Indian Institute of Engineering Science and Technology, Shibpur

B. Tech. (CST) 6^{th} Semester End-Term Examination, April 2025

Operating Systems (CS 3201)

Full Marks: 50 Time: 3 hours

- **Attempt any five (5) questions.**
- **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 what you understand by metadata of files, folders, and filesystems in an operating system; and the purpose they serve. [6]

   (b) Explain how filesystem organization influences the random-access nature of files in an operating system. [4]

2. (a) Explain with suitable example(s) how the attempt(s) to eliminate the possibility of race-condition may lead to deadlock in a system. [5]

   (b) How can deadlock be detected in a system having multiple instances of resources? [5]

3. (a) Explain the idea of paging in memory management by operating systems along with its hardware requirement(s). [5]

   (b) How does paging facilitate virtual memory and virtual memory facilitate "concurrent" execution of multiple processes? [5]

4. (a) Explain the usage of the file-related system calls provided by Linux (or Unix-like) operating system. [5]

   (b) Explain how those file-related system calls can uniformly be used for accessing different resources (other than files) of a system. [5]

5. (a) Explain the **role** and **usage** of *pipe* (|) as an Inter-Process-Communication tool provided by the operating system. [5]

   (b) When and how does the operating system code execute on a multi-tasking system? [5]

6. Write short notes on the following.

   (a) Device files on a Linux (Unix-like) Operating System [5]

   (b) Object Code and Loadable Module [5]

Indian Institute of Engineering Science and Technology, Shibpur
B.Tech CST 6th Semester Final Examinations, April/May 2025

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 9)
All parts of the same question must be answered together

1) Mandatory Question (Total Marks 20)

a) A router received an IPv4 datagram (with header size 20 bytes without any option field) containing 2800 bytes of higher layer payload. It is also observed that the DF and MF flags in the IPv4 header are set to zero (0). The datagram must be forwarded to the next hop over the connected link, where MAC frames can carry payload data up to 1220 bytes (i.e., MTU=1220). Answer the followings –

(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.

[1+3]

b) Consider a network where IP and ARP protocols are used. A host in this network, S having the IP address SI and MAC address SM wants to send an IP packet to another host D having IP addresses DI and MAC address DM. The default gateway for this network is G, having IP address GI and MAC address GM. Assume that host S knows the IP addresses GI and DI but does not know the MAC addresses GM and DM.

Describe the actions taken by S for knowing the MAC address of the node to which it should send the data packets, when
(i) D is in the same local network as S, and
(ii) D is in a different network.
State the IP and MAC addresses of each packet transmitted by S or G during this process.

[3+3]

c) In classful addressing, find the Class of following IPv4 addresses
(i) 190.15.50.121, (ii) 15.34.121.10

[2]

d) Each of the following IPv4 addresses belongs to a block. Find the first and last usable IP address of each block – (i) 27.23.71.18/24 and (ii) 100.33.61.181/28

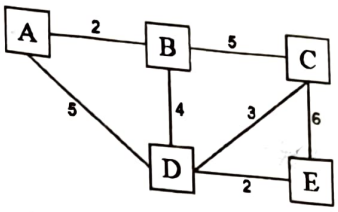
[2]

e) An ISP is granted the block 80.70.90.0/25 IPv4 address. The ISP needs to allocate address among three organizations, Org-A, Org-B and Org-C with 54, 28 and 24 IP addresses respectively. For every organization, find the following with brief explanation:
(i) Network Id, (ii) Netmask, (iii) Range of IP addresses, (iv) Directed broadcast IP address

[6]

2) A five node autonomous system (AS) is shown using the following graph, where routers are represented by the nodes of the graph. The cost of individual link between the routers is mentioned in the graph itself. The Link State Routing protocol is used as the intra-AS routing. Answer the following questions

a) Mention Initial Link State knowledge of every router on neighbor discovery procedure.
b) Mention the Link State Database (LSDB).
c) Mention the routing table at node C.



