Indian Institute of Engineering Science and Technology, Shibpur

B. Tech. (CST) 6th Semester End-Term Examination, April 2024

Operating Systems (CS 3201)

Full Marks: 50 Time: 3 hours

- **Attempt any five (5) questions.**
- **All questions carry equal marks.**
- **Answers should be precise, to the point, and in your own words as far as practicable.**
- **Make your own assumptions, if necessary, and state them at proper places.**

1. (a) Explain the idea of "*mounting*" a filesystem (present in secondary storage) under a running operating system, with particular emphasis on how it facilitates subsequent operations on the files/folders of the filesystem.
   (b) Explain how inconsistencies may crop up in a filesystem (present in secondary storage) if it is not "*unmounted*" and the computer is switched off abruptly. [5+5]

2. (a) Explain how the idea of "*Resource Allocation Graph*" or its variants can be used in **Deadlock Detection** and **Deadlock Avoidance**.
   (b) Explain the idea of "*safe state*" in the context of **Deadlock Avoidance** and how it can be identified in a system having multiple instances of resources. [5+5]

3. (a) Explain the role of "*paging*" in **Virtual Memory**.
   (b) What are the different strategies for maintaining **Page Table** in **Memory Management**? [5+5]

4. (a) Explain how semaphores can be used in different scenarios for synchronization among different sections of code across multiple processes.
   (b) What are the different "*tools*" provided by **pthread** for **thread synchronization** and how are those tools used? [5+5]

5. Explain how protection is enforced in a *Unix-like* operating system in terms of "*ugo*" (user, group, and others) and "*rwx*" ('read', 'write', and 'execute') bits over resources (like file, directory, semaphore, shared memory, IO devices, process, etc.). [10]

6. Write short notes on ~~any two of~~ the following.
   (a) Block Device and Character Device
   (b) Signal Handler [5+5]

Indian Institute of Engineering Science and Technology, Shibpur
B.Tech CST 6th Semester Final Examinations, April-May 2024

Data Communication and Computer Network CS-3202

Full Marks: 50 Time: 3 hours

Attempt mandatory question 1 and any five (5) from the rest (from 2 to 8)
All parts of the same question must be answered together

1) Mandatory Question (Total Marks 20)

(a) Two stations in the network use a two-dimensional even parity scheme for error detection. The bit sequence of a received frame at the receiving station is as follows

1 1 0 0 1 0 1 0 0 0 1 1 0 0 1 1 1 0 0 0 1 0 0 0 1 1 1 0 1 1 1 1 1 0 0 1 0 0 1 0

Specify the actual information bits (information without parity bits) sent by the transmitting station. Assume that no error occurred in the actual information part. Is this frame going to be accepted by the receiver? Answer with justification. [4]

(b) Station A needs to send a message consisting of 9 packets to Station B using a sliding window (window size 3) and go-back-N error control strategy. All packets are ready and immediately available for transmission. If every 5th packet that A transmits gets lost (but no acks from B ever get lost), then what is the number of packets that A will transmit for sending the message to B? Answer with justification. [3]

(c) Node X has a TCP connection open to node Y. The packets from X to Y go through an intermediate IP router R. Ethernet switch S is the first switch on the network path between X and R. Consider a packet sent from X to Y over this connection. What will be the destination IP and destination MAC address of the IP packet sent from node X? [3]

(d) In classful addressing, find the Class of following IPv4 addresses
(i) 01100001 10101011 00001011 11101111, (ii) 180.5.51.131, (iii) 20.33.120.11 [3]

(e) Each of the following IPv4 addresses belongs to a block. Find the first and last usable IP address of each block – (i) 26.23.71.22/24 and (ii) 110.33.61.193/28 [3]

192 & 206

(f) A router received an IPv4 datagram containing 3800 bytes of payload. It is also observed that the DF flag in the IPv4 header is set to zero (0). The datagram has to be forwarded to next-hop over an Ethernet LAN. The Ethernet frames may carry payload data up to 1500 bytes (i.e. MTU=1500 bytes), and note that the size of the IP header is 20 bytes (*there is no option field in the IP header*)

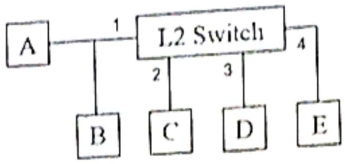
(i) How many IP fragments will be transmitted in total?
(ii) Mention the value of each fragment's MF and Fragment-Offset of IPv4 header. [4]

2) (a) In the context of Distance Vector Routing, explain the algorithm used by a router A to update its routing tables on receiving the distance vector from another router B. The RIP protocol can be used as a reference to explain the algorithm.

