Roll No: | | | | | | | | | | | |

GAIN MORE KNOWLEDGE
REACH GREATER HEIGHTS

PRESIDENCY UNIVERSITY

Presidency University Act, 2013 of the Karnataka Act No. 41 of 2013 | Established under Section 2(f) of UGC Act, 1956
Approved by AICTE, New Delhi | Approved By BCI
Bengaluru

Mid Term Examinations - October 2026

Date: 05/10/2026 **Time:** 09:30 AM - 11:00 AM

Course Code: CBC3400 **Course Name:** Cryptography and Security in Blockchain

Semester: Fifth Semester **Max. Marks:** 50 **Weightage:** 50%

CO - Levels	CO1	CO2
Marks	46	44

PART A: Answer Following Questions. 10 M

Q.N.	Questions	M	CO	BT
1	**What is a digital signature? Name the algorithm used by Bitcoin and Ethereum for it.**	2	CO1	BT1
2	**Write any two reasons why ECC is preferred over RSA in blockchain.**	2	CO1	BT1
3	**What is a smart contract? Give a daily life example.**	2	CO1	BT1
4	**What is a mining pool? Write one benefit of joining a mining pool.**	2	CO2	BT1
5	**A DPoS network has 1,000 token holders and only 10% of them vote. How many votes are cast? How many votes give a majority of the votes cast? What percentage of all token holders is that?**	2	CO2	BT3

PART B : Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
6	**Explain the lifecycle of a blockchain transaction step by step. Also explain why consensus is needed.**	10	CO1	BT2
7	**Four blocks are linked using hashes (each block stores the previous block's hash). An attacker changes a payment in Block 2 from ₹500 to ₹5,000. (i) Explain what happens to Block 2, Block 3 and Block 4. (5 marks) (ii) Name the hash property responsible for this. (1 mark) (iii) Why is blockchain called tamper-evident, not tamper-proof? (2 marks) (iv) What must the attacker do to hide the change? Why is it hard? (2 marks)**	10	CO1	BT3

PART C: Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
8	**Explain how a digital signature works in a blockchain transaction, with a diagram. State what it provides and what it does not provide.**	10	CO1	BT2

9	**(i) Alice sends a secret message to Bob using asymmetric cryptography. Which key encrypts and which key decrypts? (2 marks)** **(ii) Alice signs a transaction. Which key signs and which key verifies? (2 marks)** **(iii) Symmetric keys needed for n users = n(n−1)/2. Find this for 10, 50 and 100 users. (3 marks)** **(iv) How many key pairs are needed with asymmetric cryptography for the same users? Why does it scale better? (3 marks)**	10	CO1	BT3

PART D: Answer Any 1 Following Questions. 10 M				
Q.N.	**Questions**	**M**	**CO**	**BT**
10	**Explain PBFT. Include the meaning of a Byzantine node, the roles (client, primary, replicas), the message phases with a diagram, and view change.**	10	CO2	BT2
11	**(i) A PBFT network has n = 16 nodes. Find the maximum number of faulty nodes f it can tolerate. (2 marks)** **(ii) Find the minimum number of nodes needed to tolerate f = 1, 2, 3 and 5 faulty nodes. (4 marks)** **(iii) A student says, "PBFT can tolerate up to half of the nodes being malicious." Is this correct? Explain using n = 7 nodes. (4 marks)**	10	CO2	BT3

PART E: Answer Any 1 Following Questions. 10 M				
Q.N.	**Questions**	**M**	**CO**	**BT**
12	**What is a fork? Differentiate hard fork and soft fork (any four points). What is replay protection? What are orphan blocks – are they always caused by attacks?**	10	CO2	BT2
13	**(i) Define the following, stating the size of each: bit, byte, word, block size, and State. (3 marks)** **(ii) How many rounds does AES perform, and how many steps are there in each round? Name the four steps, in order. (3 marks)** **(iii) Draw the input array (4×4) for a 128-bit block, and show how it maps to the State array (label the bytes S_{00} to S_{33}). (2 marks)** **(iv) With a simple block diagram, show the overall structure of AES encryption — from the 128-bit plaintext, through the Pre-round Transformation, Round 1 to Round 10, to the 128-bit ciphertext. Also show where Key Expansion supplies keys (W_0–W_3, W_4–W_7, …, W_{40}–W_{43}) to each stage. (2 marks)**	10	CO2	BT3