Roll No.												

PRESIDENCY UNIVERSITY

BENGALURU

End - Term Examinations – MAY 2025

Date: 29-05-2025 **Time:** 09:30 am – 12:30 pm

School: SOCSE	**Program:** B. Tech CBC	
Course Code: CSE3345	**Course Name:** Blockchain Security and Performances	
Semester: VI	**Max Marks**: 100	**Weightage**: 50%

CO - Levels	CO1	CO2	CO3	CO4	CO5
Marks	38	36	26	-	-

Instructions:

(i) Read all questions carefully and answer accordingly.

(ii) Do not write anything on the question paper other than roll number.

Part A

Answer ALL the Questions. Each question carries 2marks. **10Q x 2M=20M**

1.	Define a double-spending attack and its impact on blockchain transactions.	**2 Marks**	**L1**	**CO1**
2.	Identify the purpose of mixing (coin tumbling) in blockchain transactions.	**2 Marks**	**L1**	**CO1**
3.	Construct a python code snippet to create a class named Block including the attributes.	**2 Marks**	**L3**	**CO1**
4.	Define homomorphic encryption and its role in blockchain security.	**2 Marks**	**L1**	**CO1**
5.	What is the purpose of public key cryptography?	**2 Marks**	**L1**	**CO2**
6.	Define an elliptic curve digital signature algorithm (ECDSA).	**2 Marks**	**L1**	**CO2**
7.	What is Keccak-256?	**2 Marks**	**L1**	**CO2**
8.	Compare UTXO and Account-based transaction models.	**2 Marks**	**L2**	**CO3**
9.	Define Tamper-resistance in the context of blockchain.	**2 Marks**	**L1**	**CO3**
10.	What is pseudonymity in blockchain?	**2 Marks**	**L1**	**CO3**

Part B

Answer the Questions. **Total Marks 80M**

11.	**a.**	Examine how coin mixing (tumbling) enhances privacy and security in blockchain transactions. Discuss its functioning, benefits, challenges, and practical applications.	**10M**	**L4**	**CO1**
	b.	Discriminate the implications of smart contract vulnerabilities leading to cyber-attacks, providing examples and possible solutions.	**10M**	**L4**	**CO1**
		Or			

12.	**a.**	Explain the working of Non-Interactive Zero-Knowledge (NIZK) proofs in blockchain transactions with suitable examples.	**10M**	**L6**	**CO1**
	b.	Analyze how anonymous signatures enhance transaction privacy in blockchain with examples.	**10M**	**L4**	**CO1**

13.	**a.**	Construct and demonstrate a simple consensus algorithm. i) Simulate Proof of Work (PoW) or Proof of Stake (PoS). ii) Validate the chain by achieving consensus among multiple nodes.	**10M**	**L6**	**CO1**
	b.	Create a program to generate a Bitcoin address and validate its checksum.	**10M**	**L6**	**CO2**
		Or			
14.	**a.**	Create a program to Simulate and Detect Vulnerabilities in Blockchain Client Interactions. i) Create scenarios for potential attacks like phishing or keyloggers. ii) Demonstrate secure key management techniques.	**10M**	**L6**	**CO1**
	b.	To implement a simple demonstration of inter-exchange address format validation using Protocol (IXCAP).	**10M**	**L6**	**CO2**

15.	**a.**	Explain the different types of cryptographic techniques and their applications. Describe the role of cryptographic hash functions in securing digital data.	**10M**	**L**	**CO2**
	b.	Explain the working of Public Key Cryptography with an example. Describe the process of key generation and management in Public Key Cryptography.	**10M**	**L2**	**CO2**
		Or			
16.	**a.**	How does digital signature work in blockchain? Explain its importance in cryptographic security.	**10M**	**L1**	**CO2**
	b.	Explain the principles of Elliptic Curve Cryptography (ECC) and its advantages over RSA.	**10M**	**L2**	**CO2**

17.	**a.**	Explain the UTXO transaction model with an example. Discuss its benefits and limitations.	**10M**	**L2**	**CO3**
	b.	Interpret the CAP theorem and analyse its applicability to blockchain systems with real-world examples.	**10M**	**L5**	**CO3**
		Or			
18.	**a.**	Analyse the scalability challenges in both UTXO and Account-Based models. What are the proposed solutions to overcome these issues?	**10M**	**L4**	**CO3**
	b.	Explain how privacy-enhancing technologies like zk-SNARKs and ring signatures are integrated into blockchain. Discuss their impact on transaction confidentiality.	**10M**	**L2**	**CO3**