長庚大學112學年度第二學期作業系統實務期中測驗(總分106)

<<請依題號順序作答，跳號作答不予計分，跳號作答不予計分，跳號作答不予計分>>

系級: 姓名: 學號:

1. (10%) For the directory design in file systems, (a) please define Acyclic-Graph Directories. (b) Please present one problem if we extend the directory design to General Graph Directories.

Answer: (a) Acyclic-Graph Directories: Based on a tree structure, this design further allows the sharing of files without having any cycle in the directory structure.
(b) Answer 1: When traversing directories, there could be some infinite loops in the directory structure. Answer 2: There could be some self-referencing cycles, which could make some problems in file deletion.

2. (12%) Please define the (a) Hard Link and the (b) Soft Link. (c) We first create a file ABC, and then create a hard link HL to ABC, a soft link SL1 to ABC, and a soft link SL2 to HL. Now, we remove HL (rm -rf HL in Linux). Can we use the soft link SL1? Can we use the soft link SL2? The reasons have to be provided to support your answers.

Answer: (a) In the hard link design, each directory entry creates a link of a filename to the i-node that describes the file's contents.
(b) A soft link is implemented as a file that contains a pathname to the target file.
(c) SL1: Yes, it refers to the path of ABC, and the path exists.
SL2: No, it refers to the path of HL, and the path is removed.

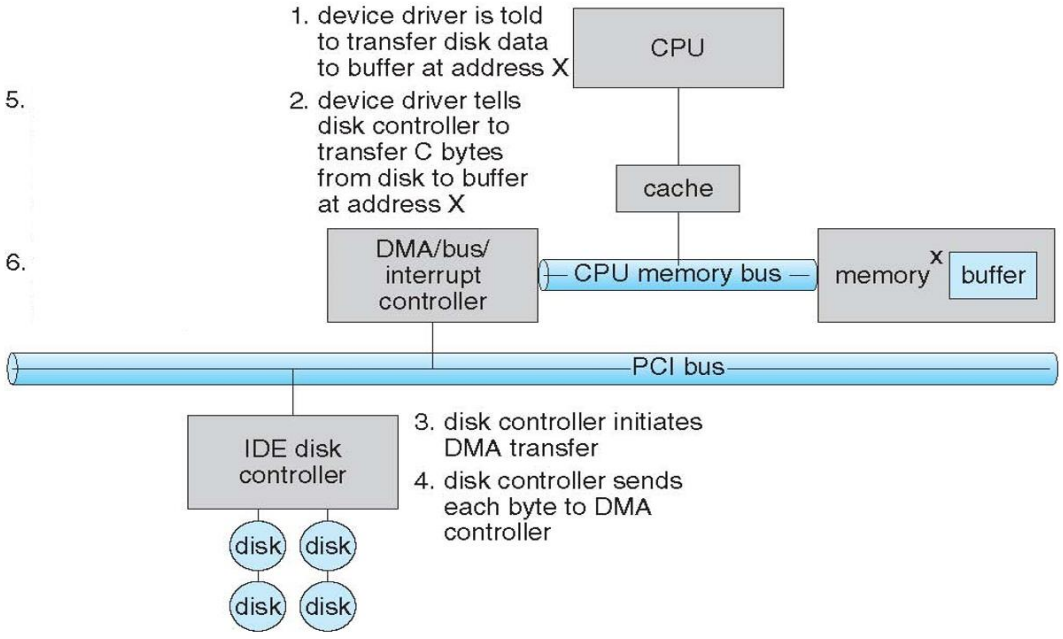
3. (8%) There are three basic methods of file allocation, i.e., Contiguous Allocation, Linked Allocation, and Indexed Allocation. (a) Please answer that the FAT file system is developed on which type of allocation? (b) How does FAT do to reduce the cost of random reads and writes?

Answer: (a) Basically, FAT is a kind of linked allocation.
(b) FAT separates the pointers of linked lists and the data in two different areas. The pointers are collected in the file allocation table for quickly finding out all pointers of a linked list.

4. (8%) For free space manage management of file systems, please explain (a) the Bit Map approach and (b) the Linked List approach with the Counting method.

Answer: (a) There is an array in which each bit indicates the state (free or occupied) of a block.
(b) The first block of a sequence of free blocks will keep the number of the free blocks in the sequence and the pointer to the first block of the next sequence of free blocks.

