Christopher K. Leung (2965-7518-69)
CSCI-531 Applied Cryptography

Implementation of

Merkle Tree Proof of Inclusion and Consistency

Introduction

The Merkle Tree data structure is comprised of a binary tree where leaf values are data nodes, parents are conjoined hashes of their children, and the root node is the entire hash of all elements in the tree. The proof of inclusion and consistency serve a purpose to ensure that data integrity is maintained throughout the lifespan of additions to this data structure

Environment

For my environment, I am running PyCharm 2022.3.2 Professional Edition on Windows 11 Home version 22H2. I have treelib and hashlib imported to help with the generation of the Merkle tree

Usage

I have generated 3 files for the grader:

1. buildmtree.py
2. checkconsistency.py
3. checkinclusion.py

buildmtree.py Functional Description

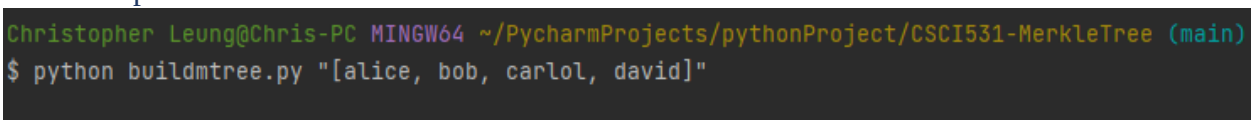
Usage:

python buildmtree.py "[<data1,data2, ..., datan>]"

Description:

This python script builds a full binary tree by passing in a list of names from the command line interface. This program outputs a file (merkle.tree) which can be read using a text editor to determine all nodes, hashes, and root nodes that are contained within Merkle tree.

Screen Captures:



```
Christopher Leung@Chris-PC MINGW64 ~/PycharmProjects/pythonProject/CSCI531-MerkleTree (main)
$ cat merkle.tree
UID:d0
Data:alice
Hash:2bd806c97f0e00af1a1fc3328fa763a9269723c8db8fac4f93af71db186d6e90
L_Node:None
R_Node:None

UID:d1
Data: bob
UID:h0
Data:2bd806c97f0e00af1a1fc3328fa763a9269723c8db8fac4f93af71db186d6e90f90e570d710dec6fa02a2f3129e489e41e53554fea8e23fa93971125cdd36f63
Hash:579e77f42f310b99d3fec66ce9438748bc13dc86695a8a182881d4756e396ba1
L_Node:d0
R_Node:d1

UID:h1
Data:299aca7e224cb9694867fbd0577c9af1830b9cc9ab552e9b0a4469652b19cb7d4e9bafdff34cc0cba000609b8c76731ec29171bd680ead7575be86987f0d182c
Hash:8eb4da3c8529ed612fa60fb80502fd4c82d760d8bdc60d8e509f9fb1956524f5
UID:h0
Data:2bd806c97f0e00af1a1fc3328fa763a9269723c8db8fac4f93af71db186d6e90f90e570d710dec6fa02a2f3129e489e41e53554fea8e23fa93971125cdd36f63
Hash:579e77f42f310b99d3fec66ce9438748bc13dc86695a8a182881d4756e396ba1
L_Node:d0
R_Node:d1

UID:h1
Data:299aca7e224cb9694867fbd0577c9af1830b9cc9ab552e9b0a4469652b19cb7d4e9bafdff34cc0cba000609b8c76731ec29171bd680ead7575be86987f0d182c
Hash:8eb4da3c8529ed612fa60fb80502fd4c82d760d8bdc60d8e509f9fb1956524f5
L_Node:d2
R_Node:d3

UID:Root
Data:579e77f42f310b99d3fec66ce9438748bc13dc86695a8a182881d4756e396ba18eb4da3c8529ed612fa60fb80502fd4c82d760d8bdc60d8e509f9fb1956524f5
Hash:26df2478ab9ba3f923f6f5f810dc11aa898ee2820098e6fbf7eab10825d4eed6
L_Node:h0
R_Node:h1
```

Note to grader:

The Merkle Tree generation will ensure that the tree generated is full. It will copy the last leaf node certain amount of times to obtain a power of 2. Please see piazza post below for verification of concatenation of non-full leaf nodes to complete the binary tree.

