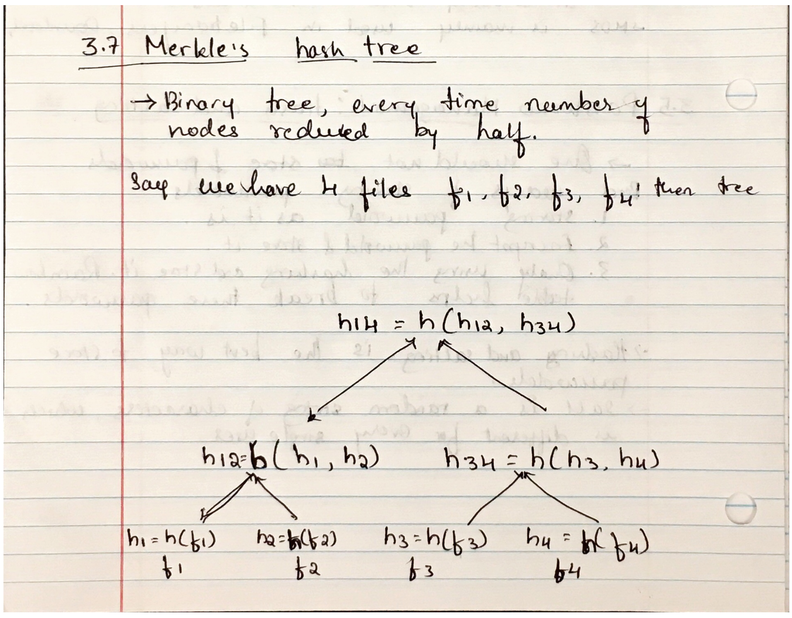
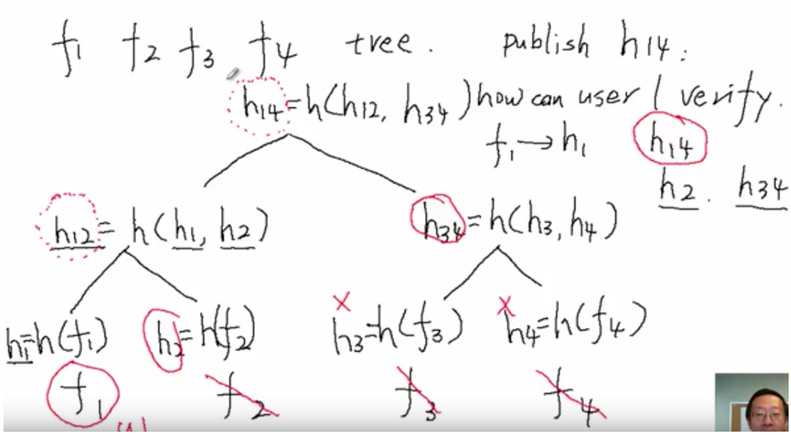
Property of a good Hash Function.

* Block 1: One way hash function.
  → Map variable length i/p string to fixed length string.
  * Easy to hash i.e. easy to get Hash(x) for x.
  * For any given H(x) it is almost impossible to get x
  * Almost impossible to have 1000 files say x & y having same hash.
  * Minor change in x, large change in Hash(x)

Merkle's Harsh Tree





- The beauty of the Merkle's hash tree is even the the user has h1, and provided with h2, h34, the file f2, f3 and f4 can't be found by hashes.

Real time example of Merkle's hash tree is to use in checking the integrity of online movie streaming sites, where they divide the whole file into f1,f2,..,f100.