(b) What is Count-to-Infinity problem? [4+2]

3) Mention the functionalities of <u>any 2</u> layers of OSI model among the following: [2x3]
(a) Data Link, (b) Network, (c) Presentation Layer

4) Five hosts A, B, C, D, and E are connected using a Layer-2 switch. Assume that the switch initially does not know anything about any of the hosts (empty lookup table). The first few frames are transmitted in the given order:



(a) A → C, (b) A → B, (c) C → A, (d) E → B, (e) E → C, (f) B → D, (g) D → A and (h) C → D

Which of these frames are broadcast by the L2-switch and which frames are unicast? Answer with brief justification. [6]

5) A router in an IP network has the following routing table:

Subnet Number	Subnet Mask	Interface
33.197.152.0	255.255.248.0	Eth0
33.197.128.0	255.255.252.0	R2
33.86.0.0	255.255.192.0	R4
33.197.130.0	255.255.254.0	R1
Default		R2

Find the next hop for packets having the following destination IP addresses:
(a) 33.86.16.234, (b) 33.197.131.25, (c) 33.86.130.186, (d) 33.197.155.138 [6]

6) An ISP is granted the block 180.20.56.128/26 IPv4 address. As of now, the ISP is required to allocate IP addresses among three organizations, Org-1, Org-2, and Org-3, with 12, 6, and 4 usable IP addresses respectively. The granted block is utilized effectively, following the conservation of IP addresses strategy. Propose the following for every organization:
(a) Network Id, (b) Netmask, (c) Range of Usable IP addresses, (d) Directed broadcast IP [6]

7) Following is the part or complete TCP header dump (contents) in hexadecimal format.

CAF30050 00004E20 00004650 503070FF 00000190

Answer following questions with <u>brief justification</u>:
(a) Is this complete TCP header dump?
(b) Mention the source port and destination port number.
(c) What is the sequence number?
(d) Is acknowledgement number valid? If yes, then what is the acknowledgement number?
(e) What is the total amount of yet to be acknowledged bytes?
(f) What is the application layer protocol? [6]

8) Write short note on <u>any 2</u> from the following:
(a) User Datagram Protocol (UDP)
(b) Border Gateway Protocol (BGP)
(c) Virtual-circuit Network [2x3]

Indian Institute of Engineering Science and Technology, Shibpur

B. Tech (CST) 6th Semester End-Semester Examination, April, 2024

Software Engineering (CS3203)

Full Marks: 50 *Time: 3 Hours*

- *Answer to only five questions. No answer to extra question will be evaluated.*
- *Section-A is mandatory and answer any two questions from Section-B*
- *Answer all parts to a same question together.*
- *Use diagram wherever possible*

Section-A
(Mandatory)

1. Choose the correct alternative. A short explanation/elaboration behind the answer is needed.

(a) I: DFD is not a UML diagram, II: Sequence diagram is a UML diagram
(i) I-True, II –False (ii) I-True, II – True (iii) I- False, II –False (iv) I- False, II – True

(b) What is the 4th stage of a very simplified software engineering model?
(i) Feasibility study (ii) Coding (iii) Testing (iv) Design

(c) Which of the following is not associated to software design?
(i) Boundary value analysis (ii) Navigation (iii) Algorithm (iv) Structure chart

(d) A software engineering model is selected based on
(i) Requirements (ii) Development team and users (iii) Project type & associated risks (iv) All of these

(e) Incorrect phase of waterfall model is
(i) Requirement analysis (ii) Coding (iii) Staffing (iv) Design

(5×2=10)

2. Clearly decide the correctness of the following statements with proper justifications. If justifications are incorrect/ambiguous/inconsistent with your decision, then marks will not be considered.

(a) When a customer demands for increasing number of software users, then this type of requirement is functional.

(b) A good software interface should be built for novice users only.

(c) Line of code cannot estimate project duration perfectly.

(d) Black box testing does not require the knowledge of control flow in a source code.

(e) As per most of coding standards, use of global variables should be restricted.

