KFUPM
College of Computer Science and Engineering
Computer Engineering Department
COE 449: Privacy Enhancing Technologies

Fall 2019 (191)

Assignment 4: Due date Tuesday 17/12/2019

Question1: Merkle Hash Tree (20 pts)

(a) Construct a binary Merkle tree for data blocks $D_i \ \forall i \in [1, 16]$. In your tree, represent the hash of each block with $Hash(D_i)$. Similarly, represent the hash of each node with $Hash(N_i)$, where N_i is the i^{th} node in the tree.

(b) Given block D_6, list the set of hash values needed to validate the integrity of D_6.

Question2: Bitcoin Fundamentals (40 pts)

Read the Bitcoin white paper [1] and answer each of the following questions in your own words.

(a) Explain how Bitcoin addresses the double-spending problem

(b) Explain how Bitcoin deters denial of service attacks or other service abusers

(c) Explain how does Bitcoin incentivize nodes to mine on the network

[1] `https://bitcoin.org/bitcoin.pdf`

(d) Explain how does Bitcoin deal with fork chains