[2+2+2]

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

Subnet Number	Subnet Mask	Interface	Next-hop
233.197.152.0	255.255.248.0	eth0	-
233.86.0.0	255.255.192.0	eth2	R2
233.197.130.0	255.255.254.0	eth3	R1
Default		eth4	R3

Find the next-hop (and interface) for packets having the following destination IP addresses:
a) 233.86.16.234, b) 233.86.130.186, c) 233.197.155.138 [3x2]

4) In a 10mbps Ethernet (CSMS/CD) network, two stations A and B situated apart 1800 meter and the propagation speed is 2×10^8 meter/sec. If station A transmitting at time T1, then answer with justification. (*Note that μs stands for microseconds*).

a) Does the protocol allow station B to start transmitting at time T1 + 8 μs?
b) Does the protocol allow station B to start transmitting at time T1 + 12 μs? [3+3]

5) a) In the context of Distance Vector Routing protocol, 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]

6) a) Describe TCP connection termination procedure using suitable examples.
b) What is the use of TIME_WAIT state in TCP? [4+2]

7) a) Mention brief understating of URG and PSH flags in TCP header.
b) What is TCP pseudo header and why it is important? [4+2]

8) Write the difference between Go-Back-N and Selective Repeat ARQ protocol, mentioning function of working, strengths, weaknesses, and applicability. [6]

9) Write short note on any 2 from the following:

a) Internet Control Message Protocol (ICMP)
b) Network Address Translation (NAT)
c) The support of QoS in IP Header [2x3]

Indian Institute of Engineering Science and Technology, Shibpur

B. Tech (CST), 6th Semester, End-Semester Examination, 2025

Software Engineering (CS3203)

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

- ***Answer only five questions. No answer to extra question will be evaluated.***
- ***Answer any three questions from Section-A and Section-B is mandatory***
- ***Answer all parts to a same question together.***
- ***Use diagram wherever possible***
- ***In case of typing mistake/error/confusion in the question paper: Don't panic. Don't call invigilators out. You will get the deserved marks on an honest attempt.***

Section-A
(Answer any three questions)

1. Read the following paragraph as a context, not as the source of all answers.

Software testing is a critical phase in software engineering, ensuring that the product functions as intended and is free from defects. Testing includes various methods such as unit testing, integration testing, system testing (alpha and beta), and acceptance testing, each focusing on different aspects of the software. The goal is to identify and fix bugs, ensuring the software meets user expectations and adheres to quality standards. Maintenance, on the other hand, is an ongoing process that continues after the software has been deployed. It involves fixing issues that arise after release, updating software for compatibility with new systems, and adding new features as required. Both testing and maintenance are essential for maintaining software performance, reliability, and user satisfaction throughout its lifecycle. On the other hand, software project management coordinates activities like planning, executing, and overseeing the development of software projects. It encompasses tasks such as defining project goals, allocating resources, managing risks, setting timelines, and ensuring that the project stays within budget. Effective management helps meet deadlines and deliver quality software on time. A key part of this process is the software requirements specification (SRS), which outlines the functional and non-functional requirements of the software. An SRS document serves as a contract between the stakeholders and the development team, guiding the development process and ensuring that the software meets the user's needs. Clear, detailed specifications are crucial for avoiding misunderstandings and minimizing the risks of scope creep during the project.

(a) Answer in one sentence only

(i) What is the main purpose of software testing?
(ii) What phase follows after software deployment for ensuring continuous improvement?
(iii) Correct the statement- "Beta testing focuses on checking individual components of the software."
(iv) Coordination is the primary goal of software _____. (designer /project management/system analyst)
(v) "Acceptance testing is nothing but testing the software in a real-world environment by the developers only"—Do you agree?

(b) Match the following. No marks will be awarded for partially correct matching

A. System Testing	1. Testing the interactions between integrated components
B. Integration Testing	2. Ensuring the project stays within the allocated financial resources
C. Budget Control	3. Testing as a whole to verify the entire product functions correctly
D. Risk Management	4. Ensuring that project deadlines are met by tracking progress
E. Timeline Management	5. Identifying and mitigating potential obstacles that may impact the project

(5+5=10)

2. Write meaning of the following terminologies briefly. Your statements should be very specific. No marks will be awarded for vague answers.

(a) Horizontal partitioning of a problem (b) Vertical partitioning of a problem (c) Functional abstraction (d) Data abstraction (e) Top-down design (f) Bottom-up design (g) Requirement's review (h) Requirement prioritization (i) Non-functional requirements (j) Volatile requirements

(1×10 = 10)

3. (a) Explain how the Lines of Code (LOC) method is used to estimate the size of a software project.

(b) Write two limitations of LOC?

(c) Describe two common staff organization structures used in software engineering projects. Hence, discuss their impacts in success of a project?

(d) List and explain three key skills that are essential for a good software engineer. How do these skills contribute to software quality?

