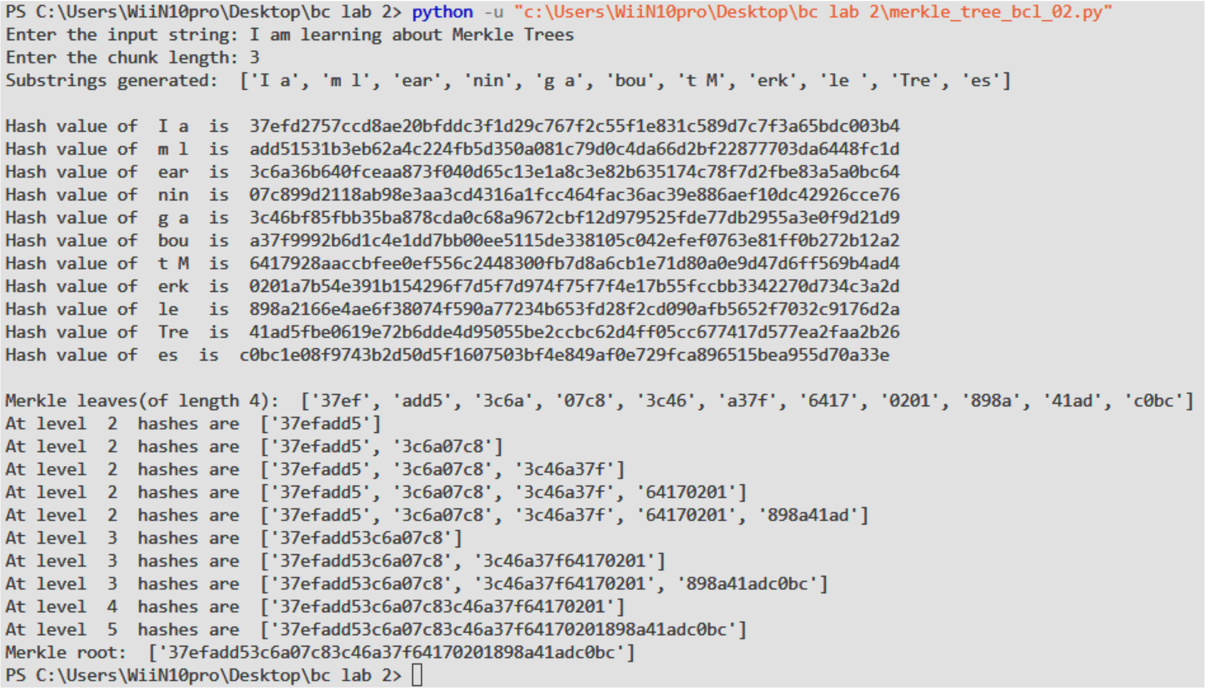
Practical 2: Merkle Trees

Harshvardhan Singh

1019161

```
import hashlib
def getSubString(msg,chunkLength):
    subStrings = []
    for i in range(0,len(msg),chunkLength):
        subStrings.append(msg[i:i+chunkLength])
    return subStrings
def getHash(subStrings):
    hashes = []
    for subString in subStrings:
        subStrHash =
hashlib.sha256(str(subString).encode()).hexdigest()
        print("Hash value of ",subString," is
",subStrHash)
        hashes.append(subStrHash[:4])
    return hashes
def getMerkleRoot(merkleLeaves,level):
    if len(merkleLeaves)==1:
        return merkleLeaves
    root = []
    for i in range(0,len(merkleLeaves),2):
        if i == len(merkleLeaves) -1:
            root.append(merkleLeaves[i])
        else:
     root.append(merkleLeaves[i]+merkleLeaves[i+1])
            print("At level ",level," hashes are ",root)
    leaf = getMerkleRoot(root,level+1)
    return leaf
msg = input("Enter the input string: ")
chunkLength = int(input("Enter the chunk length: "))
subStrings = getSubString(msg,chunkLength)
print("Substrings generated: ",subStrings)
print()
merkleLeaves = getHash(subStrings)
print()
print("Merkle leaves(of length 4): ",merkleLeaves)
print("Merkle root:
",getMerkleRoot(merkleLeaves,2))
```



```
PS C:\Users\WiiN10pro\Desktop\bc lab 2> python -u "c:\Users\WiiN10pro\Desktop\bc lab 2\merkle_tree_bcl_02.py"
Enter the input string: I am learning about Merkle Trees
Enter the chunk length: 3
Substrings generated:  ['I a', 'm l', 'ear', 'nin', 'g a', 'bou', 't M', 'erk', 'le ', 'Tre', 'es']

Hash value of  I a  is  37efd2757ccd8ae20bfddc3f1d29c767f2c55f1e831c589d7c7f3a65bdc003b4
Hash value of  m l  is  add51531b3eb62a4c224fb5d350a081c79d0c4da66d2bf22877703da6448fc1d
Hash value of  ear  is  3c6a36b640fceaa873f040d65c13e1a8c3e82b635174c78f7d2fbe83a5a0bc64
Hash value of  nin  is  07c899d2118ab98e3aa3cd4316a1fcc464fac36ac39e886aef10dc42926cce76
Hash value of  g a  is  3c46bf85fbb35ba878cda0c68a9672cbf12d979525fde77db2955a3e0f9d21d9
Hash value of  bou  is  a37f9992b6d1c4e1dd7bb00ee5115de338105c042efef0763e81ff0b272b12a2
Hash value of  t M  is  6417928aaccbfee0ef556c2448300fb7d8a6cb1e71d80a0e9d47d6ff569b4ad4
Hash value of  erk  is  0201a7b54e391b154296f7d5f7d974f75f7f4e17b55fccbb3342270d734c3a2d
Hash value of  le   is  898a2166e4ae6f38074f590a77234b653fd28f2cd090afb5652f7032c9176d2a
Hash value of  Tre  is  41ad5fbe0619e72b6dde4d95055be2ccbc62d4ff05cc677417d577ea2faa2b26
Hash value of  es  is  c0bc1e08f9743b2d50d5f1607503bf4e849af0e729fca896515bea955d70a33e

Merkle leaves(of length 4):  ['37ef', 'add5', '3c6a', '07c8', '3c46', 'a37f', '6417', '0201', '898a', '41ad', 'c0bc']
At level  2  hashes are  ['37efadd5']
At level  2  hashes are  ['37efadd5', '3c6a07c8']
At level  2  hashes are  ['37efadd5', '3c6a07c8', '3c46a37f']
At level  2  hashes are  ['37efadd5', '3c6a07c8', '3c46a37f', '64170201']
At level  2  hashes are  ['37efadd5', '3c6a07c8', '3c46a37f', '64170201', '898a41ad']
At level  3  hashes are  ['37efadd53c6a07c8']
At level  3  hashes are  ['37efadd53c6a07c8', '3c46a37f64170201']
At level  3  hashes are  ['37efadd53c6a07c8', '3c46a37f64170201', '898a41adc0bc']
At level  4  hashes are  ['37efadd53c6a07c83c46a37f64170201']
At level  5  hashes are  ['37efadd53c6a07c83c46a37f64170201898a41adc0bc']
Merkle root:  ['37efadd53c6a07c83c46a37f64170201898a41adc0bc']
PS C:\Users\WiiN10pro\Desktop\bc lab 2> 
```