5. (10%) I/O device management is a critical issue of operating systems. (a) What is the advantage for using Direct Memory Access (DMA)? (b) Please refer to the following figure to explain the details of DMA. Steps 1 to 4 are provided. You have to provide the contents of Steps 5 and 6.



Answer: (a) It can bypass the CPU to transfer data directly between I/O devices and memory so that the CPU can be available for other computing jobs.
(b) Check the details in the lecture slides or textbook by yourselves.

6. (12%) Consider disk scheduling, let a hard drive consist of 300 cylinders, from cylinder 0 to cylinder 299. Assume that the read-write head is now at cylinder 100 and moving toward cylinder 299. Now, there are multiple read/write requests (to be served) in the disk I/O queue, and no other request will further arrive. The queued requests are at the following cylinders: 30, 255, 34, 97, 277, 119, 26, 129. Please illustrate the scheduling results of the (a) SSTF scheduling, (b) SCAN scheduling, and (c) C-LOOK scheduling. (Note that: If the read-write head has to visit cylinder 0 or 299, you have to illustrate that in your answer.)

Answer: (a) SSTF: 97 → 119 → 129 → 34 → 30 → 26 → 255 → 277
(b) SCAN: 119 → 129 → 255 → 277 → (299) → 97 → 34 → 30 → 26
(c) C-LOOK: 119 → 129 → 255 → 277 →26 → 30 → 34 → 97

7. (16%) Please explain (a) **RAID 1**. Assume we use two disks to run a RAID 1, where for each disk, the mean time to failure is 10,000 hours, and the mean time to repair is 100 hours. (b) Please derive the mean time to data loss. (c) Based on RAID 1, if we want to improve not only the reliability but also the performance, we can do RAID 1+0. Please explain **RAID 1+0**. (d) Why is RAID 1+0 better than RAID 0+1?

Answer: (a) Mirroring or shadowing keeps duplicate of each disk
(b) Mean time to failure of any of the two disks: 10,000/2 = 5,000
The possibility for another disk to fail within the 100 hours: 100/10,000 = 1/100
Mean time to data loss is 5,000 / (1/100) = 500,000 hours
(c) For each disk, another disk is used to do the RAID 1 mirroring.
Several RAID 1 volumes are used together for RAID 0 data striping.
(d) When a hard disk fails, in RAID 1+0, only the bad hard disk should be offline. But in RAID 0+1, all hard disks in the data striping group of the bad hard disk should be offline.

8. (12%) Please carefully define the concepts of (a) Buffering, (b) Caching, and (c) Spooling.

Answer: (a) Buffering: Buffering is to store data in some intermediate devices, such as DRAM, while the data are transferring between devices. It can be used to cope with some problems of the device speed mismatch and the device transfer size mismatch.
(b) Caching: A cache is a region of fast memory that holds copies of data. The difference between a buffer and a cache is that a buffer may hold the only existing copy of a data item, whereas a cache, by definition, holds a copy on faster storage of an item that resides elsewhere.
(c) Spooling: A spool is a buffer that holds multiple outputs for a device, such as a printer, that cannot accept interleaved data streams.

9. (8%) There are several security violation methods. Please explain (a) Man-in-the-middle attack and (b) Replay attack.

Answer: (a) Man-in-the-middle attack: Intruder sits in data flow, masquerading as sender to receiver and vice versa
(b) Replay attack: Send a recorded message again as is or with message modification

10. (10%) Assume that there are a public key K_e and a private key K_d, where K_e and K_d are a pair. E() and D() are the encryption and decryption functions, respectively. $E(K_e, X)$ is the encryption result of any data X by using function E() with the key K_e, and $D(K_d, Y)$ is the decryption result of any ciphertext Y by using function D() with the key K_d. Now, let Emilly have key K_e, and David have key K_d.
    (a) If Emilly wants to send private data Q to David, what should they do?
    (b) If David wants to prove that he is David (i.e., having the private key K_d) to Emilly, what should they do?

Answer: (a) 1. Emilly sends the encryption result $E(K_e, Q)$ to David.
2. David then gets the decryption result $D(K_d, E(K_e, Q))$ → Q.
(b) 1. Emilly sends the encryption result E(Ke, P) to David.
2. David then gets the decryption result D(Kd, E(Ke, P)) → P.
3. David sends the result P back to Emilly to prove that David has the private key.