Piazza post https://piazza.com/class/lcgjdtutgvz7o9/post/149

Christopher K. Leung (2965-7518-69)
CSCI-531 Applied Cryptography

checkinclusion.py Functional Description

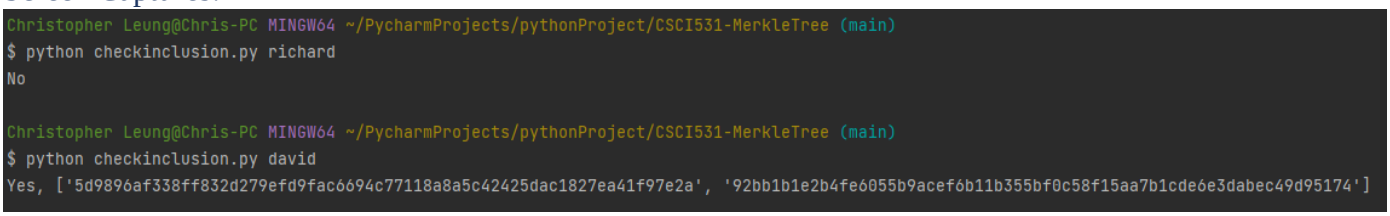
Usage:

python checkinclusion.py <name>

Description:

This python script builds parses merkle.tree and finds the minimum number of nodes required to verify the root hash.

Screen Captures:



Christopher K. Leung (2965-7518-69)
CSCI-531 Applied Cryptography

checkconsistency.py Functional Description

Usage:

python checkinclusion.py "[<data1,data2, ..., datan>]" "[<data1,data2, ..., datan>]"

Note: Please use quotations (“ “) and brackets ([]) to denote Tree 1 and Tree2 separately

Description:

This python script takes in 2 lists and determines to see if the first one is a subset of the second

Screen Captures:

Test 1 “[alice, bob, carlol, david]” “ [alice, bob, carlol, david, eve, fred]”

```
Christopher Leung@Chris-PC MINGW64 ~/PycharmProjects/pythonProject/CSCI531-MerkleTree (main)
$ python checkconsistency.py "[alice, bob, carlol, david]" "[alice, bob, carlol, david, eve, fred]"
Yes, ['0241d53ad33e6e6ae115fdd957c7d09003471d422f18d2a7e9bffcb23a3d9e9a', '44635ddae2d7a6f4a1c1a3cec23f89532fe23eb9f75c38232c4f7213997ff689', 'cd005ff771566071bfe26ac5deb47f3e5619c226036034 58a533e5d43afcbe3c']
```

```
$ cat merkle.trees
--- Begin Tree 1 ---
UID:d0
Data:alice
Hash:2bd806c97f0e00af1a1fc3328fa763a9269723c8db8fac4f93af71db186d6e90
L_Node:None
R_Node:None

UID:d1
Data:bob
Hash:81b637d8fcd2c6da6359e6963113a1170de795e4b725b84d1e0b4cfd9ec58ce9
L_Node:None
R_Node:None

UID:d2
Data:carlol
Hash:5d9896af338ff832d279efd9fac6694c77118a8a5c42425dac1827ea41f97e2a
L_Node:None
R_Node:None

UID:d3
Data:david
Hash:07d046d5fac12b3f82daf5035b9aae86db5adc8275ebfbf05ec83005a4a8ba3e
L_Node:None
R_Node:None

UID:h0
Data:2bd806c97f0e00af1a1fc3328fa763a9269723c8db8fac4f93af71db186d6e9081b637d8fcd2c6da6359e6963113a1170de795e4b725b84d1e0b4cfd9ec58ce9
Hash:92bb1b1e2b4fe6055b9acef6b11b355bf0c58f15aa7b1cde6e3dabec49d95174
L_Node:d0
R_Node:d1

UID:h1
Data:5d9896af338ff832d279efd9fac6694c77118a8a5c42425dac1827ea41f97e2a07d046d5fac12b3f82daf5035b9aae86db5adc8275ebfbf05ec83005a4a8ba3e
Hash:deab4c2ec0d3420cb4064a3043150d5ae7028b71a490f35e34c2a099e1bc2f23
L_Node:d2
R_Node:d3
```

```
UID:Root
Data:92bb1b1e2b4fe6055b9acef6b11b355bf0c58f15aa7b1cde6e3dabec49d95174deab4c2ec0d3420cb4064a3043150d5ae7028b71a490f35e34c2a099e1bc2f23
Hash:0241d53ad33e6e6ae115fdd957c7d09003471d422f18d2a7e9bffcb23a3d9e9a
L_Node:h0
R_Node:h1

--- End Tree 1 ---
```

```
--- Begin Tree 2 ---
UID:d0
Data:alice
Hash:2bd806c97f0e00af1a1fc3328fa763a9269723c8db8fac4f93af71db186d6e90
L_Node:None
R_Node:None

UID:d1
Data:bob
Hash:81b637d8fcd2c6da6359e6963113a1170de795e4b725b84d1e0b4cfd9ec58ce9
L_Node:None
R_Node:None

UID:d2
Data:carlol
Hash:5d9896af338ff832d279efd9fac6694c77118a8a5c42425dac1827ea41f97e2a
L_Node:None
R_Node:None

UID:d3
Data:david
Hash:07d046d5fac12b3f82daf5035b9aae86db5adc8275ebfbf05ec83005a4a8ba3e
L_Node:None
R_Node:None

UID:d4
Data:eve
Hash:85262adf74518bbb70c7cb94cd6159d91669e5a81edf1efebd543eadbda9fa2b
L_Node:None
R_Node:None

UID:d5
Data:fred
Hash:d0cfc2e5319b82cdc71a33873e826c93d7ee11363f8ac91c4fa3a2cfcd2286e5
L_Node:None
R_Node:None
```

```
UID:d6
Data:fred
Hash:d0cfc2e5319b82cdc71a33873e826c93d7ee11363f8ac91c4fa3a2cfcd2286e5
L_Node:None
R_Node:None

UID:d7
Data:fred
Hash:d0cfc2e5319b82cdc71a33873e826c93d7ee11363f8ac91c4fa3a2cfcd2286e5
L_Node:None
R_Node:None

UID:h0
Data:2bd806c97f0e00af1a1fc3328fa763a9269723c8db8fac4f93af71db186d6e9081b637d8fcd2c6da6359e6963113a1170de795e4b725b84d1e0b4cfd9ec58ce9
Hash:92bb1b1e2b4fe6055b9acef6b11b355bf0c58f15aa7b1cde6e3dabec49d95174
L_Node:d0
R_Node:d1

UID:h1
UID:h5
Data:51ef3f857b1e1c0d59b4150ff4aba5137fdbbd32cba7a3fcb6495408bcb79aa7b10d7fbf17980e519b6c5d87f5a70f5621d9456fc6de38f68a50d38d83066ea7
Hash:44635ddae2d7a6f4a1c1a3cec23f89532fe23eb9f75c38232c4f7213997ff689
L_Node:h2
R_Node:h3

UID:Root
Data:0241d53ad33e6e6ae115fdd957c7d09003471d422f18d2a7e9bffcb23a3d9e9a44635ddae2d7a6f4a1c1a3cec23f89532fe23eb9f75c38232c4f7213997ff689
Hash:cd005ff771566071bfe26ac5deb47f3e5619c22603603458a533e5d43afcbe3c
L_Node:h4
R_Node:h5

--- End Tree 2 ---
```

