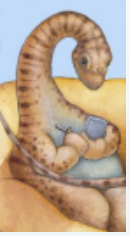


- In computer security, a **covert channel** is a type of computer security attack that creates a capability to transfer information objects between processes that are not supposed to be allowed to communicate by the computer security policy.
- A **logic bomb** is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files (such as a salary database trigger).



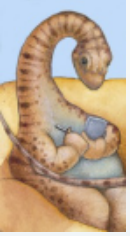
System Threats-OS files/resources are misused

- **VIRUS**: Vital Information Resource Under Seize or Very Important Resource Under Seize ..both are correct.
- Small progs. Written to alter the way a computer operates.
- designed to “infect” other programs.
- Executes without user permission.
- Can replicate itself.
- Once a virus reaches a target machine, a program known as virus dropper inserts virus onto system..



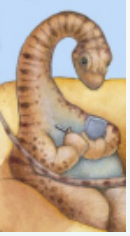
Worms

- Small programs that do -Self propagating or self duplicating.
- Contains malicious code that cause major damage to OS files.
- If a device gets infected, it sends the copies of itself onto the network to other devices.
- Sometimes more dangerous, it might go into your email, find your contacts, sends copies of itself to all the contacts.



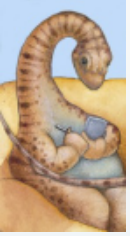
Threat Monitoring

- Check for suspicious patterns of activity – i.e., several incorrect password attempts may signal password guessing.
- Audit log – records the time, user, and type of all accesses to an object; useful for recovery from a violation and developing better security measures.
- Scan the system periodically for security holes; done when the computer is relatively unused.



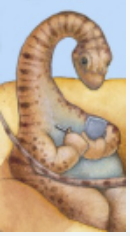
Threat Monitoring (Cont.)

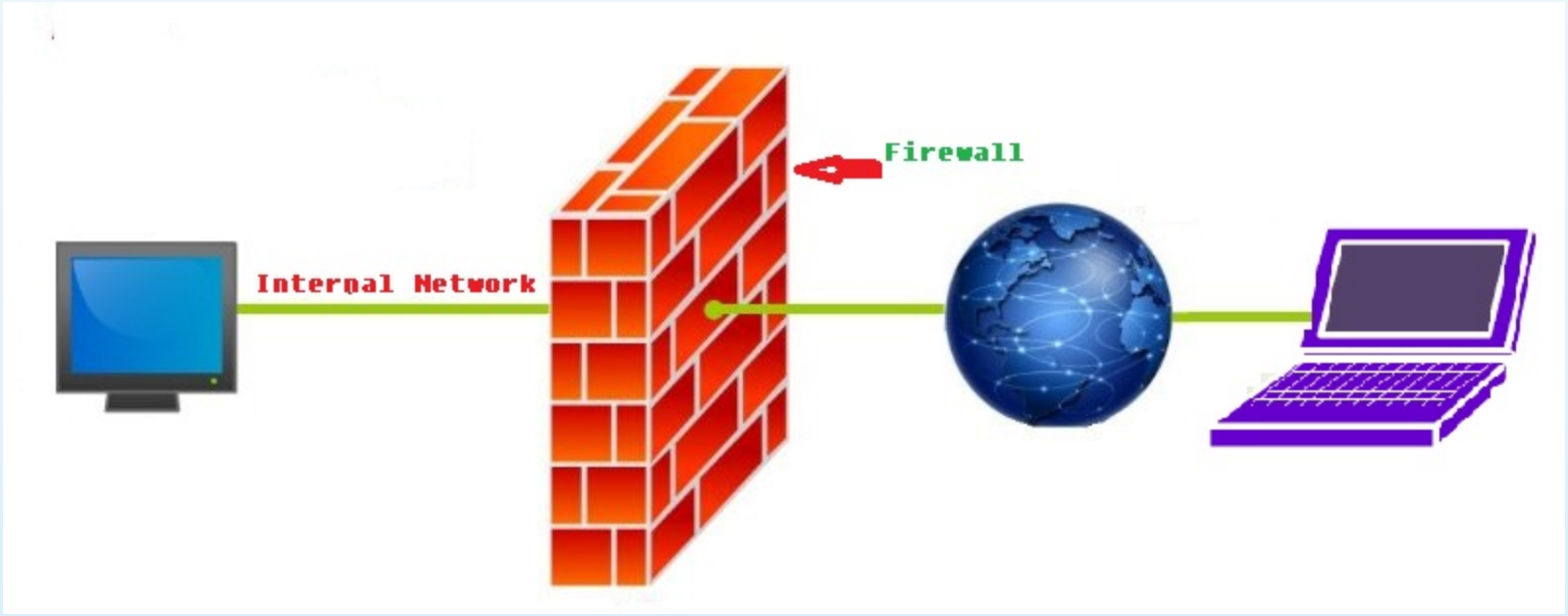
- Check for:
  - Short or easy-to-guess passwords
  - Unauthorized set-uid programs
  - Unauthorized programs in system directories
  - Unexpected long-running processes
  - Improper directory protections
  - Improper protections on system data files
  - Changes to system programs: monitor checksum values

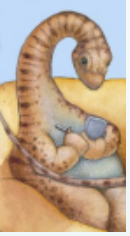


FireWall

- A **firewall** is a device or set of devices designed to permit or deny network transmissions based upon a set of rules and is frequently used to protect networks from unauthorized access while permitting legitimate communications to pass.
- A firewall is placed between trusted and untrusted hosts.
- The firewall limits network access between these two security domains.

