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

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

Maximum Marks: 40
Time: 3 hrs

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.
3. Assumptions, if any, should be stated at the beginning of the answer.

Q.1. John's cafeteria offers a special deal to avail free goodies by solving a crypto puzzle. The puzzle includes a bitcoin locking script which if unlocked properly can have tokens sent to those bitcoin addresses (that provide correct unlocking script). The lock script is mentioned below.

```
OP_2DUP OP_EQUAL OP_NOT OP_VERIFY OP_SHA1 OP_SWAP OP_SHA1 OP_EQUAL
```

a) What should be the corresponding unlock script to obtain tokens to avail free goodies at John's cafeteria? Explain your answer with a clear reasoning for script formulation using stack-based processing. [3 M]

b) Does the unlock script resemble an attack category? Explain. [2 M]

Opcodes OP_2DUP and OP_SHA1 duplicates the top two stack items and hashes the input using SHA-1 respectively. OP_NOT complements the input if it is 0 or 1. Otherwise the output remains 0. OP_EQUAL returns 1 if the inputs are exactly equal, otherwise 0. OP_VERIFY marks a transaction as invalid if the top stack value is not true. The top stack value is removed as well. OP_SWAP exchanges top two stack items.

Q.2. The bitcoin script opcode OP_RETURN marks the script as invalid, guaranteeing that no scriptSig exists that could possibly spend that output. Considering the scriptPubKey as OP_RETURN, what will be its effect on:

a. UTXO set [2 M]
b. Transactions set in local memory pools [1 M]
c. Briefly explain whether such transactions cost mining fees or not [2 M]

Q.3. Consider the following signature scheme:

Let Z_q represents a group of positive integers under modulo q where all elements of the group can be generated by one or more integers (of the same group) using some arithmetic operation, q is a large prime number and g is the generator for Z_q. A user has a private key α and a public key $X = g^{\alpha}$. To sign a message m, one first computes $h = H(m)$ for some hash function H. Then one computes $z = \alpha/h$ (assuming $h \neq 0$). The signature is $s = g^{\bar{z}}$. Verification of the signature s consists of checking whether $s^h = X$.

a. Will correct signatures be accepted in the given signature scheme? If yes, describe the procedure for the same, otherwise explain the flaw in the protocol. [3 M]
b. Is it possible to sign an arbitrary message without knowing α? Explain. [1 M]

Q.4. The block cipher divides the plaintext into multiple blocks and converts them to ciphertext block-by-block, where different keys can be used in each block. Consider a message digest scheme based on a block cipher E_k of block size n and a hash function h with output size n. The message digest generation works as follows:

i) For any message m of size $N > n$, the message digest is computed as $MD(m) = E_k(h(m))$
ii) For messages of size exactly n compute $MD(m) = E_k(m)$

a. Show that this message digest scheme is not secure. [3 M]
b. How the given scheme can be secured? [1 M]

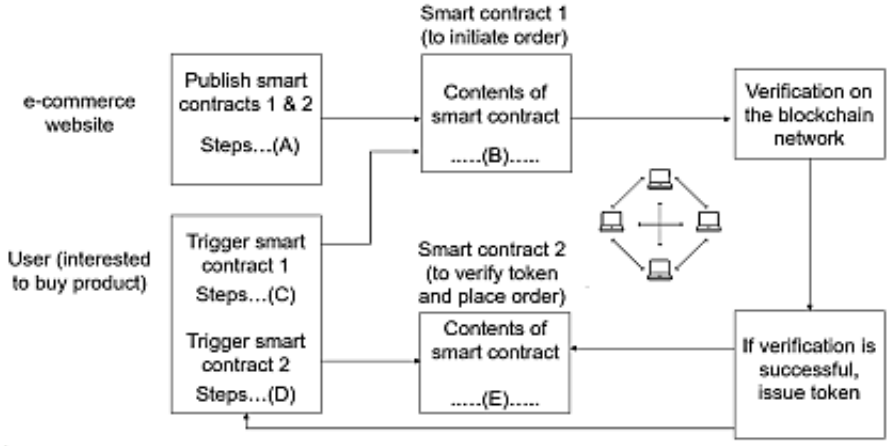
Q.5. Answer the following:

a. How is a node's overall score identified in Proof-of-Importance (PoI)? [2 M]
b. Explain how a block is finalized in Ethereum? [2 M]
c. Why is an orderer node different from a ledger peer in Hyperledger fabric? Explain your answer with an example. [3 M]
d. With reference to lifecycle, explain how chaincode and endorsement policies are upgraded in Hyperledger fabric 1.x? What is the effect of upgradation on ledger state? [3 M]

Q.6. Let us assume that each block in Ethereum has a target size of 15 million gas. The block limit is 30 million gas and an increase in base fees is fixed to 12.5%. The first block is added to the network with the base fees of 500 gwei after consuming 15 million gas. After that, four consecutive blocks are added with their gas requirements as 15, 30, 30, and 15 million respectively.

a. What will be the base fees for the sixth block that comes with 30 million gas? [4 M]
b. Considering the same trend as given above for every six blocks in the Ethereum network, at which block number the base fees reach out to 900.99? [1 M]

Q.7. An e-commerce business website specializes in selling five different items for a particular business domain. The website is available publicly and processes online orders through prepaid tokens only. A user seeking a product from the website needs to obtain a token and get verified through the blockchain network. The below diagram illustrates the functioning of the system where e-commerce website and users are supposed to come together for agreement/ verification of smart contracts and orders for successful delivery of the product.



You are required to fill in the missing entries in places represented by A, B, C, D, and E so that the complete functioning of the system can be availed. Do not use simple story sentences to describe each entity's functioning. The answer should be precise and use only relevant information such as simplified and meaningful pseudocodes or specific statements. [7 M]

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