Test 2 "[alice, bob, carlol, david]" "[alice, bob, david, eve, fred]":

```
Christopher Leung@Chris-PC MINGW64 ~/PycharmProjects/pythonProject/CSCI531-MerkleTree (main)
$ python checkconsistency.py "[alice, bob, carlol, david]" "[alice, bob, david, eve, fred]"
No
```

```
$ cat merkle.trees
--- Begin Tree 1 ---
UID:d0
Data:alice
Hash:2bd806c97f0e00af1a1fc3328fa763a9269723c8db8fac4f93af71db186d6e90
L_Node:None
R_Node:None

UID:d1
Data:bob
Hash:81b637d8fcd2c6da6359e6963113a1170de795e4b725b84d1e0b4cfd9ec58ce9
L_Node:None
R_Node:None

UID:d2
Data:carlol
Hash:5d9896af338ff832d279efd9fac6694c77118a8a5c42425dac1827ea41f97e2a
L_Node:None
R_Node:None

UID:d3
Data:david
Hash:07d046d5fac12b3f82daf5035b9aae86db5adc8275ebfbf05ec83005a4a8ba3e
L_Node:None
R_Node:None

UID:h0
Data:2bd806c97f0e00af1a1fc3328fa763a9269723c8db8fac4f93af71db186d6e9081b637d8fcd2c6da6359e6963113a1170de795e4b725b84d1e0b4cfd9ec58ce9
Hash:92bb1b1e2b4fe6055b9acef6b11b355bf0c58f15aa7b1cde6e3dabec49d95174
L_Node:d0
R_Node:d1

UID:h1
Data:5d9896af338ff832d279efd9fac6694c77118a8a5c42425dac1827ea41f97e2a07d046d5fac12b3f82daf5035b9aae86db5adc8275ebfbf05ec83005a4a8ba3e
Hash:deab4c2ec0d3420cb4064a3043150d5ae7028b71a490f35e34c2a099e1bc2f23
L_Node:d2
R_Node:d3

UID:Root
Data:92bb1b1e2b4fe6055b9acef6b11b355bf0c58f15aa7b1cde6e3dabec49d95174deab4c2ec0d3420cb4064a3043150d5ae7028b71a490f35e34c2a099e1bc2f23
Hash:0241d53ad33e6e6ae115fdd957c7d09003471d422f18d2a7e9bffcb23a3d9e9a
L_Node:h0
R_Node:h1

--- End Tree 1 ---
```

```
--- Begin Tree 2 ---
UID:d0
Data:alice
Hash:2bd806c97f0e00af1a1fc3328fa763a9269723c8db8fac4f93af71db186d6e90
L_Node:None
R_Node:None

UID:d1
Data:bob
Hash:81b637d8fcd2c6da6359e6963113a1170de795e4b725b84d1e0b4cfd9ec58ce9
L_Node:None
R_Node:None

UID:d2
Data:david
Hash:07d046d5fac12b3f82daf5035b9aae86db5adc8275ebfbf05ec83005a4a8ba3e
L_Node:None
R_Node:None

UID:d3
Data:eve
Hash:85262adf74518bbb70c7cb94cd6159d91669e5a81edf1efebd543eadbda9fa2b
L_Node:None
R_Node:None

UID:d4
Data:fred
Hash:d0cfc2e5319b82cdc71a33873e826c93d7ee11363f8ac91c4fa3a2cfcd2286e5
L_Node:None
R_Node:None

UID:d5
Data:fred