(2+2+3+3)

4. Consider the following code in C language

```
int f (int N)
{
int sum = 0;
      for (int i = 1; i <= N; i++)
      {
            sum =sum + i;
      }
return sum;

}
```

(a) Consider that execution testing verifies that a code runs without crashing or halting under normal conditions. On the other hand, operation testing checks memory usage of the code. Then what is the result execution testing and operation testing on the given code?

(b) What type of white box testing is performed when in above code **'sum + i'** is replaced by **'sum - i'**? Discuss the impact in result when N=3?

(c) Draw a Control Flow Graph (CFG) on the above code and mention how it is useful in testing?

(d) While performing 'Black Box Testing' on the above code, what is the maximum and minimum value that N can afford to have? Consider size of signed integer is 4 Bytes.

(2+2+3+3)

5. Risk management

(a) Define risk identification and explain why it is a critical step in the risk management process.

(b) Differentiate between risk avoidance and risk reduction with examples.

(c) Give one example the following risks encountered in software development:

(A) Project risk (B)Technical risk (C) Business risk

(d) What kind of risk are these? Justify your answer.

Case A: In a company, a critical team member resigns, causing a delay in feature development.

Case B: A competitor company launches a similar app with better performance and lower pricing before your product's release.

Case C: Bugs in source code

(2+2+3+3)

Section-B
(Mandatory)

6. Choose the correct alternative. No explanation is needed for your answer

(i) Which level of the DIKW pyramid represents raw, unprocessed facts and figures?
(A) Data (B) Information (C) Knowledge (D) Wisdom

(ii) How does software engineering contribute to increased productivity?
(A) By reducing team collaboration (B) By breaking down development into smaller tasks (C) By eliminating the need for communication (D) By focusing solely on coding without planning

(iii) What is the primary purpose of a Software Requirements Specification (SRS) document?
(A) To outline the project timeline (B) To describe the software design and architecture (C) To define the functional and non-functional requirements of the software (D) To manage team workflows and collaboration

(iv) What does legal feasibility primarily evaluate in software engineering? (A) Project timeline (B) Compliance with laws and regulations (C) Software performance speed (D) User interface design

(v) What is a key principle of good user interface (UI) design?
(A) Maximizing the number of clickable options (B) Focusing strictly on graphics over functionality
(C) Providing a simple and easy experience for users (D) Using complex terminology to demonstrate expertise

(vi) In visual programming, programs are typically created
(A) By writing code in text editors (B) By manipulating graphical elements and flowcharts
(C) By compiling machine code directly (D) By using only command-line interfaces

(vii) During coding, what is the most important factor for maintainability?
(A) Writing code as quickly as possible (B) Using complex algorithms without comments
(C) Clear documentation and structured code (D) Skipping unit testing to save time

(viii) Which factor mainly affects software portability?
(A) The number of developers on the project (B) Platform dependencies and system-specific features
(C) The size of the source code (D) The software release date

(ix) Which of the following formulas is used to estimate the effort (E) in PM for the Basic COCOMO?
(A) $E = a \times (KLOC)^b$ (B) $E = a \times (KLOC)^{20}$ (C) $E = (KLOC)^b$ (D) $E = a + b + \sqrt{KLOC}$

(x) How do CASE tools contribute to improving software quality?
(A) By eliminating the need for coding standards. (B) By providing error detection and automated testing features.
(C) By reducing the team size required for development. (D) By outsourcing testing to third parties.

$(1 \times 10 = 10)$

7. Clearly write **True** or **False** for the following statements. No justification is needed for your answer.

(i) Wisdom is the second highest level of the DIKW pyramid, representing the ability to use knowledge effectively and ethically in complex situations

(ii) Software engineering principles make it harder to maintain and update software over time.

(iii) An SRS document is only necessary for small software projects.

(iv) Technical feasibility focuses primarily on user satisfaction and market demand.

(v) The Spiral Model involves iterative development and risk management at every cycle.

(vi) Navigation design is just about the visual appeal rather than ensuring user's efficient movement through an application or website.

(vii) Proper coding practices can reduce the need for extensive debugging.

(viii) High software portability reduces the need for significant code changes when moving to a new platform.

(ix) The formula for development time (TDEV) in the organic COCOMO model is $TDEV = 2.5 \times E^{0.38}$, where E represents the effort in person-months.

(x)
```
void greet (char * name)
{
        printf ("Hello %s", name);
}
```
The above code is only reusable when the code is written in a single file where logic is embedded in main function instead of greet.

