

Premier University
Department of Computer Science and Engineering
6th Semester (B.Sc.) Midterm Examination, Spring 2025
Course Title: Computer and Cyber Security Course Code: CSE 3637

Time: 45 mins

Marks: 20

NB: Answer any of two (2) from the following three (3) questions. Each question carries equal marks.

- | | | | | |
|---|-----|--|---|-----|
| 1 | (a) | Explain the three principles of the CIA (Confidentiality, Integrity, and Availability) Triad in information security. For each principle, describe its definition, importance, and provide one example of a security measure that supports it. | 5 | CO1 |
| | (b) | Using the Playfair cipher with the key "EXAMPLE", encrypt the message "HIDE THE GOLD". Show all the steps involved in the encryption process. | 5 | CO2 |
| 2 | (a) | Which security services are involved when an individual signs a completed credit card application form? Explain in detail. | 5 | CO1 |
| | (b) | Given $a = 13$, $b = 17$, and modulus $m = 60$, check if a and m are relatively prime using prime factorization, then calculate $a^b \bmod m$ using modular exponentiation. | 5 | CO2 |
| 3 | (a) | Describe the key differences between stream cipher and block cipher in terms of encryption process, speed, and security. | 5 | CO1 |
| | (b) | Explain the Key Generation, Encryption, and Decryption of the DES algorithm in detail. | 5 | CO2 |

Premier University
Department of Computer Science and Engineering
Midterm Examination
Session: Spring 2025
6th Semester (B.Sc.) (Section: C & D)

Course: Project Management and Entrepreneurship Course Code: MGT 3301

Time: 45 Minutes

Marks: 20

Answer any two of the following questions-

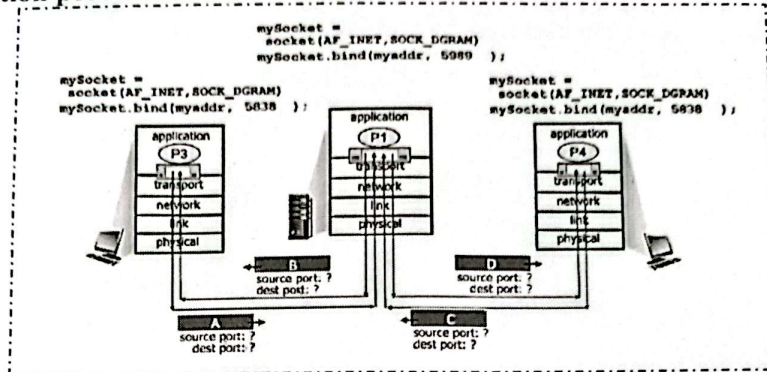
1. a)	What do you mean by entrepreneur and entrepreneurship?	3	CO1
b)	Define Social Entrepreneurship with examples.	3	CO1
c)	What is Entrepreneurial mindset? Differentiate between Fixed mindset and Growth mindset.	1+3	CO1
2.a)	'Entrepreneurial process has four distinct phases' explain those phases.	5	CO1
b)	Briefly describe the legal and regulatory aspects of entrepreneurship.	5	CO1
3. a)	Define project and project management. Distinguish between Project and Operations.	2+1	CO2
b)	What is SWOT analysis? Describe the key components of a SWOT analysis with example.	5	CO2
c)	What is Kanban?	2	CO2

Total Marks: 20

Answer any two question sets

Time: 45 mins.

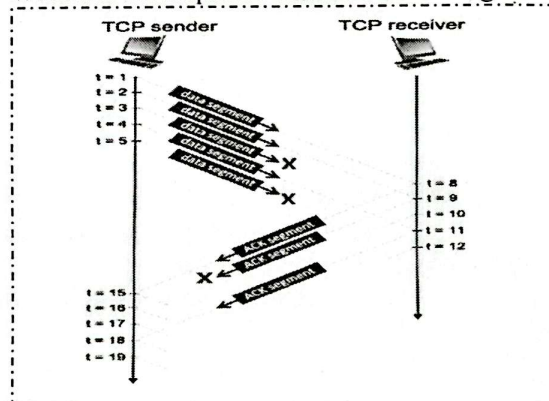
- 1(a) How does a transport layer protocol deliver a received packet to the correct process? Use connectionless demultiplexing to find the source port and destination port numbers. 2+2



- 1(b) What are the advantages of UDP? List down the services provided by TCP. 2+2
 1(c) Write short note on TCP three-way handshake. 2

- 2(a) In the following communication, suppose, the initial value of the sequence number is 71 and every segment contains 887 bytes. Assuming there are no timeouts and any out of order segments received are thrown out, answer the following questions: 3

- What are the sequence numbers of the segment sent at $t=3$ and $t=4$?
- What are the values of the ACK sent at $t=10$ and $t=11$?
- What are the sequence numbers of the segment sent at $t=16$ and $t=17$?



- 2(b) Define sequence number and acknowledgements? How can you use sequence number and ACK to ensure reliable communication? 2+2
 2(c) Define Explicit Congestion Notification (ECN)? Define TCP retransmit scenario where cumulative ACK covers for earlier lost ACK. 1+2
 3(a) Explain how TCP slow start avoids congestion. Why is checksum used in transport layer communication? Explain with an example. 2+3
 3(b) Suppose that TCP's current estimatedRTT and DevRTT are 370 msec and 36 msec, respectively. Suppose that the next three measured values of the RTT are 350 msec, 210 msec, and 370 msec respectively. Compute TCP's new value of DevRTT, estimatedRTT, and the TCP timeout value after each of these three measured RTT values is obtained. Use the values of $\alpha = 0.125$, and $\beta = 0.25$. 5

Premier University

Department of Computer Science and Engineering

6th Semester (B.Sc.) Midterm Examination, Spring 2025

Course Title: Software Engineering

Course Code: CSE - 3233

Time: 45 mins

Marks: 20

Instructions:

- (a) Answer any two questions.
- (b) Each question carries equal marks.