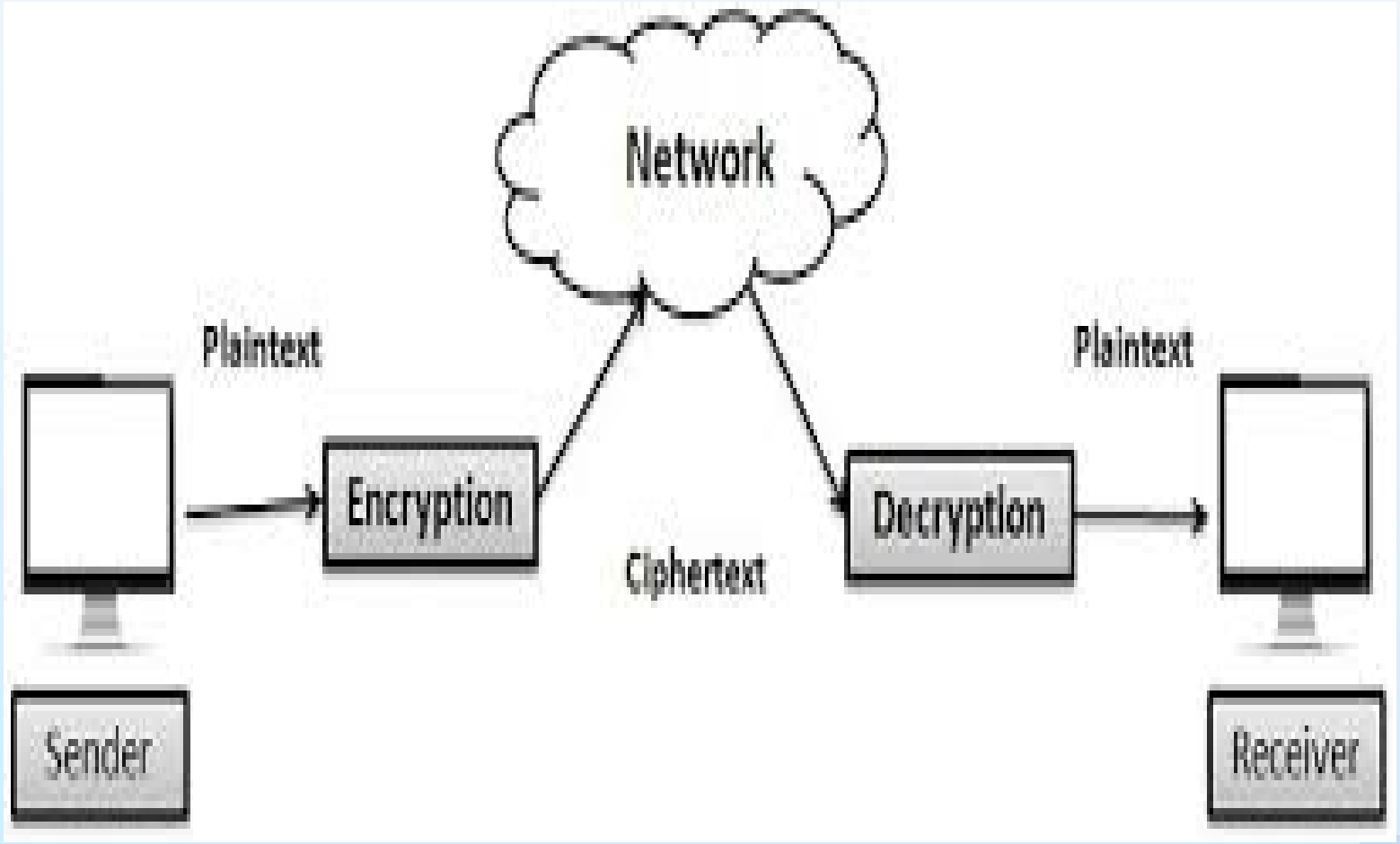


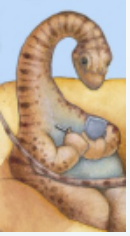

Firewall
Internal Network



Encryption

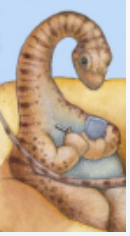
- Encrypt clear text into cipher text.
- Substitution and transposition ciphers
- Properties of good encryption technique:
  - Relatively simple for authorized users to encrypt and decrypt data.
  - Encryption scheme depends not on the secrecy of the algorithm but on a parameter of the algorithm called the encryption key.
  - Extremely difficult for an intruder to determine the encryption key.
- *Data Encryption Standard* substitutes characters and rearranges their order on the basis of an encryption key provided to authorized users via a secure mechanism. Scheme only as secure as the mechanism.


Network
Plaintext
Plaintext
Encryption
Decryption
Ciphertext
Sender
Receiver



Encryption (Cont.)

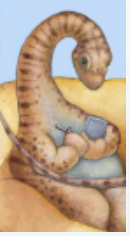
- **Public-key cryptography** refers to a cryptographic system requiring two separate keys, one to lock or encrypt the plaintext, and one to unlock or decrypt the cyphertext.
- Neither key will do both functions.
- One of these keys is published or public and the other is kept private.
- Public key cryptography was invented in 1976 by Whitfield Diffie and Martin Hellman. For this reason, it is sometime called *Diffie-Hellman encryption.*
- It is also called *asymmetric encryption* because it uses two keys instead of one key (*symmetric encryption*).



