AbdelRahman Adel
17012296

No.
Date / /

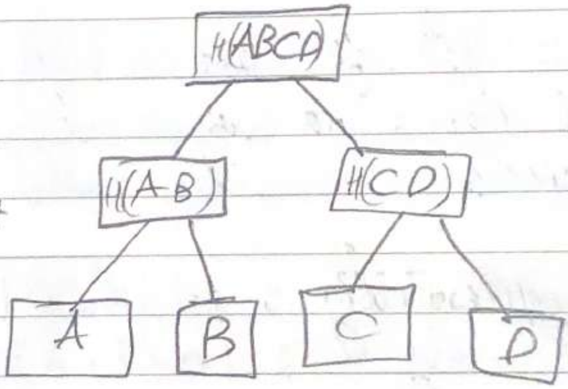
Assignment 1

① a) The hash of h(Tail) & h(head) both are unique so without the random string you can know the actual result if you have both hashes.

b) No, r XOR "Tail" will also create a random string, which means that h(r XOR "Tail") will also be random, as long as r is large enough nothing will change.

② Assume this Tree

and we will edit file (B) into B^*



after editing

we will need the sibling of (B) from the same Paren

use it to get AB^* & then get CD & create a new root hash AB^* CD

No.

Date. / /

(3) using byte with the values from 0 to 9
when 1 bit changes all 256 bits of the
hash changes.

(4) Yes, due to the hashing properties of collisson
resistance to make sure that the message
m is Correct H(m) must equal h & if not
the either h & m are corrupted or missed

(5) No it's not safe, some one might have changed the message
and there is no way to verify it's actually correct
response

(6) - Sequentially : 1027.0169
Randomly : 1029.6384

- The is around 2^{k} where k = difficulity
so at k = 10 it's around 1024

- The average doubles when you increment by one
& halfs when you decrement by one

9 : 511.485
11 : 2047.069 #

- No Difference between sequential or Random

No.

Date / /

(7) $H_3(x) = H_1(x)$ xor $H_2(x)$
is the only one that might not be collission resistant

There is no gurantee that xor of two unique bit arrays to produce a unique byte

ex

10 xor 01 = 11

01 xor 10 = 11

I acknowledge that I am aware of the academic integrity guidelines of this course and that I worked on this assignment independently without any authorized help.

عبدالرحمن عادل عبدالفتاح