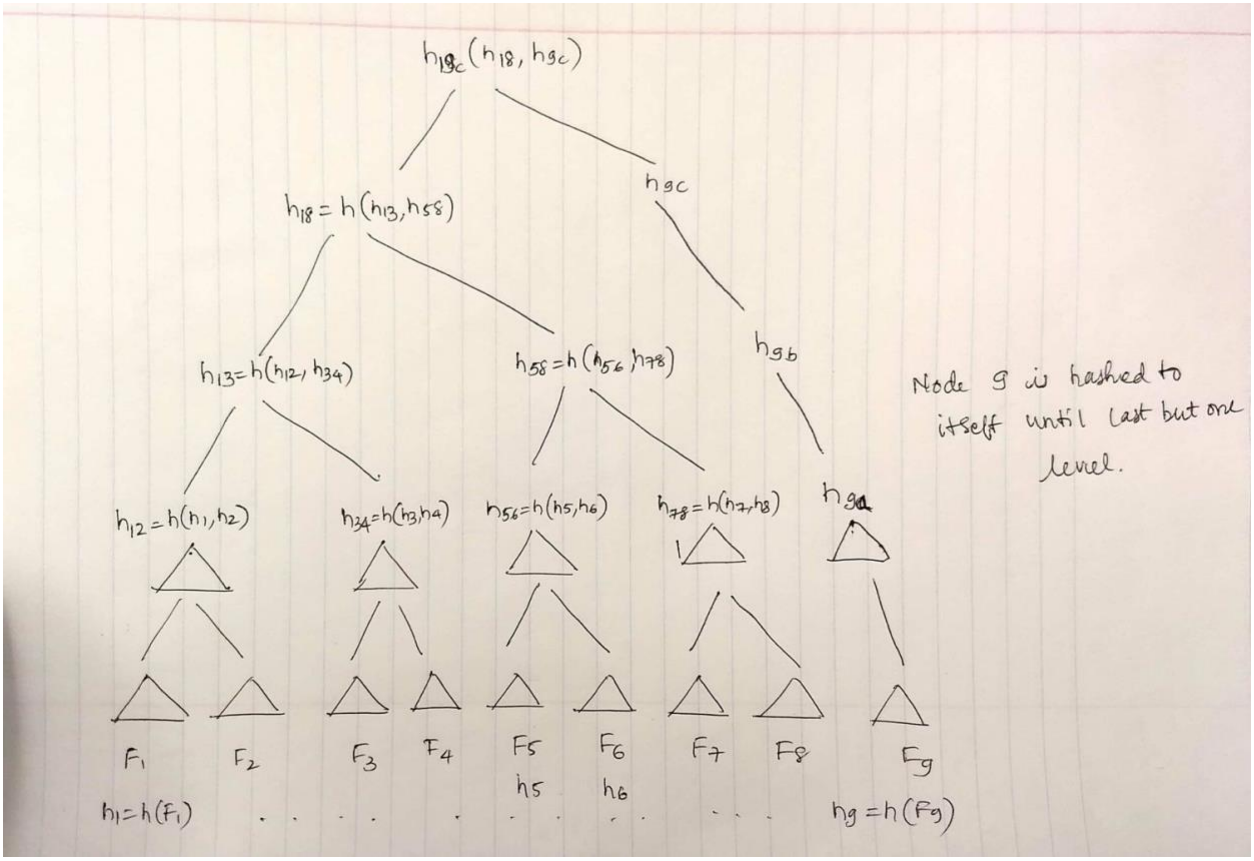
Q1. Hash functions can at times produce collisions (but very rare). The attacker can find a message the completely matches the hash value of the previous file and store it. Alice will not even notice as the hash values will be same.

There isn't an algorithm yet to that completely evades the possibility of collisions. The best algorithm to use as of today is SHA-256. It seems safe for the foreseeable future.

This attack can't be prevented. However, to minimize the possibility we can use key k which is derived from user's password to get the hash. If the attacker breaks into the system, he/she will not get k so they will not be able to manipulate the contents.

Q2a.



Q2b. If the creator of F6 needs to verify the identity, he will need following hash values,

- H5
- H78
- H13
- H9C

Steps:

- The H56 is calculated using H5 and H6.
- H78 needs to be provided. Using this H58 is calculated.
- H13 needs to be provided. Using this H18 is calculated.
- H9C needs to be provided. Using this H19C is calculated.