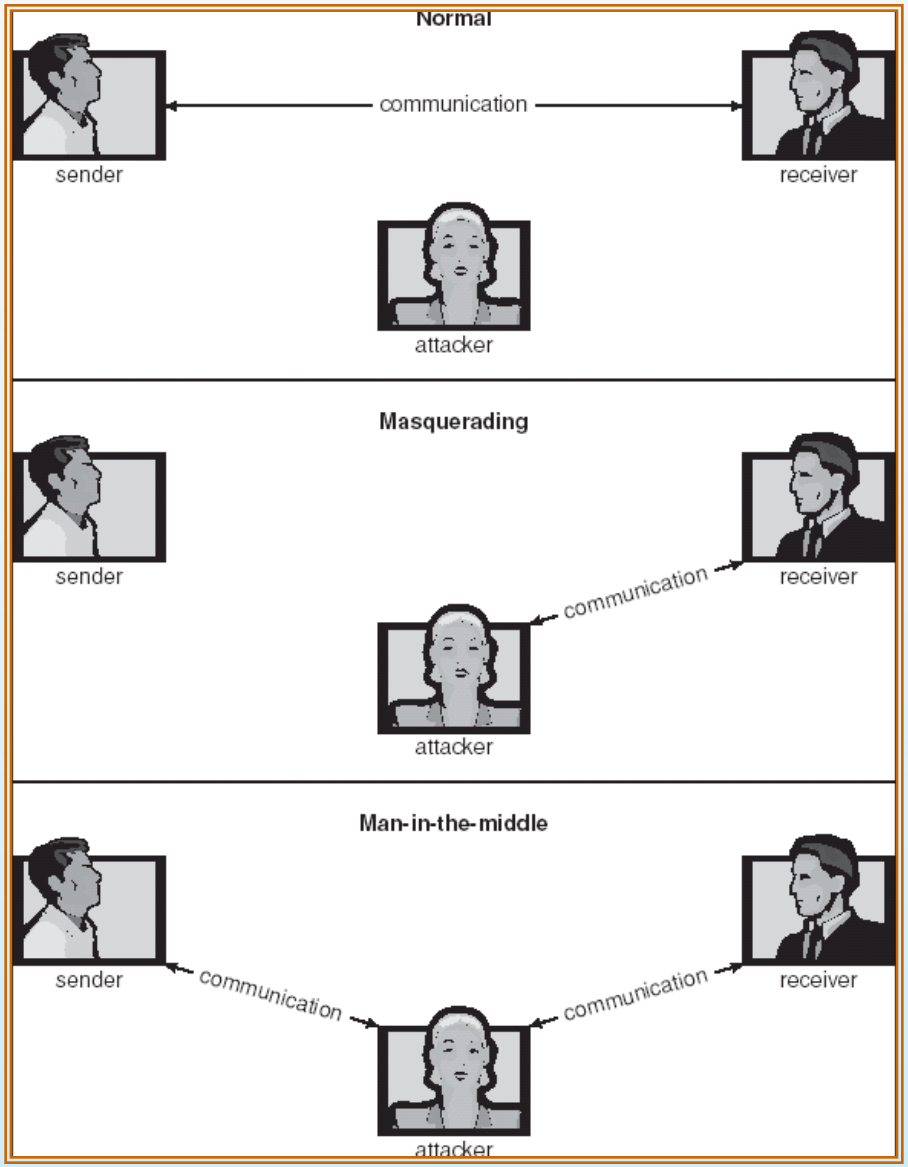
Private key encryption

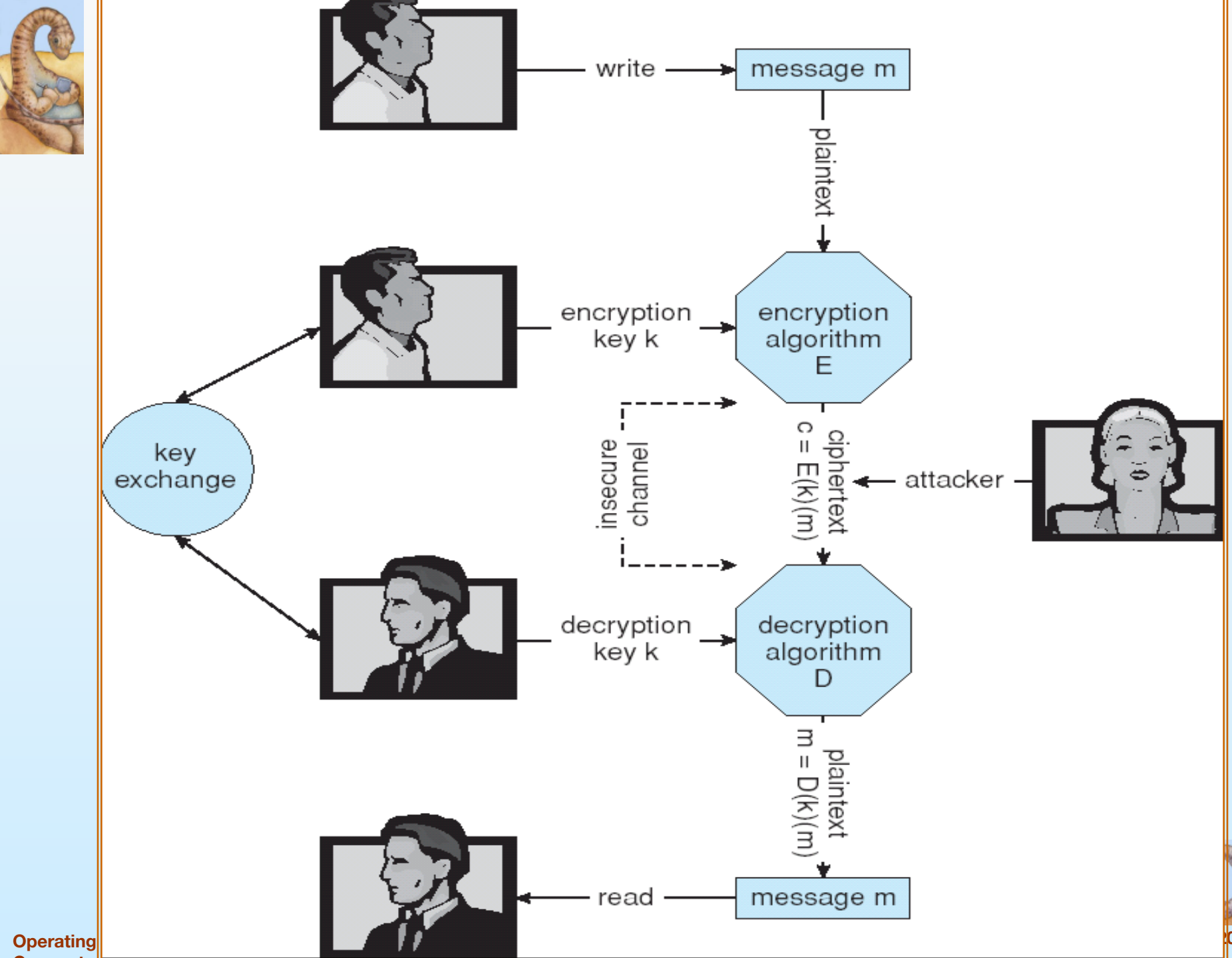
- **Symmetric encryption** (also called *private-key encryption* or *secret-key encryption*) involves using the same key for encryption and decryption.

- Encryption involves applying an operation (an algorithm) to the data to be encrypted using the private key to make them unintelligible.



15.01


Normal
communication
sender
receiver
attacker
Masquerading
sender
receiver
communication
attacker
Man-in-the-middle
sender
communication
communication
receiver
attacker


write
message m
plaintext
encryption key k
encryption algorithm E
key exchange
insecure channel
ciphertext c = E(k)(m)
attacker
decryption key k
decryption algorithm D
plaintext m = D(k)(m)
read
message m

