Indian Statistical Institute

Mid-Semestral Examination
M.Tech.(CrS)-II

Blockchains & Cryptocurrencies

Date: 09.09.2025 **Duration: 2 hours** **Max marks: 30**

Only precise and to the point answer will get full mark(s).

1. Define agreement problem. Explain the notion of implicit and explicit agreement. Suppose A be a multi-valued agreement protocol which takes a constant number of rounds and $O(n)$ messages, where n is the number of nodes in the network. Design an explicit agreement protocol which takes $O(1)$ rounds and $O(n)$ messages. Analyze the correctness and complexity of your protocol. [3+3+6]

2. Design and analyze any Byzantine agreement protocol that you learned in the classroom. State all the necessary assumptions. [10]

3. Define a blockchain protocol. Design a blockchain protocol using Dolev-Strong Reliable Broadcast (RB) protocol and argue its correctness. Calculate the confirmation time of the blockchain protocol, given that the adopted RB protocol adopted realizes Multi-Valued Reliable Broadcast for a n-node distributed system, tolerating up to f failures.

[3 + 6 + 3]

– END of the Question Paper –