Hash:d0cfc2e5319b82cdc71a33873e826c93d7ee11363f8ac91c4fa3a2cfcd2286e5
L_Node:None
R_Node:None
```

```
UID:d5
Data:fred
Hash:d0cfc2e5319b82cdc71a33873e826c93d7ee11363f8ac91c4fa3a2cfcd2286e5
L_Node:None
R_Node:None

UID:d6
Data:fred
Hash:d0cfc2e5319b82cdc71a33873e826c93d7ee11363f8ac91c4fa3a2cfcd2286e5
L_Node:None
R_Node:None

UID:d7
Data:fred
Hash:d0cfc2e5319b82cdc71a33873e826c93d7ee11363f8ac91c4fa3a2cfcd2286e5
L_Node:None
R_Node:None

UID:h0
Data:2bd806c97f0e00af1a1fc3328fa763a9269723c8db8fac4f93af71db186d6e9081b637d8fcd2c6da6359e6963113a1170de795e4b725b84d1e0b4cfd9ec58ce9
Hash:92bb1b1e2b4fe6055b9acef6b11b355bf0c58f15aa7b1cde6e3dabec49d95174
L_Node:d0
R_Node:d1

UID:h1
Data:07d046d5fac12b3f82daf5035b9aae86db5adc8275ebfbf05ec83005a4a8ba3e85262adf74518bbb70c7cb94cd6159d9166 9e5a81edf1efebd543eadbda9fa2b
Hash:f4c62a5b8158da17b90dcc2e599cc9a70bffad3d409021998f9934a0a842bd9a
L_Node:d2
R_Node:d3

UID:h2
Data:d0cfc2e5319b82cdc71a33873e826c93d7ee11363f8ac91c4fa3a2cfcd2286e5d0cfc2e5319b82cdc71a33873e826c93d7ee11363f8ac91c4fa3a2cfcd2286e5
Hash:b10d7fbf17980e519b6c5d87f5a70f5621d9456fc6de38f68a50d38d83066ea7
L_Node:d4
R_Node:d5
```

```
UID:h3
Data:d0cfc2e5319b82cdc71a33873e826c93d7ee11363f8ac91c4fa3a2cfcd2286e5d0cfc2e5319b82cdc71a33873e826c93d7ee11363f8ac91c4fa3a2cfcd2286e5
Hash:b10d7fbf17980e519b6c5d87f5a70f5621d9456fc6de38f68a50d38d83066ea7
L_Node:d6
R_Node:d7

UID:h4
Data:92bb1b1e2b4fe6055b9acef6b11b355bf0c58f15aa7b1cde6e3dabec49d95174f4c62a5b8158da17b90dcc2e599cc9a70bffad3d409021998f9934a0a842bd9a
Hash:87c7a717ab52e55c62a15c0bf3694b5300d09874c032c097bf87243ddfa9e2db
L_Node:h0
R_Node:h1

UID:h5
Data:b10d7fbf17980e519b6c5d87f5a70f5621d9456fc6de38f68a50d38d83066ea7b10d7fbf17980e519b6c5d87f5a70f5621d9456fc6de38f68a50d38d83066ea7
Hash:4115dd817d2d1c49ab056ad465620cd7d4cf8ea2c83d3b582119d63923a121d5
L_Node:h2
R_Node:h3

UID:Root
Data:87c7a717ab52e55c62a15c0bf3694b5300d09874c032c097bf87243ddfa9e2db4115dd817d2d1c49ab056ad465620cd7d4cf8ea2c83d3b582119d63923a121d5
Hash:b8b3a4bb245a48ee2d130193b589fc25e59599606cba8c0286e12a4dd6c62dba
L_Node:h4
R_Node:h5

--- End Tree 2 ---
```

