Department of Electrical Engineering
Sharif University of Technology

Foundations of Blockchain
by: Dr. Mohammad A. Maddah-Ali
Fall 1399(2020)

Practical Homework 1

Issued: Tuesday, Aban 13, 1399 **Due: Wednesday, Aban 28, 1399**

Note: You must use Python for solving all questions.

Hash Functions

Question 1: We use hash function in many applications. In this part, we are going to work with this function in order to learn it better and address some problems of that. We use Sha-256 for hashing and might use less significant bits of that. For example we can construct our hash function as below:

$$H(x) := SHA256(x) \bmod 2^{20}$$

An example may help clarify the point.

Sha256("Hi")="3639EFCD08ABB273B1619E82E78C29A7DF02C1051B1820E99FC395DCAA3326B8"
Sha256("Good Bye")="570398A0EE87C360188291D4116AE9D70183DE80C385F006133DC90C077C1C60"

H("Hi")= "326B8"
H("Good Bye")=" C1C60"

A)Assume a network in which we store the hash of every one's id (H(id)). Your id is your student number. Find an integer (t) or string (t) which H(t)=H(id). (you can use libraries which contain SHA256).

Submission: For this part you should submit a text file(x.txt) .In the first line write your name (your id) and in the second line type t. Be careful about the extra spaces.

Report:A detailed report of how your code works is needed.

B)In this part we want to find two integers which their hashes are identical. We use a time limit for this part.

Submission: For this part you should submit a code and it should print first integer in the first line and second integer in the second line and your code should return numbers in a random way. It means it should change the numbers every time we run that function.

Hint: A brute force approach will not get you a full score. See The Birthday Problem.

Report:A brief summary of Birthday Problem and your code is needed

C)We want to find a way for authentication problem using hash function. We know that it is hard to find a collision in a hash function so we use this feature. We assume that we have a string s which is already shared between sender and receiver through a safe channel and no one else would know that.
Now one of them wants to send a message through a channel which is not safe and every one can read their message.
What can receiver do to make sure that the sender himself has sent that message?(you can find it in slides)

Hint: It is not important for them if someone else can read the message as a result their sent message can contain the original text as one of the parts of the sent message. They just want to know that the message is not changed or sent by another user.

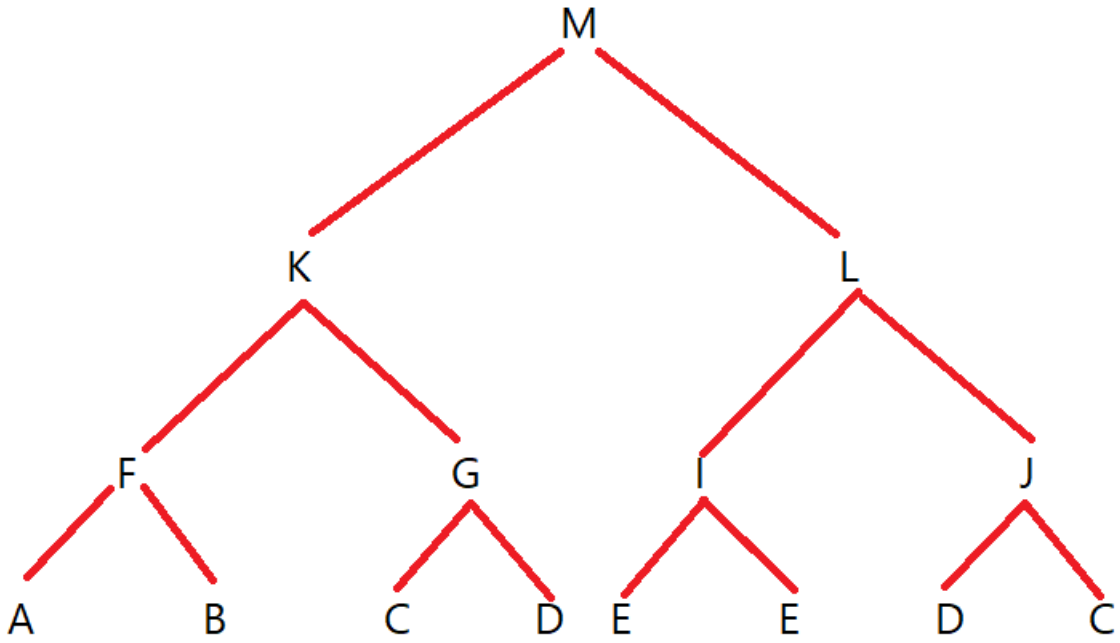
Submission: Your code should have 2 parts. One for sender and another for receiver.
For the sender your code should have 2 inputs and 1 output:
Inputs: message m (string), and string s
Output: the sent message(might include more than 1 parts)
For the receiver your code again should have 2 inputs and 1 output which is described below
Inputs: sent message, string s
Output:If the message is sent from the appropriate sender your code should print the recovered message. Else, it should print "The message has been changed!"

