Roll No.												

PRESIDENCY UNIVERSITY

BENGALURU

Mid - Term Examinations – October 2025

Date: 28-10-2025 **Time:** 11.00am to 12.30pm

School: SOCSE	**Program:** IST	
Course Code : CSE3022	**Course Name:** CRYPTO CURRENCY TECHNOLOGY	
Semester: VII	**Max Marks**: 50	**Weightage**: 25%

CO - Levels	**CO1**	**CO2**	**CO3**	**CO4**	**CO5**
Marks	**26**	**24**	**-**	**-**	**-**

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. **5Q x 2M=10M**

1	Describe collision-resistance in the context of cryptographic hash functions.	**2 Marks**	**L**	**CO1**
2	Identify the three algorithms that make up a digital signature scheme?	**2 Marks**	**L**	**CO2**
3	Describe a message digest and discuss its relation to cryptographic hash functions?	**2 Marks**	**L**	**CO1**
4	Explain why storing only the latest block's hash is enough to detect tampering in a blockchain?	**2 Marks**	**L**	**CO2**
5	Discuss about "nonce" in the context of commitment schemes?	**2 Marks**	**L**	**CO1**

Part B

Answer the Questions. **Total Marks 40M**

6.	**a.**	Summarize digital signatures and discuss how the unforgeability game defines their security.	**10 Marks**	**L**	**CO1**
	b.	Describe GoofyCoin's mechanism and analyze its security flaw showing the double-spending challenge in cryptocurrencies.	**10 Marks**	**L**	**CO1**
		Or			
7.	**a.**	Discuss why a reliable source of randomness is vital in ECDSA and how poor randomness can compromise key generation and signature security	**10 Marks**	**L**	**CO1**
	b.	Describe how cryptography ensures security in cryptocurrencies and compare its use with traditional encryption.	**10 Marks**	**L**	**CO1**

8.	**a.**	Describe the components of a digital signature and discuss how the unforgeability game validates its security.	**10 Marks**	**L**	**CO2**
	b.	Distinguish cash-based and credit-based systems and discuss their advantages, drawbacks, and relevance to online payments.	**10 Marks**	**L**	**CO2**
		Or			
9.	**a.**	Explain how public keys serve as identities in decentralized systems, noting their benefits and related privacy concerns.	**10 Marks**	**L**	**CO2**
	b.	Discuss how hash pointers make a blockchain tamper-evident and discuss why altering data within the chain would fail.	**10 Marks**	**L**	**CO2**