End of Chapter 15

Chapter 12: Secondary-Storage Structures

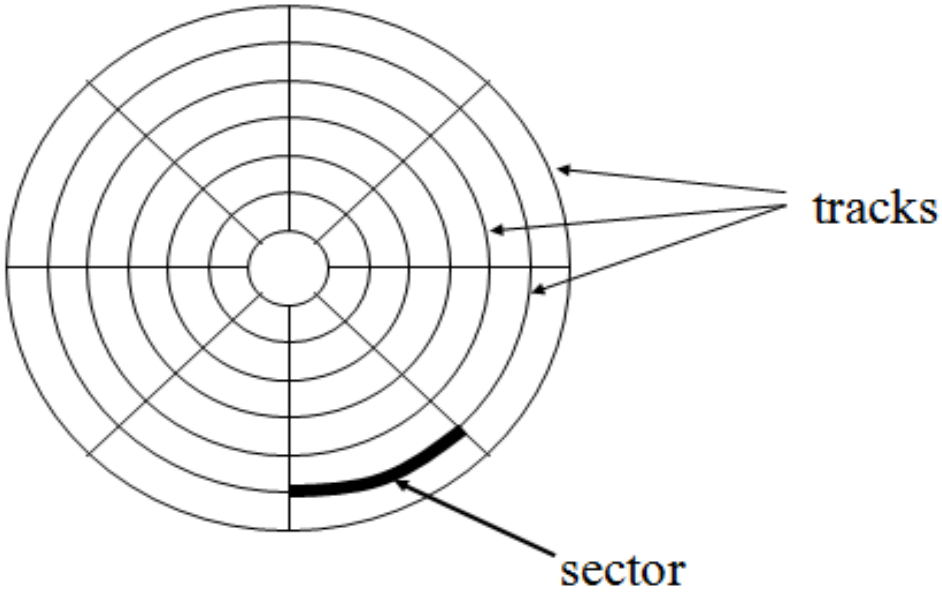
Overview of Mass Storage Structure

- Magnetic disks provide bulk of secondary storage of modern computers
  - Drives rotate at 60 to 200 times per second
  - **Transfer rate** is rate at which data flow between drive and computer
  - **Positioning time** (**random-access time**) is time to move disk arm to desired cylinder (**seek time**) and time for desired sector to rotate under the disk head (**rotational latency**)
  - **Head crash** results from disk head making contact with the disk surface
- Disks can be removable
- Drive attached to computer via **I/O bus**

Magnetic Disks

- Bits of data (0's and 1's) are stored on circular magnetic platters called disks.
- A disk rotates rapidly (60 to 200 times per second).
- A disk head reads and writes bits of data as they pass under the head.
- Often, several platters are organized into a disk pack (or disk drive).

Looking at a surface



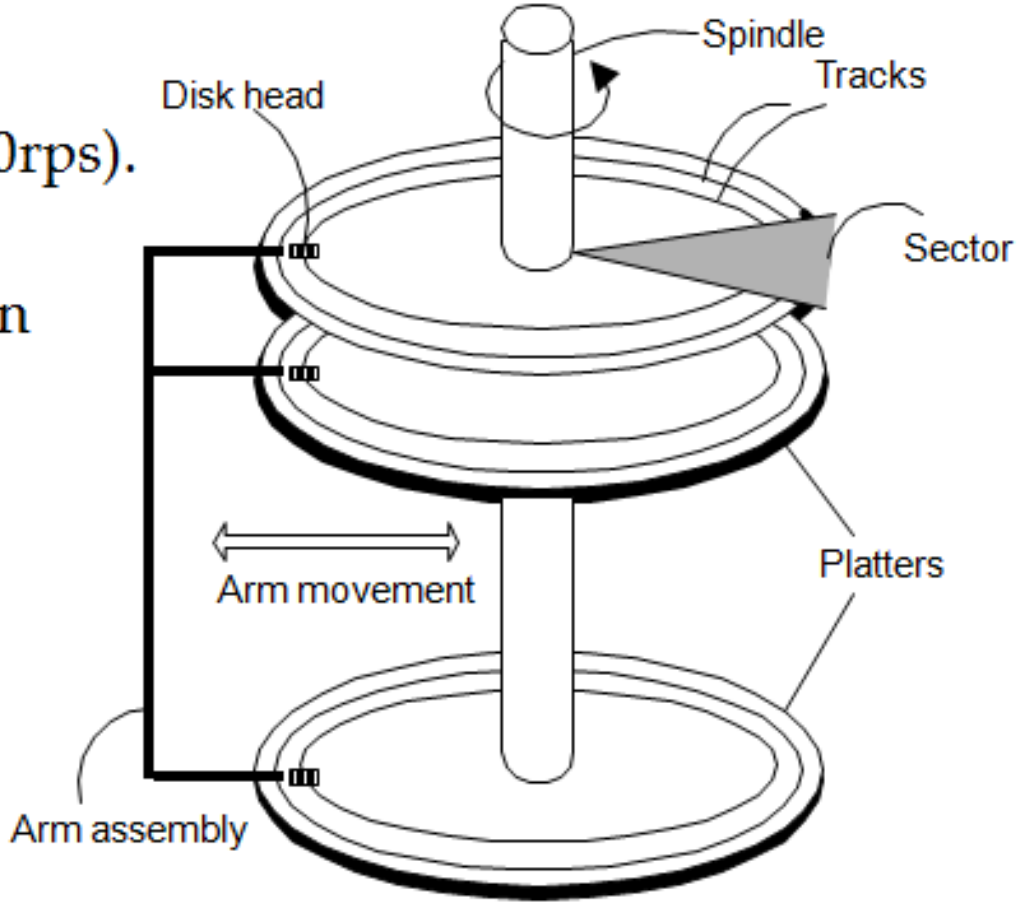
Surface of disk showing tracks and sectors

Organization of Disks

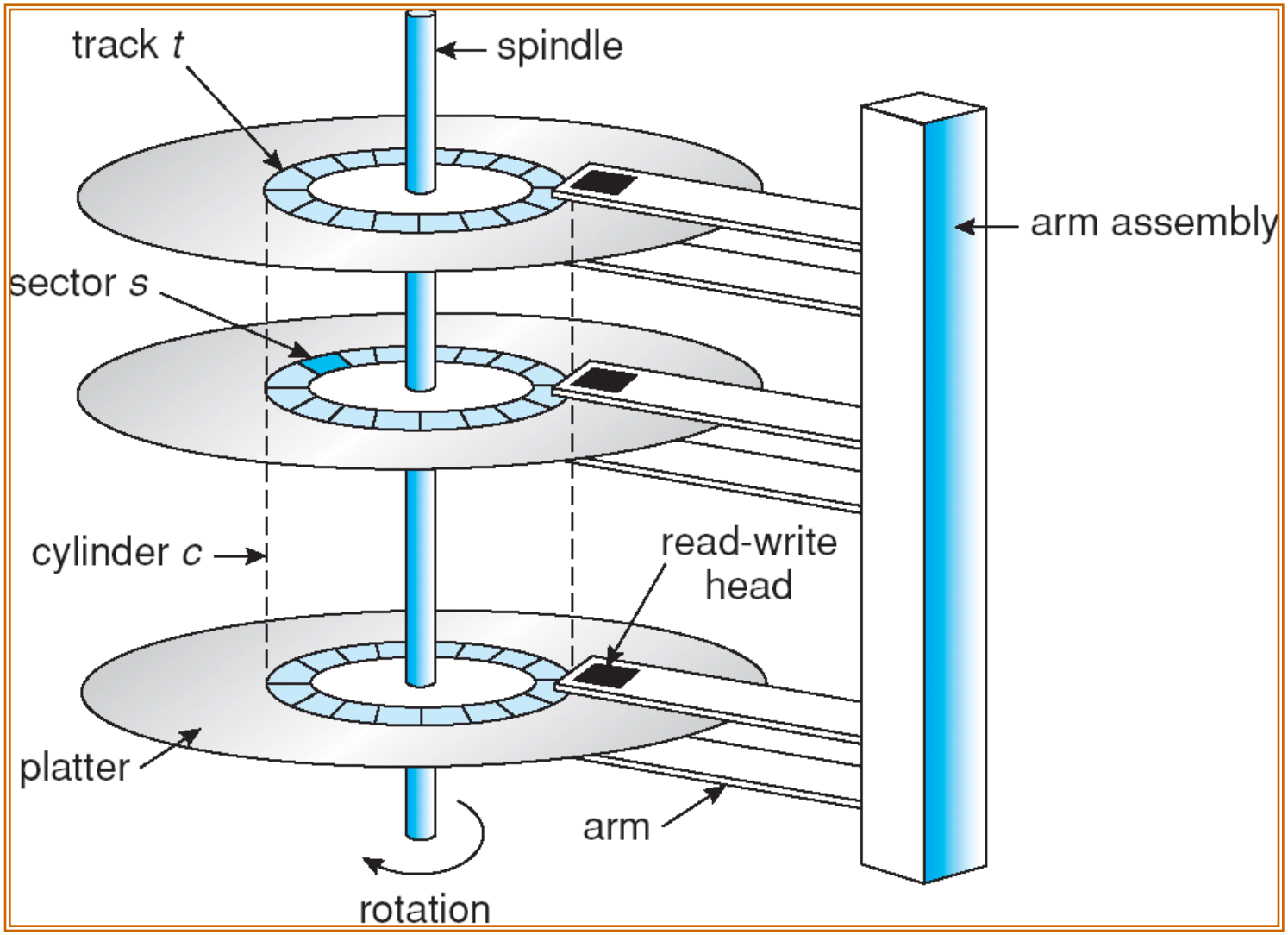
- Disk contains concentric **tracks.**
- Tracks are divided into **sectors**
- A **sector** is the smallest addressable unit in a disk.