Test 3 “[alice, bob, carlol, david]” “[alice, bob, carol eve, fred, davis]”

```
Christopher Leung@Chris-PC MINGW64 ~/PycharmProjects/pythonProject/CSCI531-MerkleTree (main)
$ python checkconsistency.py "[alice, bob, carlol, david]" "[alice, bob, carol eve, fred, davis]"
No
```

```
$ cat merkle.trees
--- Begin Tree 1 ---
UID:d0
Data:alice
Hash:2bd806c97f0e00af1a1fc3328fa763a9269723c8db8fac4f93af71db186d6e90
L_Node:None
R_Node:None

UID:d1
Data:bob
Hash:81b637d8fcd2c6da6359e6963113a1170de795e4b725b84d1e0b4cfd9ec58ce9
L_Node:None
R_Node:None

UID:d2
Data:carlol
Hash:5d9896af338ff832d279efd9fac6694c77118a8a5c42425dac1827ea41f97e2a
L_Node:None
R_Node:None

UID:d3
Data:david
Hash:07d046d5fac12b3f82daf5035b9aae86db5adc8275ebfbf05ec83005a4a8ba3e
L_Node:None
R_Node:None

UID:h0
Data:2bd806c97f0e00af1a1fc3328fa763a9269723c8db8fac4f93af71db186d6e9081b637d8fcd2c6da6359e6963113a1170de795e4b725b84d1e0b4cfd9ec58ce9
Hash:92bb1b1e2b4fe6055b9acef6b11b355bf0c58f15aa7b1cde6e3dabec49d95174
L_Node:d0
R_Node:d1

UID:h1
Data:5d9896af338ff832d279efd9fac6694c77118a8a5c42425dac1827ea41f97e2a07d046d5fac12b3f82daf5035b9aae86db5adc8275ebfbf05ec83005a4a8ba3e
Hash:deab4c2ec0d3420cb4064a3043150d5ae7028b71a490f35e34c2a099e1bc2f23
L_Node:d2
R_Node:d3
```

```
UID:Root
Data:92bb1b1e2b4fe6055b9acef6b11b355bf0c58f15aa7b1cde6e3dabec49d95174deab4c2ec0d3420cb4064a3043150d5ae7028b71a490f35e34c2a099e1bc2f23
Hash:0241d53ad33e6e6ae115fdd957c7d09003471d422f18d2a7e9bffcb23a3d9e9a
L_Node:h0
R_Node:h1

--- End Tree 1 ---
```

```
--- Begin Tree 2 ---
UID:d0
Data:alice
Hash:2bd806c97f0e00af1a1fc3328fa763a9269723c8db8fac4f93af71db186d6e90
L_Node:None
R_Node:None

UID:d1
Data:bob
Hash:81b637d8fcd2c6da6359e6963113a1170de795e4b725b84d1e0b4cfd9ec58ce9
L_Node:None
R_Node:None

UID:d2
Data:caroleve
Hash:cf8570156e8ab3f0aacfccac1faa37b898f4c3ac1ab6949ab809c024ce0af636
L_Node:None
R_Node:None

UID:d3
Data:fred
Hash:d0cfc2e5319b82cdc71a33873e826c93d7ee11363f8ac91c4fa3a2cfcd2286e5
L_Node:None
R_Node:None

UID:d4
Data:davis
Hash:4458e908dd9a5440ad70b4d0ee13ebe96f0d25bb263b80169b3de5a9a0b90e3d
L_Node:None
R_Node:None

UID:d5
Data:davis
Hash:4458e908dd9a5440ad70b4d0ee13ebe96f0d25bb263b80169b3de5a9a0b90e3d
L_Node:None
R_Node:None
```

```
UID:d6
Data:davis
Hash:4458e908dd9a5440ad70b4d0ee13ebe96f0d25bb263b80169b3de5a9a0b90e3d
L_Node:None
R_Node:None

UID:d7
Data:davis
Hash:4458e908dd9a5440ad70b4d0ee13ebe96f0d25bb263b80169b3de5a9a0b90e3d
L_Node:None
R_Node:None

UID:h0
Data:2bd806c97f0e00af1a1fc3328fa763a9269723c8db8fac4f93af71db186d6e9081b637d8fcd2c6da6359e6963113a1170de795e4b725b84d1e0b4cfd9ec58ce9
Hash:92bb1b1e2b4fe6055b9acef6b11b355bf0c58f15aa7b1cde6e3dabec49d95174
L_Node:d0
R_Node:d1

UID:h1
Data:cf8570156e8ab3f0aacfccac1faa37b898f4c3ac1ab6949ab809c024ce0af636d0cfc2e5319b82cdc71a33873e826c93d7ee11363f8ac91c4fa3a2cfcd2286e5
Hash:8d792d7ebb8c929c74d26e30d321a239c8a93b549f69c6ebb1af3fa81e96ef41
L_Node:d2
R_Node:d3

UID:h2
Data:4458e908dd9a5440ad70b4d0ee13ebe96f0d25bb263b80169b3de5a9a0b90e3d4458e908dd9a5440ad70b4d0ee13ebe96f0d25bb263b80169b3de5a9a0b90e3d
Hash:e7f89e560c37a7e5eded926f307d70fc0f04a2a9c73eb6a1f3d2dcfb1dafc617
L_Node:d4
R_Node:d5

UID:h3
Data:4458e908dd9a5440ad70b4d0ee13ebe96f0d25bb263b80169b3de5a9a0b90e3d4458e908dd9a5440ad70b4d0ee13ebe96f0d25bb263b80169b3de5a9a0b90e3d
Hash:e7f89e560c37a7e5eded926f307d70fc0f04a2a9c73eb6a1f3d2dcfb1dafc617
L_Node:d6
R_Node:d7
```

```
UID:h4
Data:92bb1b1e2b4fe6055b9acef6b11b355bf0c58f15aa7b1cde6e3dabec49d951748d792d7ebb8c929c74d26e30d321a239c8a93b549f69c6ebb1af3fa81e96ef41
Hash:9306d655bd95f44bfcba3041a09fa85871dfa1b0752e4ef2259dd168d2dce2d
L_Node:h0
R_Node:h1

UID:h5
Data:e7f89e560c37a7e5eded926f307d70fc0f04a2a9c73eb6a1f3d2dcfb1dafc617e7f89e560c37a7e5eded926f307d70fc0f04a2a9c73eb6a1f3d2dcfb1dafc617
Hash:73c084c8859098c1d62f05a4d0391e99025d6be408f4ab6afd7cf9588342171b
L_Node:h2
R_Node:h3

UID:Root
Data:9306d655bd95f44bfcba3041a09fa85871dfa1b0752e4ef2259dd168d2dce2d73c084c8859098c1d62f05a4d0391e99025d6be408f4ab6afd7cf9588342171b
Hash:03b7543a8efcfd5d047f7f73b5235e6a5240b32536387e70010554b20fbdd82
L_Node:h4
R_Node:h5

--- End Tree 2 ---
```