(1×10 = 10)

Indian Institute of Engineering Science and Technology, Shibpur

B. Tech. 6th Semester End-Semester Examination, April 2025

Information Security and Cryptography (CS 3204)

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

[Answer question number 1 and any four from the rest]

1. Choose the correct answer from the given options:

(a) Interception causes loss of message _____.

(i) Confidentiality (ii) Integrity

(iii) Authentication (iv) Non-repudiation

(b) Which principle of security is assured using message-digest algorithms?

(i) Confidentiality (ii) Integrity

(iii) Authentication (iv) Non-repudiation

(c) Vigenere Cipher is an example of _____.

(i) Mono-alphabetic Cipher (ii) Poly-alphabetic Cipher

(iii) Homophonic Substitution Cipher (iv) Polygram Substitution Cipher

(d) Rijndael cipher is the name given to _____.

(i) AES (ii) DES

(iii) RSA (iv) None of these

(e) AES uses _____ rounds for 256-bit keys.

(i) 10 (ii) 12

(iii) 14 (iv) 16

(f) The length of input pad (ipad) in HMAC algorithm is _____.

(i) 16 bit (ii) 32 bit

(iii) 8 bit (iv) None of these

(g) Which of the malicious programs don't require host program to replicate?

(i) Trap door (ii) Logic bombs

(iii) Zombie (iv) Trojan horse

(h) Which of the following is a cryptanalysis technique?

(i) Key wrapping (ii) IP spoofing

(iii) IP sniffing (iv) Frequency analysis

(i) The input to the SHA-1 algorithm is divided into blocks of _____ bit for further processing.

(i) 32 (ii) 64

(iii) 256 (iv) 512

(j) A _____ security policy is a security policy developed primarily to provide integrity.

(i) Military (ii) Governmental

(iii) Commercial (iv) None of these

[1 x 10]

2. (a) What is the main mathematical motivation behind RSA algorithm?

(b) What are the limitations of RSA in terms of scalability and performance? Suggest some mitigation strategies for these limitations.

(c) Using RSA, encrypt the message $M = 3$, assuming the two primes chosen to generate the keys are $p = 13$ and $q = 7$. You should choose a value of encryption key $e < 10$. Also find out the value of decryption key d and show the decryption of the encrypted version using d. Show all of your calculations and assumptions.

[1 + (3 + 2) + 4]

3. (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) What is the purpose of the MixColumns operation in the AES algorithm, and why is it omitted in the final round? How does the omission of MixColumns in the final round of AES affect the security of the algorithm?

[2 + 4 + (2 + 2)]

4. (a) A noted computer security expert has said that without integrity, no system can provide confidentiality.

(i) Do you agree? Justify your answer.

(ii) Can a system provide integrity without confidentiality? Again, justify your answer.

(b) What are the properties of message digest? Confidentiality integrity

(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.

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

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

(b) What is hash-based message authentication code (HMAC)?

(c) Suppose that you know the output of an HMAC is X and you know the key K, but you do not know the message M. Can you construct a message M' that has its HMAC equal to X? If so, give an algorithm for constructing such a message. If not, why not?

(d) Write down the disadvantages of HMAC?

[3 + 1 + 3 + 3]

6. (a) What is digital certificate?

What are the contents of this certificate?

(b) Write down the steps of digital certificate creation with proper explanations of the roles of different parties involved therein?

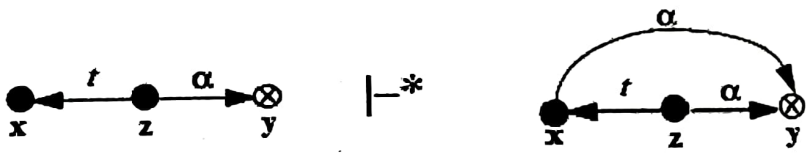
(c) How can we verify a digital certificate?

[(1 + 3) + 4 + 2]

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

(b) State and explain the *de jure* rules for the *Take-Grant Protection Model*. You must show the protection graphs for all the rules.

(c) Let *x*, *y*, and *z* be three distinct vertices in a protection graph. Vertices *x* and *z* represent subjects whereas vertex *y* may be either subject of object. Edges are labelled, and the label indicates the rights that the source vertex has over the destination vertex. Note that *t* is a special right known as *take*.
Now, show the sequence of protection graphs $G_1, \ldots, G_n$ such that $G_1 \vdash^* G_n$ using only *de jure* rules and in G_n there is an edge from *x* to *y* labelled α. You must mention the name of the applied rules in each step.



