BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE, PILANI
DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION SYSTEMS

BLOCKCHAIN TECHNOLOGY (BITS F452)
FIRST SEMESTER 2023 - 24
MID-SEMESTER EXAMINATION
(CLOSED BOOK)

Maximum Marks: 30
Time: 90 minutes

Instructions:

1. Answer all the parts of a question together in the answer sheet. Answers at separate places will not be accepted.
2. Do not write any information irrelevant to the question.

Q.1. Consider the following (flawed) authentication protocol, where s_A denotes the signature operation of party A, and it is assumed that all parties have authentic copies of all others' public keys.

$$
\begin{array}{lcll}
A & & B & \\
\rightarrow & r_A & & (1) \\
& r_B, s_B(r_B, r_A, A) & \leftarrow & (2) \\
\rightarrow & r_{A'}, s_A(r_{A'}, r_B, B) & & (3)
\end{array}
$$

The intention is that the random numbers (r_A, r_B) chosen by A and B, together with the signatures, provide a guarantee of freshness and entity authentication. However, an enemy E can initiate one protocol with B (pretending to be A), and another with A (pretending to be B), to successfully deceive B into believing E is A (and that A initiated the protocol).

a) Provide detailed steps of the attack by writing down the sent messages in the same form as for the original protocol above. Note that in the attack a few more messages have to be exchanged. [5 M]

b) Propose a simple modification of the above protocol to prevent this attack. [2 M]

Q.2. Explain how Proof-of-Stake (PoS) consensus algorithm achieves *safety* and *liveness* in a public blockchain network? Support your answer with example(s). [6 M]

Q.3. What are the population and target hash sets? Compute the probability that a random hash value is within the limit by considering that the difficulty level for the mining process is set to have "twenty-four leading zeros" in the 64-digit hexadecimal hash. [2 + 4 = 6 M]

Q.4. Answer the following:

a. What is contest-driven decentralization? Explain the requirements to have a decentralized system. [2 M]

b. Differentiate between public, private, consortium, and hybrid blockchains with respect to users and verification entities in these networks. [3 M]

Q.5. Answer the following:

a. Why bitcoin scripts are Turing incomplete? [1 M]

b. Let us consider that Alice is looking to transfer a payment of 0.015 BTC to Bob's Café using P2PKH. When Alice makes a payment to cafe's bitcoin address, a locking script is created in the below form:

```
OP_DUP OP_HASH160 <cafe_pubkeyhash> OP_EQUALVERIFY OP_CHECKSIG OP_1
OP_ADD OP_2 OP_EQUAL
```

What should be the unlocking script for the Bob's Cafe to receive UTXO from Alice? Provide process steps and outcome of the complete script functioning at Bob's Cafe. [5 M]

[---------- END OF QUESTION PAPER ----------]