

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -2 EXAMINATION- APRIL - 2023

B.Tech-VIII Semester (BT/BI)

COURSE CODE: 19B1WCI839

MAX. MARKS: 25

COURSE NAME: Foundation of Blockchain

COURSE CREDITS:

MAX. TIME: 1 Hour 30 Min

*Note: All questions are compulsory. Marks are indicated against each question in square brackets.*

- Q1.  
CO1
- Consider a situation in which you want to expand the key of the AES that affects total rounds; explain the whole concept with a suitable diagram. Mention the possible challenges of the Symmetric Key Cryptography. [4]
- Q2.  
CO2
- i. Blockchain is a decentralized network so how nodes achieve the consensus among each other to maintain the consistent state of the distributed ledger. And mention the strategy to deal when an adversary is trying to propose a forgery block in the network. [4x3]
- ii. Multiple miners can come up with the new block then how blockchain will keep consistent state by adopting only one block and ignore the rest.
- iii. Specify the block structure of the Bitcoin blockchain with description of individual fields.
- Q3.  
CO3
- i. A game theory is very important for the blockchain, define the state of Nash Equilibrium with proper example. [3x2]
- ii. Suppose we construct a transaction-chain instead of blockchain then what could be the possible issues encountered.
- iii. The size of the blockchain increases regularly and it is more than 200GB. It is complex for the miners to verify and validate the transactions faster to make network efficient. To overcome this issue which data structure is used to verify the transaction more easily and even by light node.
- Q4.  
CO3
- Blockchain is very computationally intensive kind of technology, so it is designed for small amount of data but we are also using it in many heavy loaded applications and that can create an issue of scalability. Therefore, mention both approaches to counter the issue of scalability. [3]