Indian Institute of Engineering Science and Technology, Shibpur

BTech (CST) 6th Semester Examinations, 2025

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

Full marks: 50 Time: 3 hours

Answer any *five*

1a) Sketch a circuit diagram of CMOS based SRAM cell with minimal number of transistors. Label input, output, access transistor, word lines and bit lines. 4

b) Show and explain the functioning of 3-transistor precharge circuit for SRAM. 2

c) Show a 2x2 array of SRAM that realizes CAM circuit without masking. Explain how match for key 10 can be found when the stored words are 01 and 10. 4

2a) Give sketch of a 2x2 DRAM subarray. Point out the store of a cell, word lines, bit lines and sense amplifier (SA). 3

b) Describe normal read operation of DRAM, following charge sharing, assuming that the cell capacitor is initially charged. 4

c) Following fast parallel mode show how data of first row is copied to second row of the 2x2 DRAM subarray (assume data stored in first and second row are 10 and 01 respectively, before copying). 3

3a) What is TiO2 based memristor? Explain forward and reverse biasing of such memristor. 3

b) What are the RVM, VRM and RRM in memristive design? 3

c) Compare the circuit elements - resistance, capacitance, inductance and memristance in terms of the 4 fundamental circuit variables electric current (i), voltage (v), electrical charge (q) and magnetic flux (φ). 4

4a) Define $P \rightarrow Q$ and memristor-based Material Implication (IMPLY) logic ($P \rightarrow Q$). 2

b) Show how 2-input MAGIC NOR and IMPLY logic based NOR can be realized with minimum 3 and 2 memristors respectively within a crossbar array. 4

c) Show how 2-input MAGIC NAND and IMPLY logic based NAND can be realized with minimum 3 and 3 memristors respectively within a crossbar array. 4

5a) Define bitonic sequence. Check whether the following are bitonic sequence. 2
(i) 11, 12, 14, 17, 16, 10 (ii) 8, 9, 2, 1, 0, 4 (iii) 1, 2, 1, 2 (iv) 14, 10, -6, -4, 0, 1, 2

b) Consider the unsorted list X = 14, 10; -6, -4, 0, 1, 2, 7 and show the execution steps of bitonic sorting scheme to sort X. 4

c) Give a sketch to show how bitonic sorting scheme can be realized in-memory within memristive array. 4

6) Write short notes on the following.

a) Near-memory Processing (NMP), Processing-in-Memory (PIM) and In-memory Computing (IMC) and their working set locations. 5

b) Realization of 2:1 MUX with IMPLY. 5

Indian Institute of Engineering Science and Technology, Shibpur

B. Tech. (CST) 6th Semester Class-Test Examination, 2025

Information Security and Cryptography (CS 3204)

Alok Ranjan
2022CSB091

Time: 1 Hour **Full Marks: 20**

[Answer all the questions]

1. Malware is software that is intentionally malicious, that is, malware is designed to do damage or break the security of a system. Malware comes in many familiar varieties, including viruses, worms, and Trojans.
   a. Has your computer ever been infected with malware? If so, what did the malware do and how did you get rid of the problem? If not, how have you been so lucky?
   b. In the past, most malware was designed to annoy users. Today, it is believed (with good evidence) that most malware is written for profit. How could malware possibly be profitable?

[2 + 2]

2. What is Phishing attack? Explain different types of Phishing attacks in brief.

[2 + 3]

3. Why do MD5 and SHA-1 require padding of messages that are already a multiple of 512 bits?

[2]

4. Message digests are reasonably fast, but here's a much faster function to compute. Take your message, divide it into 128-bit chunks, and XOR all the chunks together to get a 128-bit result. Do the standard message digest on the result. Is this a good message digest function? Give reasons in support of your answer.

[3]

5. Cryptographic operations can be very slow, especially for large numbers. One of the operations we need to perform 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 steps of your approach with a suitable example.

[3]

6. Computerized voting would become quite common in the next few decades. As such, it is important that the protocol for virtual elections should protect individual privacy and should also disallow cheating. Now, design a secure protocol that provides comfort both to the voters as well as to the Election Authority by preventing fake and duplicate votes. Also prove the correctness of your design by explaining the logic behind each and every steps of your virtual election process.

[3]