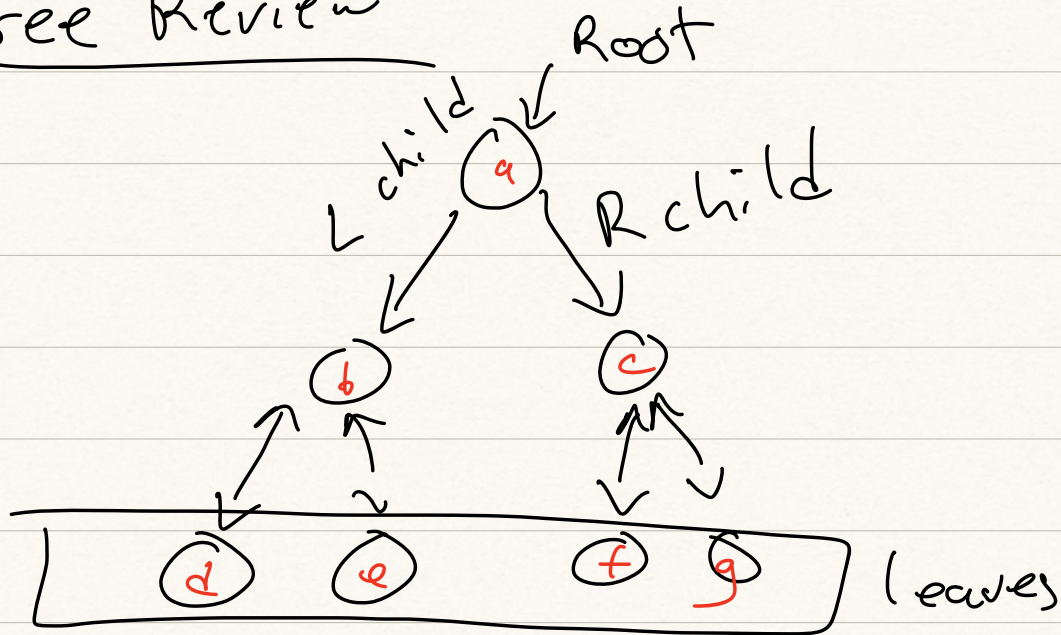


Merkle Trees

Tree Review



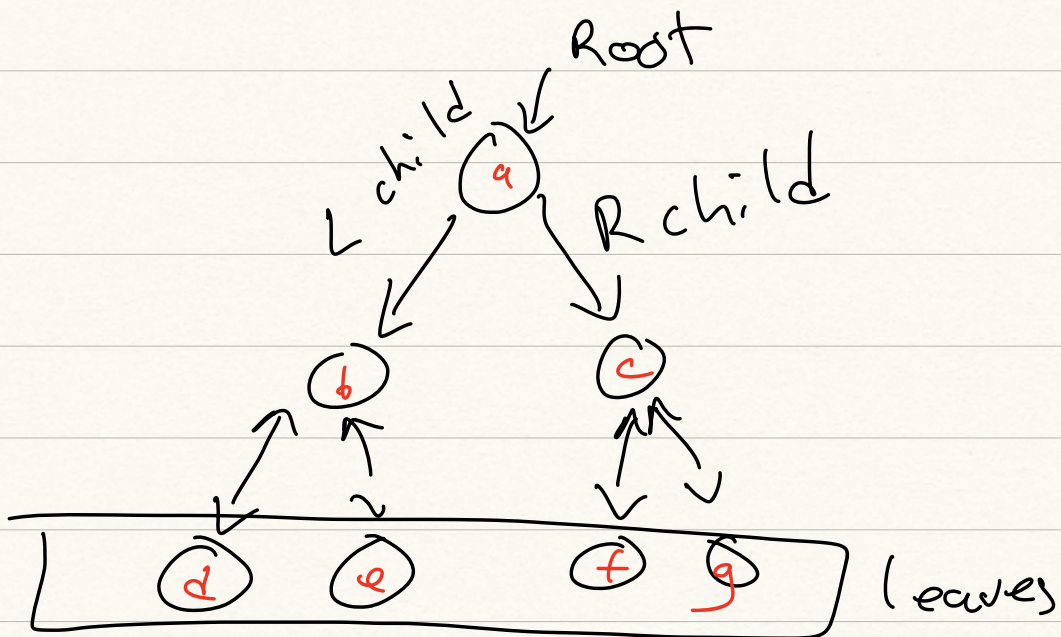
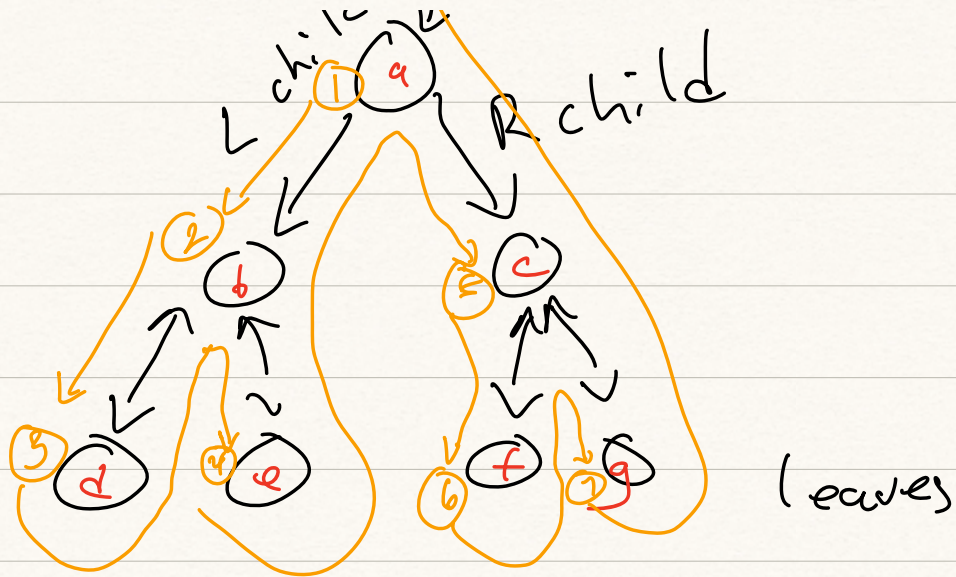
Preorder Traversal

