Merkle or Binary Hash Tree

Partner A

H1234 251855767925d26f27dd48db5ab70d965526d942a7c4bbe5c5a85fcf4210a46c

HASH FUNCTION

H1-2 c417da0f7e81033de4e3d4197457f368c9bc32813020be7de273e714

H3-4 bc0cac291ac4db3e9024ba7936de86e65928e7dd0c74886d3490a653802eef94

HASH FUNCTION

H1 86e1de74820a9b252ba33b2eed445b0cd02c445b5f4b8007205aff1762d7301a

H3 961eb43699731759fd0d04f177bb24f09971bddd41426702276e761269d0a5b9

H4 00e13ed7af55b27622f1d6eab5bec0147e68efe28dc2b12461117afa1a5ed40e

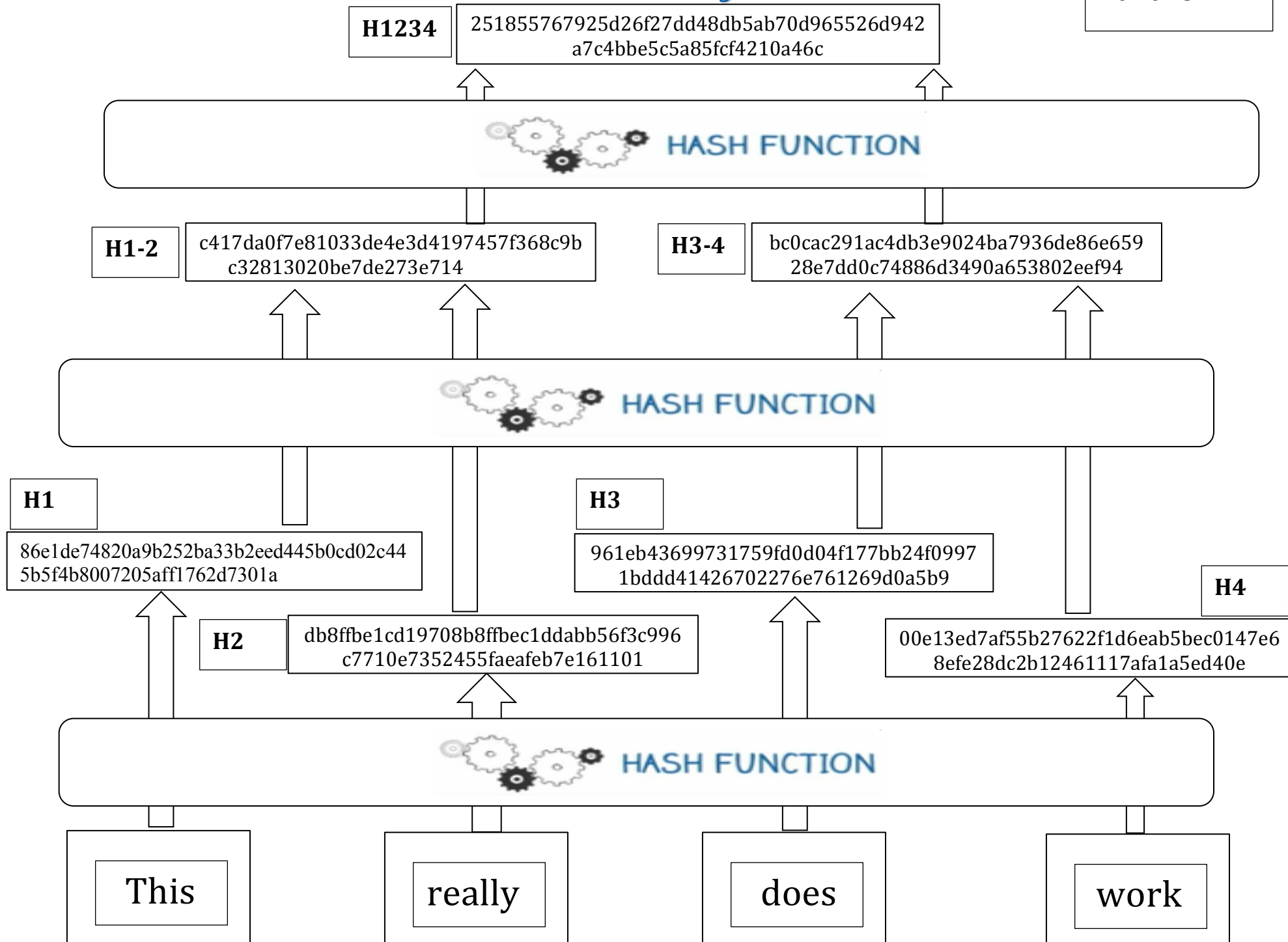**H2** db8ffbe1cd19708b8ffbec1ddabb56f3c996c7710e7352455faeafeb7e161101

HASH FUNCTION

This

really

does

work

Directions

Individual

1. Go to the Sha256 website below and create a hash (digest) for each word, exactly as it is shown on the handout.
   https://emn178.github.io/online-tools/sha256.html

   The first one has already been done for you. "This" generated the code shown in Hash1 (H1)

2. Use the hash value in H1 and the hash value in H2 as the input to create a new hash and record it in H1-2
   Note: it is important that you place them with H1 first followed directly by H2. Make sure there is no space between the two hashes when you enter them.

3. Use the hash value in H3 and the hash value in H4 as the input to create a new hash and record it in H3-4.
   Note: it is important that you place them with H3 first followed directly by H4. Make sure there is no space between the two hashes when you enter them.

4. Use the hash value in H1-2 and the hash value in H3-4 as the input to create a new hash and record it in H1234
   Note: Again, make sure there is no space between the two hashes when you enter them.

Pairs

1. Working with your partner, compare the values you recorded
2. Do you notice any differences in the input words between the two papers?
3. Do you notice any differences with each others Hash values? Where do they differ? Where are they the same?

Merkle or Binary Hash Tree

Partner B

H1234 — 37d696ceb6fb420bce911e086e054d2165c65ff681be388c572b7a8a42f1d935

HASH FUNCTION

H1-2 — 5d52e77c4aa0671f9457bec8c8acb6d25f4b28dd00634bc789a5bbb39b83f1be

H3-4 — bc0cac291ac4db3e9024ba7936de86e65928e7dd0c74886d3490a653802eef94

HASH FUNCTION

H1 — 86e1de74820a9b252ba33b2eed445b0cd02c445b5f4b8007205aff1762d7301a

H2 — 09d59056b12281326959e20973e2ffb805d4f702194c7468dad04d089a34289c

H3 — 961eb43699731759fd0d04f177bb24f09971bddd41426702276e761269d0a5b9

H4 — 00e13ed7af55b27622f1d6eab5bec0147e68efe28dc2b12461117afa1a5ed40e

HASH FUNCTION

This   Really   does   work