Components of a Disk

- The platters spin (say, 90rps).
- The arm assembly is moved in or out to position a head on a desired track. Tracks under heads make a cylinder (imaginary!).
- Only one head reads/writes at any one time.
- Block size is a multiple of sector size (which is often fixed).



Moving-head Disk Machanism



Disk Scheduling

- The operating system is responsible for using hardware efficiently — for the disk drives, this means having a fast access time and disk bandwidth.
- Access time has two major components
  - *Seek time* is the time for the disk are to move the heads to the cylinder containing the desired sector.
  - *Rotational latency* is the additional time waiting for the disk to rotate the desired sector to the disk head.
- Minimize seek time
- Seek time ≈ seek distance

Disk Scheduling (Cont.)

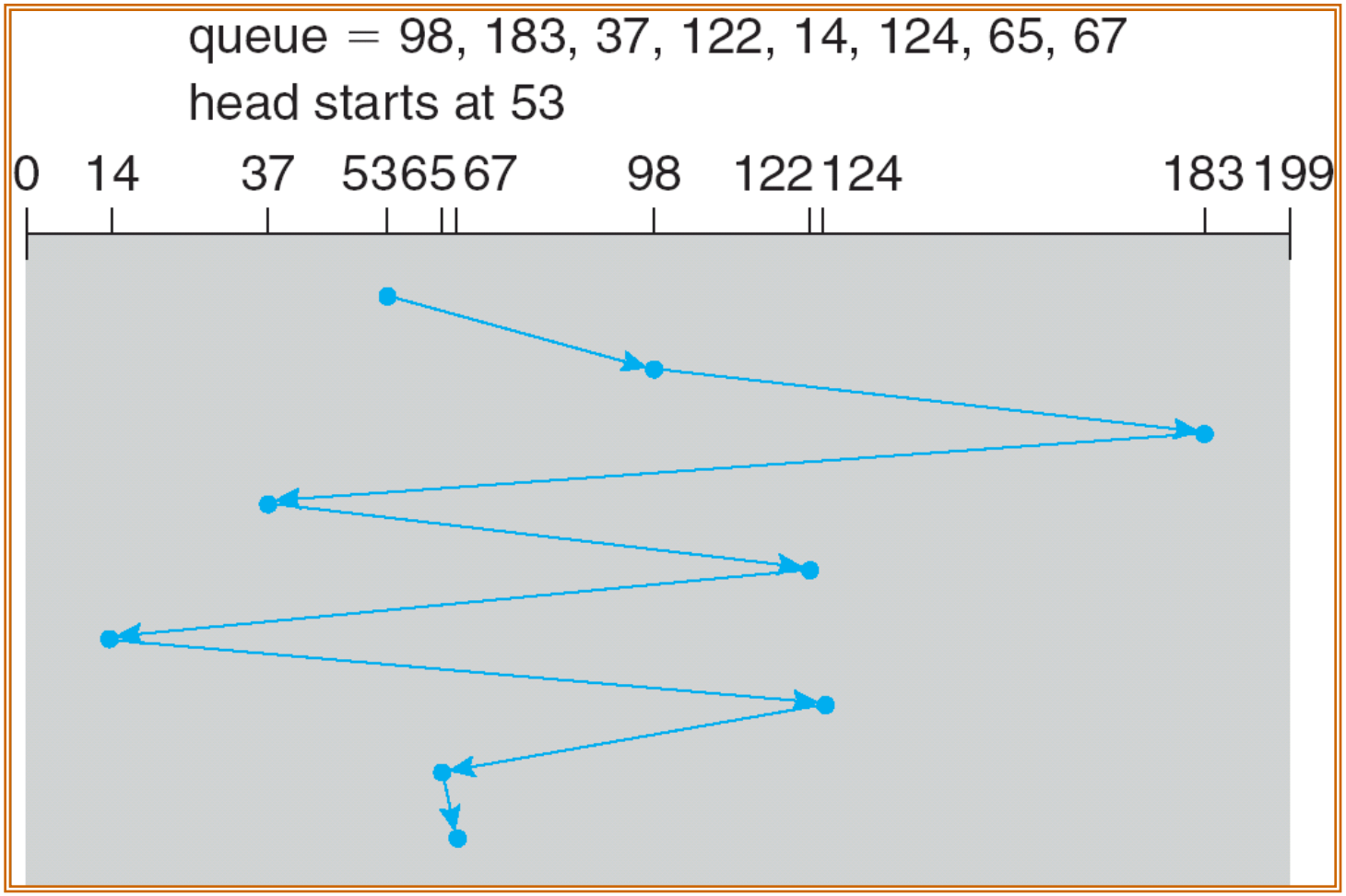
- Several algorithms exist to schedule the servicing of disk I/O requests.
- We illustrate them with a request queue (0-199).

