Exercise-4

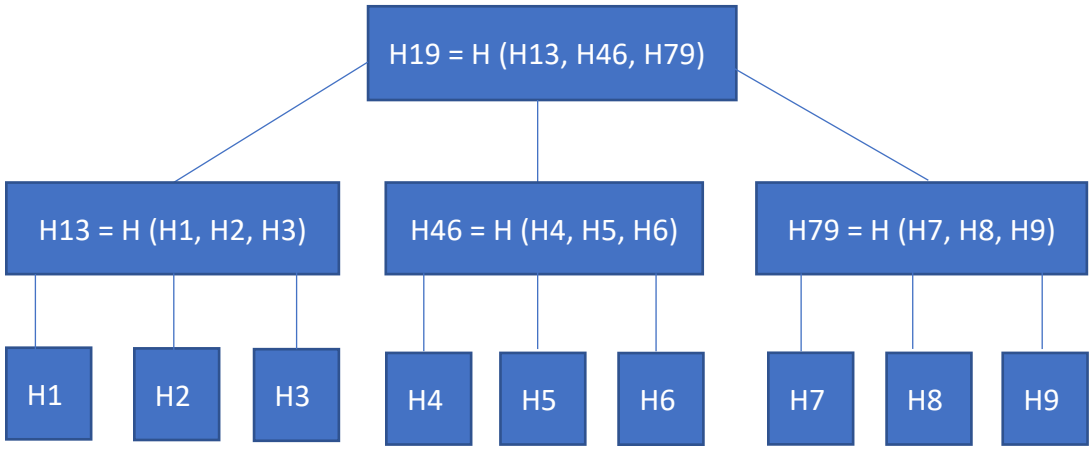
Vineeth Mylavarapu
ID.801337050
College of Computing and Informatics

Question-1

A company uses the Merkle's hash tree to provide time-stamp service. Every customer can send the hash result that she/he wants to timestamp to the company. The company will combine all the hash results and construct a hash tree so that it needs to publish only one value on the local newspaper. Now please answer:

- One day the company receives 9 hash values for the timestamp service. Please draw the structure of the 9-leaf-node Merkle's hash tree. Different from the previous homework, the newspaper does not use binary tree. On the contrary, each parent node has three children. Make sure that you show very clearly: (1) how the value of the parent node is calculated from the children; and (2) which value will be published on the newspaper.
- Use your tree structure, please identify the smallest set of leaf and intermediate level nodes that the company needs to provide to customer #7 so that she/he can verify that her/his hash value is included

A.



Merkle's hash tree for the given scenario

a. The customers C1 to C9 have supplied us with the respective hashes H1 to H9.
We first taken the first-tier hashes H13, H46, and H79, and then we considered the final hash H19 by taking the hash of H13, H46, and H79, where H19 will be publishing Newspaper.
b. For customer C7 to confirm that their hash has been included in the final outcome, they must have knowledge of H8, H9, H13, and H46.