a b d e c f g

PreOrder(Node v):

- visit(v)
- Preorder(v.left)
- Preorder(v.right)

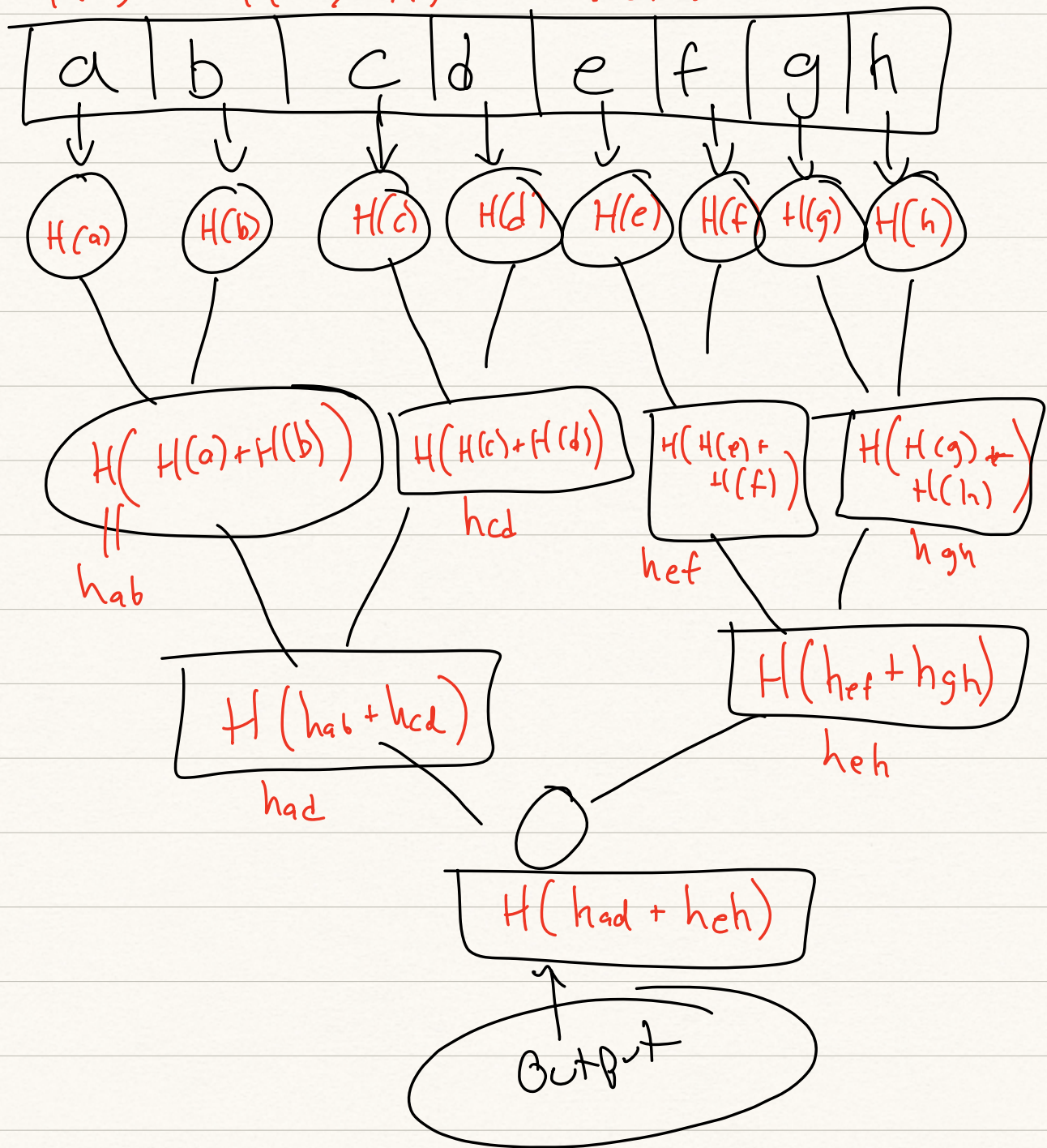
.. \ Root



Post Order (Node v) :