98, 183, 37, 122, 14, 124, 65, 67

Head pointer 53

FCFS

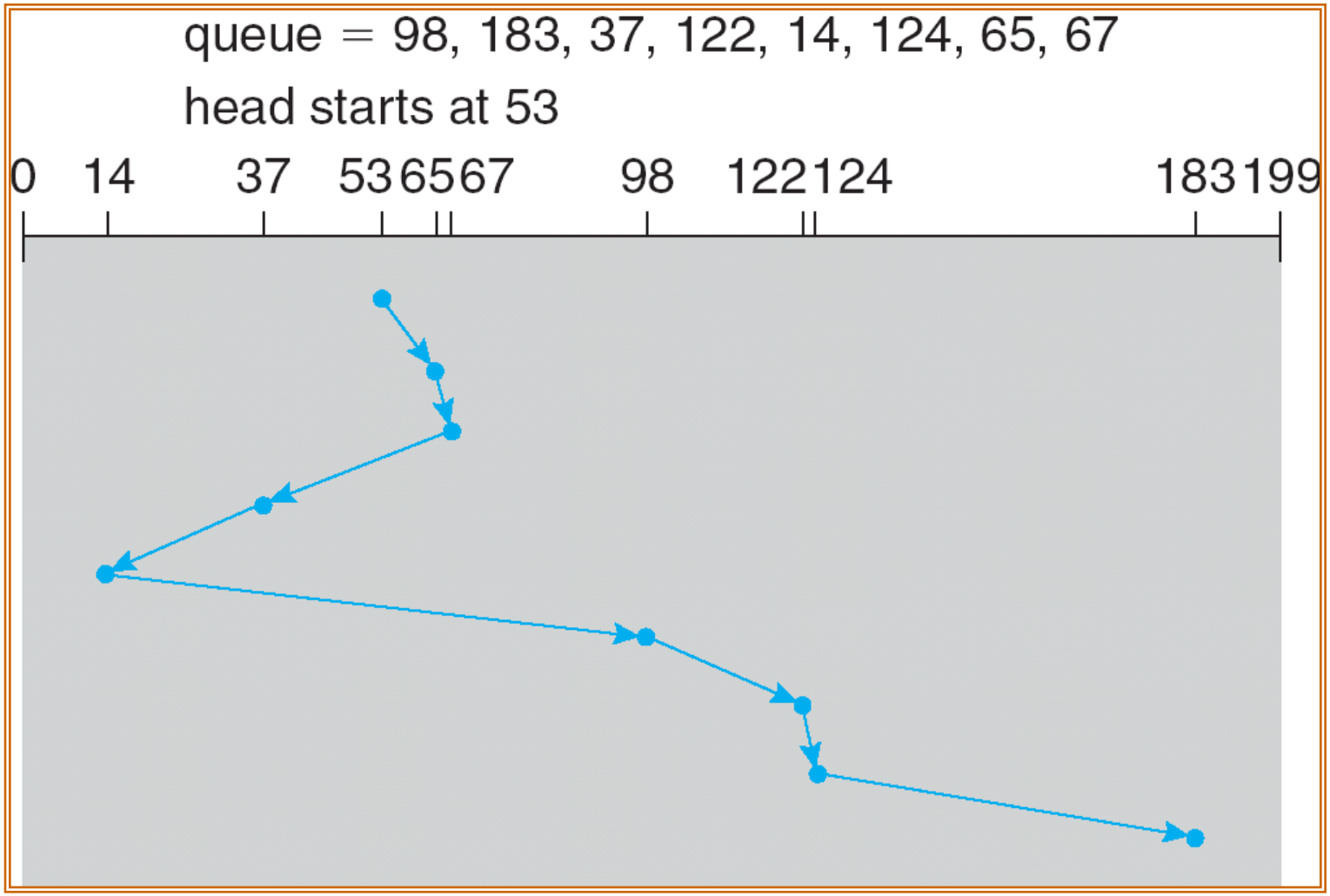
Illustration shows total head movement of 640 cylinders.



SSTF

- Selects the request with the minimum seek time from the current head position.
- SSTF scheduling is a form of SJF scheduling; may cause starvation of some requests.
- Illustration shows total head movement of 236 cylinders.

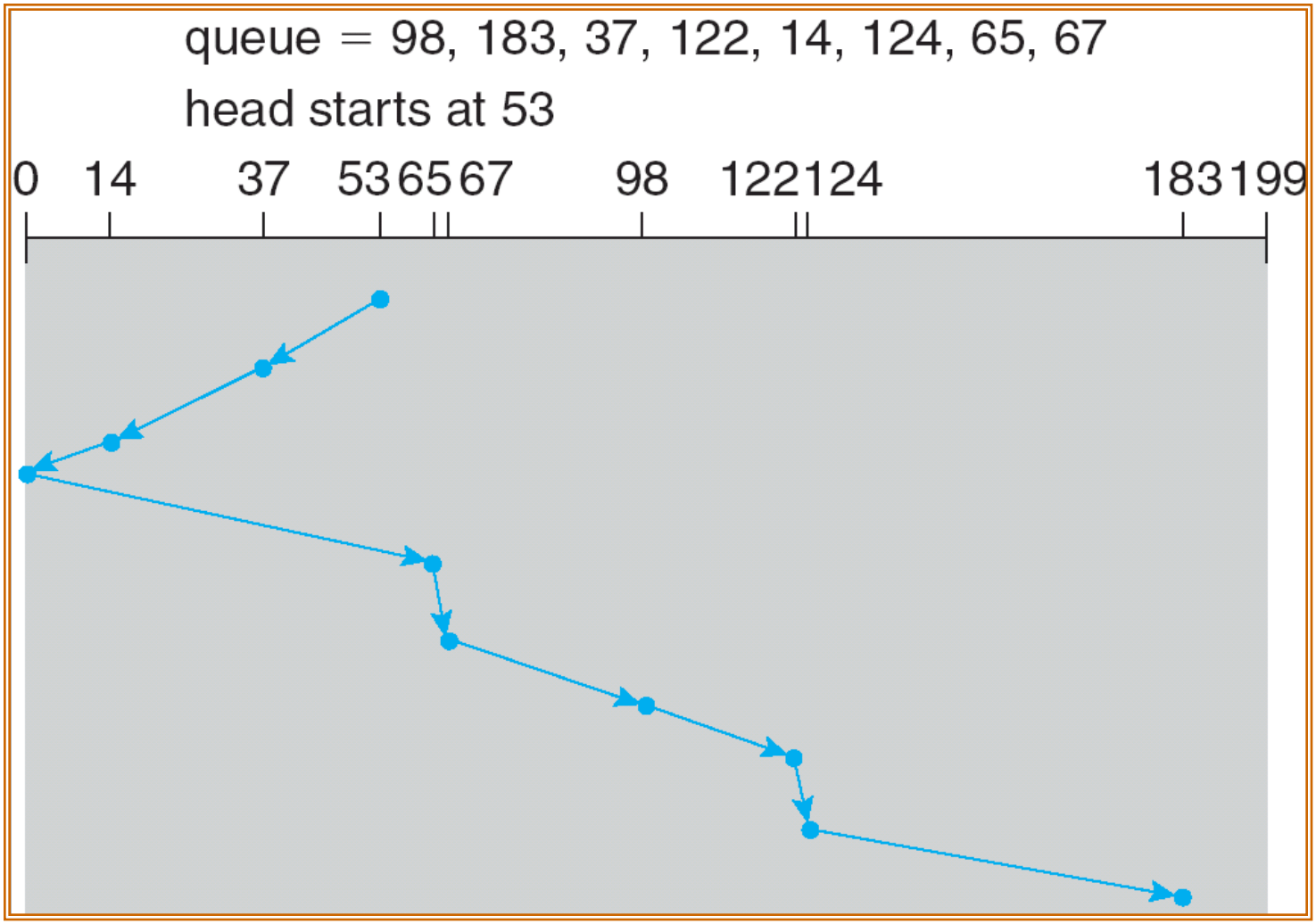
SSTF (Cont.)