(5×2=10)

3. Read the following technical paragraphs carefully and answer the questions **in one sentence.**

(a) Requirement gathering is a communication process between the parties involved and affected in the problem situation. The tools in elicitation are meetings, interviews, video conferencing, e-mails, and existing documents study and facts findings. More than 90% to 95% elicitation should be completed in the initiation stage while the remaining 5% is completed during the development life-cycle. The requirements are gathered from various sources like primary users and different secondary users.

(i) Find an alternative word for 'Requirement gathering' from this paragraph.
(ii) When a customer is in remote location, how can requirements be gathered?
(iii) What is the type of person interacting directly with the software product?
(iv) What is the type of person not interacting directly with the software product, but get benefitted from its usage?
(v) "...remaining 5% is completed during the development life-cycle"- Here the author is talking about model other than classical waterfall. Do you agree?

(b) There are two common abstraction mechanisms for software systems: Functional abstraction and data abstraction. In functional abstraction, a module is specified by the function it performs. For example, a module to sort an input array can be represented by the specification of sorting. Functional abstraction is the basis of partitioning in function-oriented approaches. That is, when the problem is being partitioned, the overall transformation function for the system is partitioned into smaller functions that comprise the system function. The second unit for abstraction is data abstraction. There are certain operations required from a data object, depending on the object and the environment in which it is used. Data abstraction supports this view. Data is not treated simply as objects, but is treated as objects with some predefined operations on them. The operations defined on a data object are the only operations that can be performed on those objects. From outside an object, the internals of the object are hidden; only the operations on the object are visible.

(i) What is the technique of partitioning problem into several functions and setting up hierarchy among these?
(ii) What is the technique of treating complex data as a simple piece of data?
(iii) In function oriented design, find an alternate word for 'a unit of function' from this paragraph.
(iv) "From outside an object, the internals of the object are hidden"-what are internals of the object here?
(v) "...to sort an input array can be represented by the specification of sorting"- Here, one of the specifications that the author indicates is whether array is sorted in ascending or descending order. Do you agree?

$(2\times5=10)$

Section-B

(Answer any two questions)

4. Write a short note on

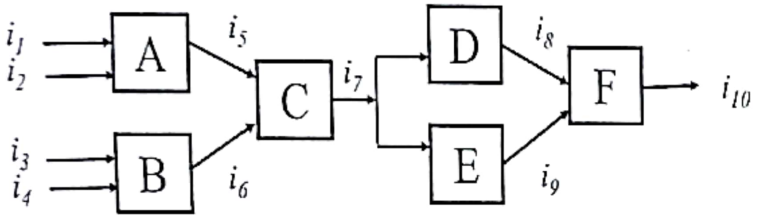
(a) Data tree
(b) Navigation
(c) Graphical widgets
(d) Brute force debugging approach: A case study
(You may select a source code of your choice.)
(e) Role of DAG to improve coding

$(5\times2=10)$

5. State the difference between
   (a) CLI vs GUI
   (b) Classical waterfall vs iterative waterfall model
   (c) Architecture design vs component design
   (d) Functional format vs project format staff organization
   (e) Exploratory approach vs engineering approach

(5×2=10)

6. Assume that an architecture design of software is represented by mathematical operations calculated through A, B, C, D, E, F modules where $i_k \in \{0,1\}$ and $k \in \{1,2,3...10\}$. Here, integration testing plan at module C is represented by C (A, B) and unit testing plan Module B is represented by truth table with empty at the output side.



Module **B**

i_3	i_4	i_6
0	0	
0	1	
1	0	
1	1	

(a) Similarly, write unit testing plan for Module A, C, D and F.
(b) Write integration testing plan with big bang approach.
(c) Is there any advantage or drawback with big bang approach? Discuss in this context.
(d) Write integration testing plan with incremental approach starting at C and towards output.
(e) Write test plan for acceptance testing when software is fully compatible with operating system and hardware.

(5×2=10)

7. (a) Write the equations of effort and development time for organic COCOMO.
(b) "Ability to work in a team is a feature of good software engineer"-Discuss.
(c) Why is ISO 9000 used for?
(d) "Other than quality analysis of end product, quality of analysis of software development stages is also possible"—Explain this statement.
(e) Mention any two technical risks to develop a software.

