Assignment 6

(a) Every DVD player has a header and body. The header contains the encryption of the content-key K under all keys K = {k_2, k_3,…..,k_{log2^n}} and the body contains the encrypted movie. Every DVD player contains a path from root to leaf node. Every dvd has a path, S_i from root to leaf node. As the hacker decrypted DVD r, he/she can decrypt all other DVD because he/she knows the kroot by decrypting kroot by content key, K of r. To prevent this, we take all siblings on the path of node r. Then we decrypt the movie by these siblings' keys. Now the DVD player, r cannot play the movie, but other can. As we take all siblings so the size of header will be $log2^n$.

(b) From (a), we can say that if one DVD is exposed then the header size will be $log2^n$. So if k DVDs are exposed then the header size will not be greater than $klog2^n$. From figure 1, node, R is exposed so we add three siblings' nodes(denoted by green color). And from figure 2, two nodes are exposed, so the header size will be four. So we can say, if k DVDs are exposed then the header size will not be greater than $klog2^n$

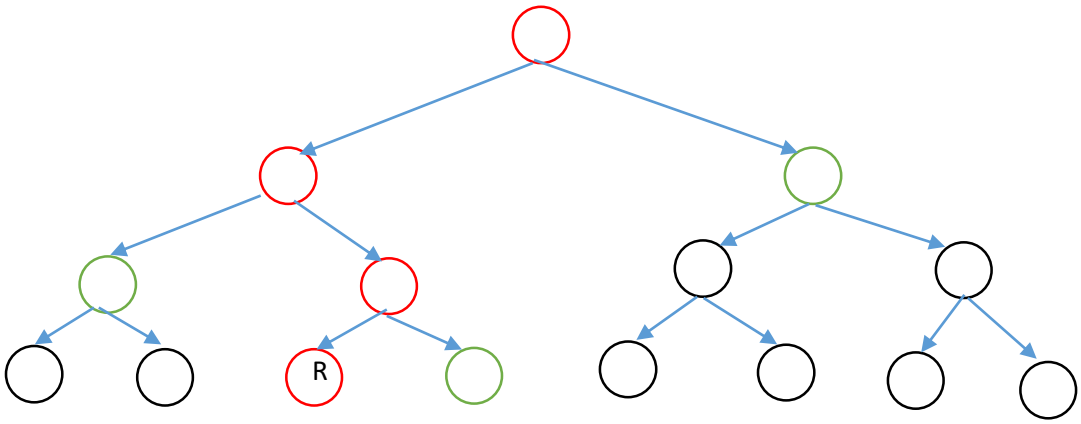

Fig 1: one dvd exposed

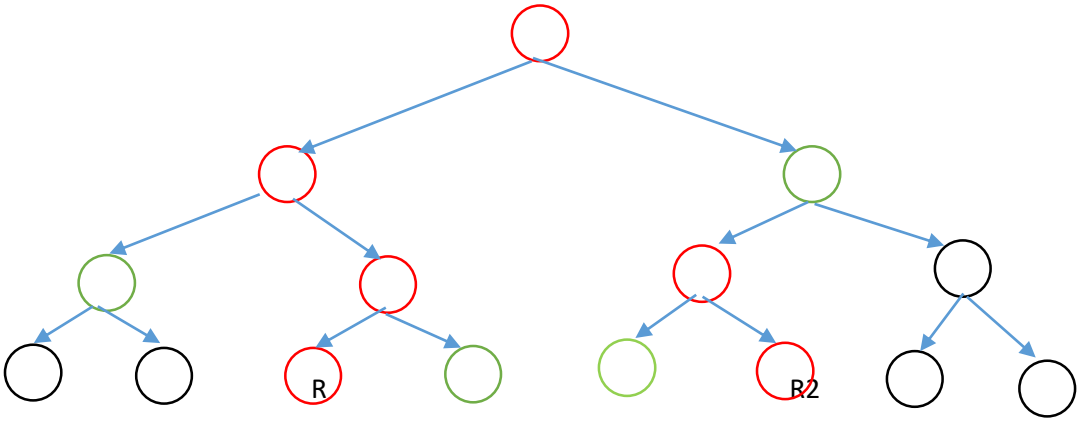

fig 2: two DVDs are exposed.