queue = 98, 183, 37, 122, 14, 124, 65, 67
head starts at 53
0
14
37
53
65
67
98
122
124
183
199

SCAN

- The disk arm starts at one end of the disk, and moves toward the other end, servicing requests until it gets to the other end of the disk, where the head movement is reversed and servicing continues.
- Sometimes called the *elevator algorithm*.
- Illustration shows total head movement of 208 cylinders.

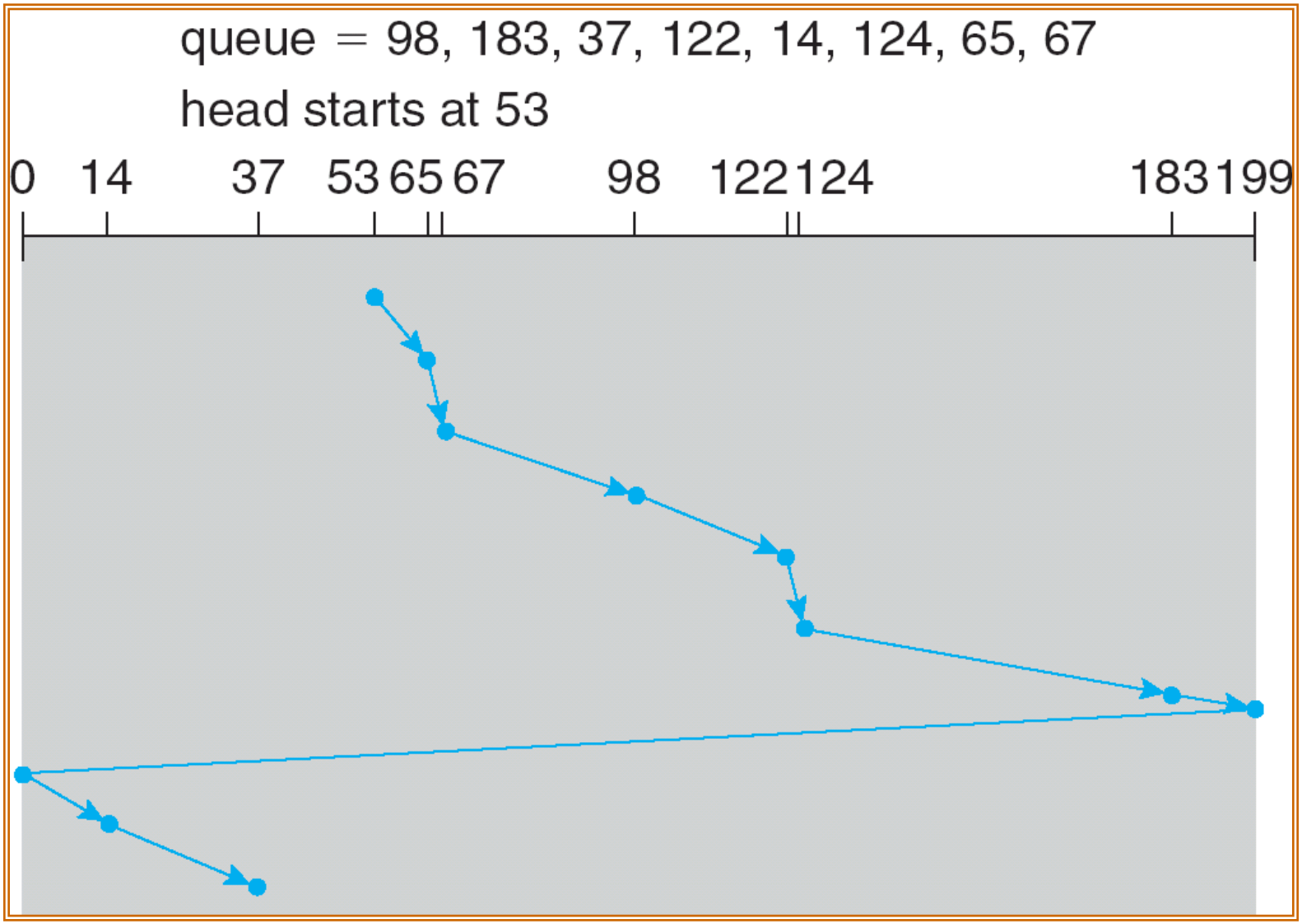
SCAN (Cont.)


queue = 98, 183, 37, 122, 14, 124, 65, 67
head starts at 53
0
14
37
53
65
67
98
122
124
183
199

C-SCAN

- Provides a more uniform wait time than SCAN.
- The head moves from one end of the disk to the other. servicing requests as it goes. When it reaches the other end, however, it immediately returns to the beginning of the disk, without servicing any requests on the return trip.
- Treats the cylinders as a circular list that wraps around from the last cylinder to the first one.

