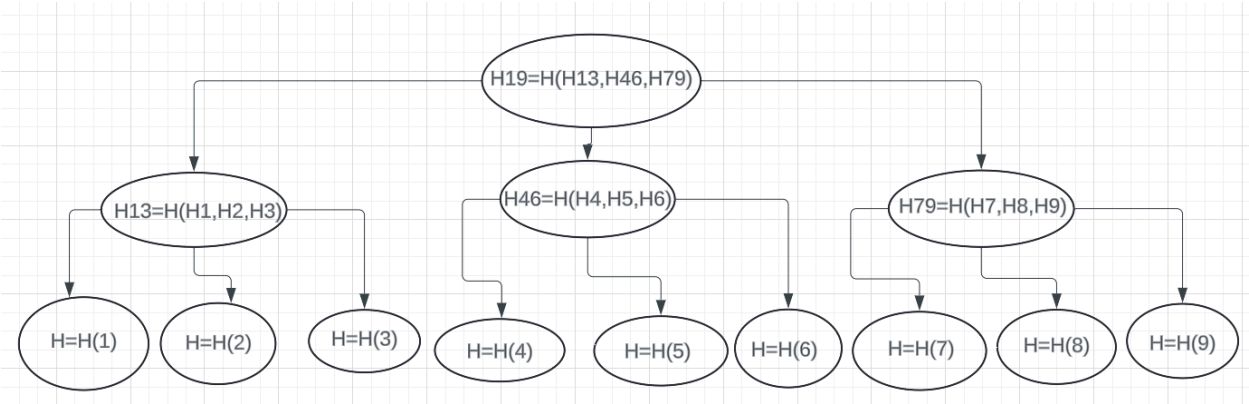
ITIS6200 EXERCISE: 04-Q1

Amaan syed (asyed15@uncc.edu)

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.**
  - **(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.**



- Customers C1, C2, C3, C4, C5, C6, C7, C8, C9 provide us with hashes H1, H2, H3, H4, H5, H6, H7, H8, H9 respectively. We calculate the first level of hashes H13, H46, H79 and then we calculate the final level of H19=H(H13, H46, H79) The newspaper will publish H19.

- If customer 7 wants to verify their value's inclusion in the published hash, the minimal set of nodes needed at both the leaf and intermediate levels would be H8, H9, H13, and H46, as provided by the company. Using these, customer 7 would first compute H79, then use H13 and H46 to calculate the published hash value, H19.