(5×2=10)

Indian Institute of Engineering Science and Technology, Shibpur
BTech 6th Semester End-Semester Examination, April 2024
Information Security and Cryptography (CS 3204)

Time: 3 Hours **Full Marks: 50**

[Answer any five questions]

1. (a) What is the main mathematical motivation behind RSA algorithm?
   (b) Cryptographic operations can be very slow, especially for large numbers. One of the operations we need to perform in RAS is to first raise a number to a certain exponent, and then find the modulus of the result. This can be very expensive for very large numbers. Now, write down one efficient solution to this problem. Also explain every step of your approach with a suitable example.
   (c) What is Euler's Totient Function and how is it related with RSA algorithm?
   (d) Using RSA, encrypt the message M = 3, assuming the two primes chosen to generate the keys are p = 13 and q = 7. You are to choose a value of encryption key $e < 10$. Show your calculations and assumptions.

   [1 + 3 + 2 + 4]

2. (a) What is the role of super-increasing sequence in Merkle-Hellman Hard Knapsack cryptosystem?
   (b) Considering $(10010011)_2$ as the plain text in Merkle-Hellman hard Knapsack Cryptosystem, show the steps of both encryption and decryption. Assume a private key correctly and find out the corresponding public key for the above encryption and decryption.
   (c) Write down the motivations behind the use of digital envelope.
   (d) Explain the working principle of digital envelope.

   [2 + 4 + 1 + 3]

3. (a) What is message-digest and what purpose does it serve?
   (b) What are the properties of message digest?
   (c) Suppose you are to find out the digest of a 6,590 bit message using MD-5 algorithm. Determine the padding that you need to concatenate to this message.
   (d) Compare and contrast MD-5 and SHA-1 algorithms.

   [2 + 3 + 2 + 3]

4. (a) What is message authentication code and how does it differ from message-digest?

   (b) What is hash-based message authentication code (HMAC) and what are the different purposes that it fulfils?

   (c) What is the role of input-pad (ipad) and output-pad (opad) in HMAC?

   (d) Write down the disadvantages of HMAC?

[3 + 2 + 2 + 3]

5. (a) What is digital certificate?

   What are the contents of this certificate?

   (b) What are the different parties involved in digital certificate creation?

   What are their roles during creation of digital certificate?

   (c) How can we verify a digital certificate?

[(1 + 3) + (1 + 3) + 2]

6. *(a) What do you mean by protection state of a system and how is it monitored?*

   (b) Explain different phases that a typical virus goes through during its lifetime and comment critically on the effects of different phases on the protection state of the affected system.

   (c) What do you mean by Ransomware Attack?

   Explain the Ransomware process with a flow diagram.

[2 + 3 + (2 + 3)]

7. Write short notes on any two of the following topics.

   (a) Digital Signature Techniques

   (b) Phishing Attacks

   (c) Authentication Token

[5 × 2 = 10]

Indian Institute of Engineering Science and Technology, Shibpur

BTech (CST) 6th Semester Examinations, February 2024

Subject: Computing-in-Memory Architecture (CS-3223)

Full marks: 50 Time: 3 hours

Answer any *five*

1. In CPU-centric von Neumann computing model, define memory wall, ILP wall, technology wall, reliability wall and cost wall. Define, in brief, the Computing-in-Memory (CIM) approaches. Denote the working set locations for such CIM approaches. 10

2. Show the construction of a DRAM cell with a capacitor and an access transistor that controls access to the cell. Describe normal read operation of DRAM, following charge sharing, assuming that the cell capacitor is initially charged. Following triple-row activation (TRA) explain how A+B and A.B (each A/B is of 1-bit) can be realized within the DRAM. 10

3. What is memristor? Show the general structure of memristive crossbar memory. Describe write and read operations in the memristive memory. Realize MAGIC (Memristor-Aided Logic) NOT and NOR in the memristive crossbar. 10

4. Define memristor-based Material Implication (IMPLY) logic. Compute Z = A NOR B with IMPLY. Show the construction of IMPLY within a crossbar. Show how a 2:1 MUX can be realized with IMPLY. 10

5. Describe bitonic sorting scheme considering the example unsorted list Y = 19, 2, 72, 3, 18, 57, 603, 101. Realize bitonic sorting scheme in memristive memory. 10

6. What is an Akers array cell? Show how an Akers array realizes the function f=xz'+yz. Describe a procedure, with example, for calculating the binary output of an Akers array. Show how in-memory computation can be done to realize 2-input NAND/NOR gates in QCA Akers array. 10

7. Write short notes on the following 10

a) In-memory searching in SRAM based CAM.

b) *n*-channel enhancement-type MOSFET