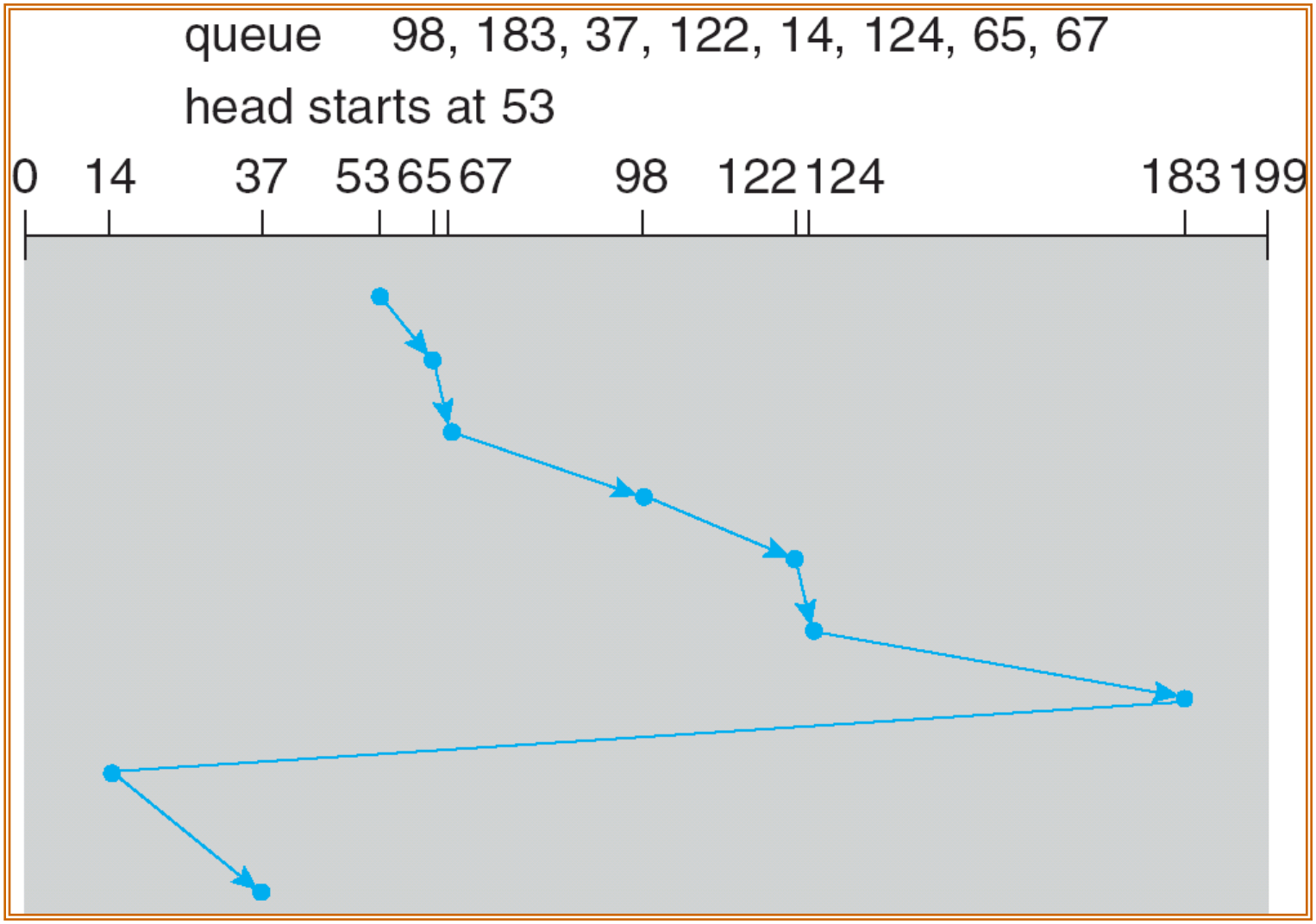
C-SCAN (Cont.)


queue = 98, 183, 37, 122, 14, 124, 65, 67
head starts at 53
0
14
37
53
65
67
98
122
124
183
199

C-LOOK

- Version of C-SCAN
- Arm only goes as far as the last request in each direction, then reverses direction immediately, without first going all the way to the end of the disk.

C-LOOK (Cont.)


queue 98, 183, 37, 122, 14, 124, 65, 67
head starts at 53
0
14
37
53
65
67
98
122
124
183
199

Selecting a Disk-Scheduling Algorithm

- SSTF is common and has a natural appeal
- SCAN and C-SCAN perform better for systems that place a heavy load on the disk.
- Performance depends on the number and types of requests.
- Requests for disk service can be influenced by the file-allocation method.
- The disk-scheduling algorithm should be written as a separate module of the operating system, allowing it to be replaced with a different algorithm if necessary.
- Either SSTF or LOOK is a reasonable choice for the default algorithm.

Disk Management

- *Low-level formatting*, or *physical formatting* — Dividing a disk into sectors that the disk controller can read and write.
- To use a disk to hold files, the operating system still needs to record its own data structures on the disk.
  - *Partition* the disk into one or more groups of cylinders.
  - *Logical formatting* or “making a file system”.
- Boot block initializes system.
  - The bootstrap is stored in ROM.
  - *Bootstrap loader* program.
- Methods such as *sector sparing* used to handle bad blocks.

Types of Devices

- • Despite the multitude of devices that appear (and
- disappear) in the marketplace and the swift rate of
- change in device technology, the Device Manager
- must manage every peripheral device of the system.
- • It must maintain a delicate balance of supply and
- demand – balancing the system’s finite supply of
- devices with users’ almost infinite demand for them.

- Device management involves four basic functions:
- – Monitoring the status of each device, such as storage drives, printers, and other peripheral devices;
- – Enforcing preset policies to determine which process will get a device and for how long;
- – Allocating the devices;
- – Deallocating them at two levels:
- • At the process (or task) level when an I/O command has been executed and the device is temporarily released;
- • At the job level when the job is finished and the device is permanently released.

Types of Devices (cont'd)

- • The system's peripheral devices generally fall into
- one of three categories:
- – Dedicated
- – Shared
- – Virtual
- • The differences are a function of the characteristics of the devices, as well as how they're managed by the Device Manager.

- **Dedicated Devices**
- – Are assigned to only one job at a time.
- – They serve that job for the entire time the job is activen or until it releases them.
- – Some devices demand this kind of allocation scheme, because it would be awkward to let several users share them.
- • Example: tape drives, printers, and plotters
- – Disadvantages
- • They must be allocated to a single user for the duration of a job’s execution, which can be quite inefficient, even though the device is not used 100% of the time.

- **Shared Devices**
- – Can be assigned to several processes.
- – For example – a disk (DASD) can be shared by several processes at the same time by interleaving their requests;
- • This interleaving must be carefully controlled by the Device Manager– All conflicts must be resolved based on predetermined policies.

- **Virtual Devices**
- – A combination of the first two types;
- – They’re dedicated devices that have been transformed into shared devices.
- • Example: printer
- – Converted into a shareable device through a spooling

program that reroutes all print requests to a disk.

- – Only when all of a job’s output is complete, and the

printer is ready to print out the entire document, is the output sent to the printer for printing.

- – Because disks are shareable devices, this technique can convert one printer into several virtual printers,

thus improving both its performance and use.

Types of Devices (cont'd.)

- • Regardless of the specific attributes of the device,the most important differences among them are speed and degree of sharability.
- • Storage media are divided into two groups:
- – **Sequential Access Media**
- • Store records sequentially, one after the other.
- – **Direct Access Storage Devices (DASD)**
- • Can store either sequential or direct access files.
- • There are vast differences in their speed and sharability.