Report: The idea should be explained and a summary of your code is needed.

Merkle Tree Construction

Question 2: In this problem, we will learn how merkle trees are constructed. To do this we will first introduce padding.

Padding: We know how to construct a merkle tree when the number of files is a power of two. Now consider a case where the number of files isn't a power of two. We need a unique way of constructing the tree. Our padding method works like this: At the maximum level(leaves) we copy some of the leaves as another one. For example if the number of leaves is 28 we use leave number 28 for the 29th, 27th for the 30th, 26th for the 31th and 25th for the 32th . In this example you can see how it works for 5 leaves. A,B,C,D,E are inputs.

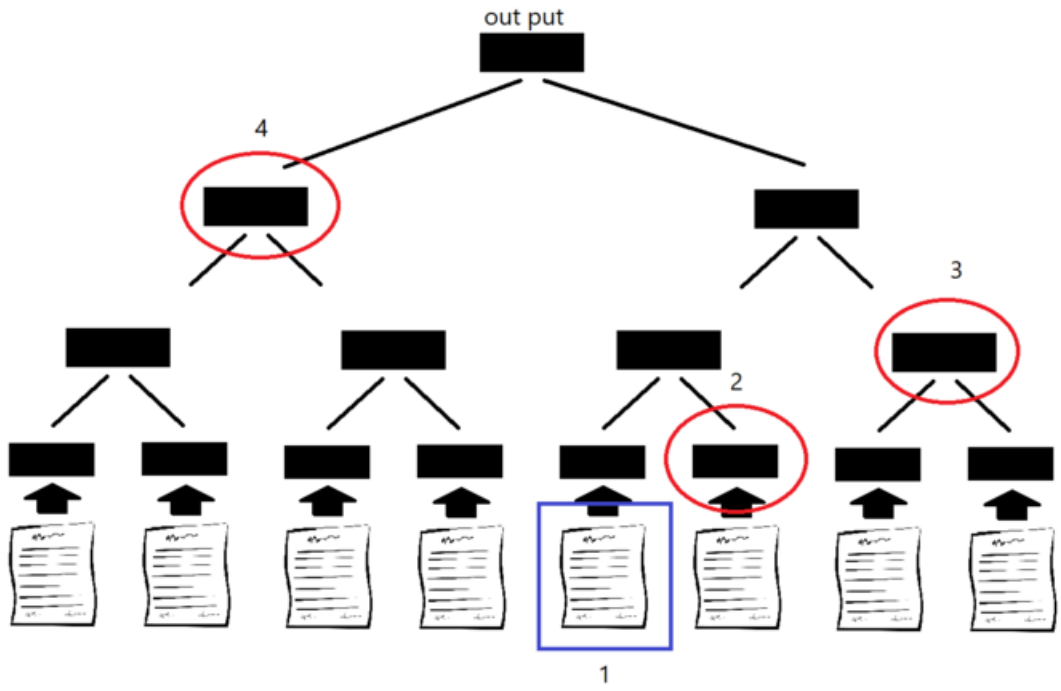


Submission: Your code should ask for the number of leaves (n) then it should scan n string as the inputs. After that you should calculate other ancestors and finally print the hex format of the merkle root.

Report:A detailed report of how merkle tree is constructed and how your code is working is needed.

Merkle Tree Proof

Question 3: In this problem we will see how the merkle tree constructed in the previous section can be used as a proof of existence of data. In the first line the user should enter the number of leaves (n).Then the code should ask for the next item. For example in this example n=8 and code should ask for the value of the nodes in this order. And after that user should enter the hex format of the merkle root. Then your code should compare the entered merkle root with the calculated merkle root and check if they have same values. In this example you should ask the user 5 parameters:
1st:the data(we want to find out if it exists in the merkle tree or not)
2nd:value of the node declared in the picture
3rd:value of the node declared in the picture
4th:value of the node declared in the picture
5th:value of the output



Submission Inputs: Your code should ask for the number of leaves(n) if n was not a power of two, you should use the algorithm described in the previous section to construct the tree. Then you should enter (log(n)+2) inputs like the example.
Output: If the existence of the data was proved, your code should print "Existed". Else it should print "Did not exist!"

Report:A detailed report of how merkle proof works and how your code is working is needed.

Note: Your report should contain a brief explanation of all questions. Your report has an important role in your marks.
If you did not understand some questions, you can contact this email or id:
parham.moradi77@gmail.com
ID: @Parham_1998

Good luck!