- Q-1** A city deploys thousands of IoT sensors (hardware) and an AI-driven traffic management system (software). Over time, both hardware and software experience failures. Using your understanding of hardware and software failure curves, explain the expected failure patterns, why early failures might be unusually high, and suggest strategies to reduce failures and improve system reliability. **10 CO2**
- Q-2** A company is developing a large-scale software system with evolving requirements. Using your knowledge of Waterfall, Spiral, Incremental, and Prototype models, explain the strengths and weaknesses of each, identify which model would be most suitable for this project, and suggest strategies to handle early challenges while ensuring timely and reliable software delivery. **10 CO2**
- Q-3** A project manager is assigning tasks to a software development team. Using your understanding of task sets and task dependencies, explain how you would organize the tasks to maximize efficiency, avoid conflicts, and ensure timely completion. Discuss potential challenges if tasks are interdependent and suggest strategies to manage them effectively. **10 CO2**

Premier University
Department of Computer Science and Engineering
6th Semester (B.Sc.) Midterm Examination, Spring 2025

Course Title: Data Communication

Course Code: CSE - 4427

Time: 45 mins

Marks: 20

Instructions:

- (a) Answer any two questions.
- (b) Each question carries equal marks.

- | | | | |
|-----|--|-----|-----|
| Q-1 | a. Briefly describe the components of a data communication system. | 3.5 | CO1 |
| | b. Explain the three types of data flow mechanisms in data communication with suitable examples. | 3 | CO1 |
| | c. What are the key factors that you need to consider to estimate the performance of the communication networks? | 2 | CO1 |
| | d. A digital signal has 29 levels. How many bits are needed per level? | 1.5 | CO2 |
-
- | | | | |
|-----|---|---|-----|
| Q-2 | a. Differentiate between the throughput and capacity. The loss in a cable is usually defined in decibels per kilometer (dB/km). If the signal at the beginning of a cable with -0.3 dB/km has a power of 2 mW, what is the power of the signal at 5 km? | 3 | CO1 |
| | b. A non-periodic composite signal has a bandwidth of 168 KHz, with a middle frequency of 276 kHz and peak amplitude of 22 V. The two extreme frequencies have an amplitude of 15V. Draw the frequency domain of the signal. | 2 | CO2 |
| | c. We have a channel with a 1000 Hz bandwidth. The SNR for this channel is 127; what is the appropriate bit rate and signal level? | 4 | CO2 |
| | d. Estimate the values of SNR and SNR_{dB} for a noiseless channel. | 1 | CO2 |
-
- | | | | |
|-----|--|---|-----|
| Q-3 | a. Represent the following signal using NRZ-I, RZ, Manchester, and bipolar AMI encoding. | 5 | CO3 |
|-----|--|---|-----|
- NRZ-L
- | | | | |
|----|---|---|-----|
| b. | Write the names of three factors that control the data rate. | 2 | CO2 |
| c. | Briefly explain the transmission impairments in data communication. | 3 | CO2 |

Premier University
Department of Computer Science and Engineering
7th Semester (B.Sc.) Midterm Examination, Spring 2025
Course Title: Network and Computer Security
Course Code: CSE - 437

Time: 45 mins

Marks: 20

Instructions:

- (a) Answer any two questions.
- (b) Each question carries equal marks.

- Q-1 ~~1~~ Define the three primary goals of network security. Describe three different attacks that threaten data integrity, and explain how each attack violates this property. 2+2 CLO1
- b. Explain why the additive cipher is also known as the shift cipher and the Caesar cipher. 2+4 CLO2
While working on a project, you receive an encrypted message "BADIA NQEIT AW" from your teammate. They inform you that the message was encrypted using multiplicative cipher with a key value of 15. Decrypt the message to obtain the original plaintext. Show all intermediate steps.
- Q-2 a. Illustrate the basic structure of the Data Encryption Standard (DES). 05 CLO2
- b. For each of the following situations, describe the type of security attack and which security goal it threatens. 05 CLO1
- i) You send an important project file to your colleague. Later, you hear from another department that they know the exact contents of that file, even though you never shared it with them.
 - ii) You transferred ₹5,000 to your friend's account, but when they checked, the amount received was not what you sent.
 - iii) You receive an email from what appears to be your company's HR department asking for your personal details. Later, you discover that no such request was made by HR.
 - iv) You purchased a phone from an e-commerce site but later told the seller you never placed the order, even though you did.

- v) You try to register for your courses online, but the site keeps showing "Service unavailable" messages for hours.

- Q-3 a. Differentiate between **Stream Ciphers** and **Block Ciphers** with an example. Explain why the Vigenere cipher is considered a type of stream cipher 2+2 CLO2
- b. You are a security officer at Cybersecure Ltd., where all confidential communications are encrypted using the **Playfair Cipher**. The company's agreed keyword is **CRYPTO**, and the letter **J** is treated as **I** in the key matrix. Today, you receive the plaintext message from your colleague: "**WE ARE DISCOVERED**". Your task is to encrypt this message using the Playfair cipher so it can be transmitted securely over an insecure network. Draw the Playfair table and show all intermediate steps, including preprocessing and encryption. 06 CLO2