- Post (v.left)
- Post (v.right)
- visit (v)

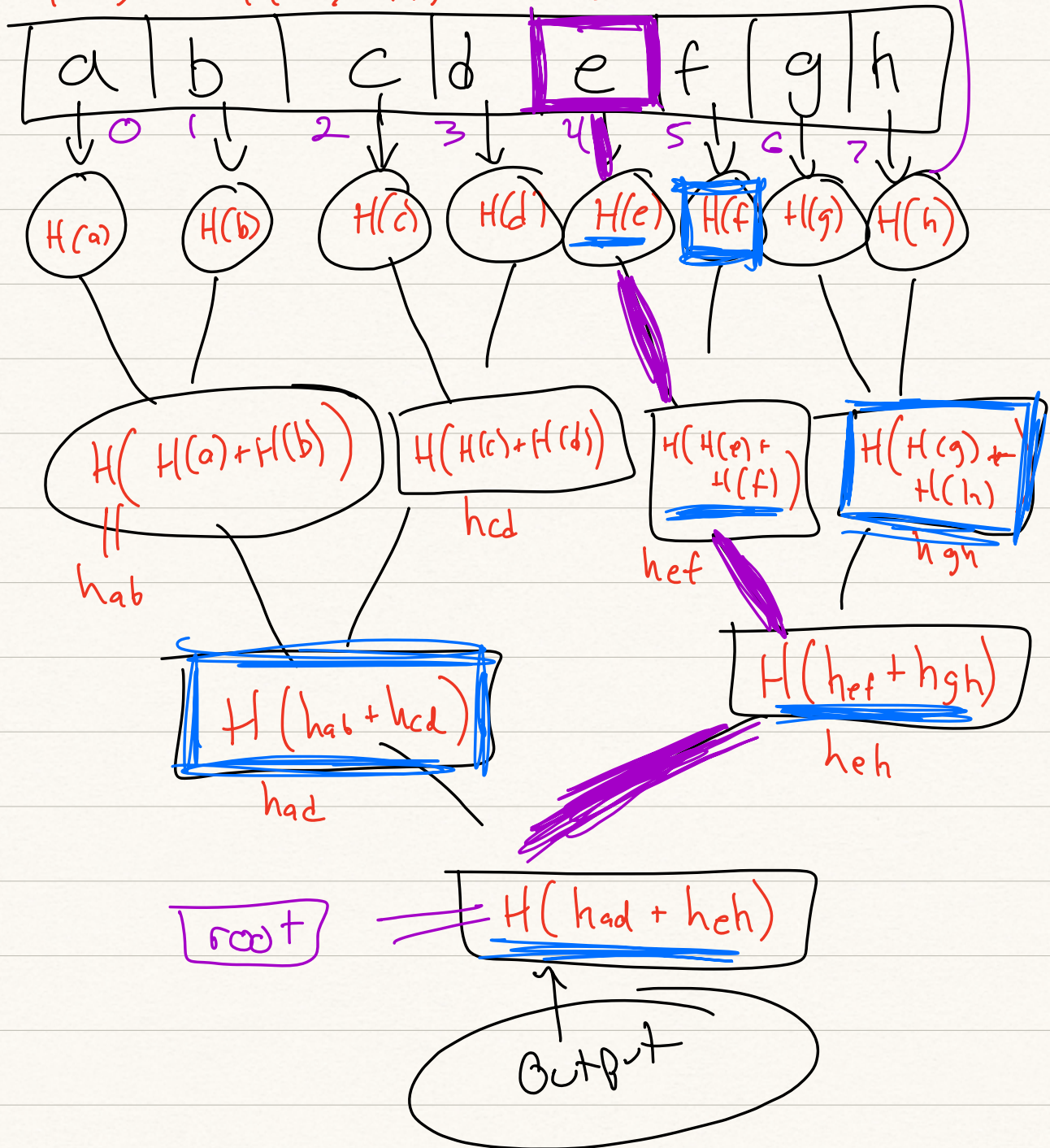
Hash $H: \{0,1\}^{2\lambda} \rightarrow \{0,1\}^\lambda$



$$H(H(H(H(H(H(a) + b) + c) + d) + e) + f)$$

(16 bits)

Hash $H: \{0,1\}^{2\lambda} \rightarrow \{0,1\}^\lambda$



Give: e

Proof: $(\underline{H(f)}, \underline{hgh}, \underline{had})$

$$\hookrightarrow \underline{hef} = (\underline{H(e)} + \underline{H(f)})$$

$$\underline{heh} = H(\underline{hef} + \underline{hgh})$$

$$\underline{hah} = H(\underline{had} + \underline{heh})$$

$\underline{hah} == \text{root} ?$