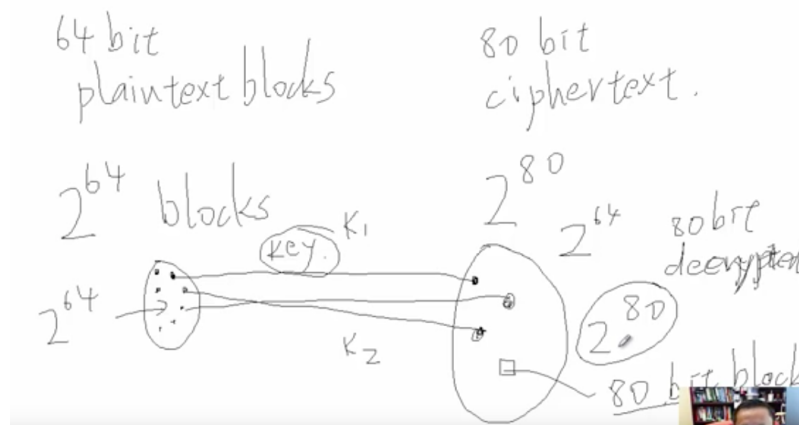


## 4.2 - Q and A about Hash and Symmetric Encryption: Part 2

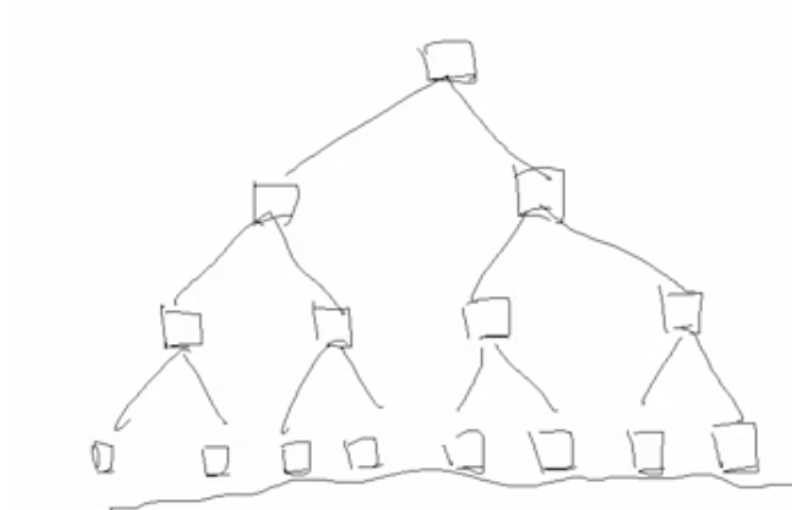
Q1) How the two files can have same hash results?

Ans: The number of files available are greater than  $2^{128}$ , so it is possible to find two files having same hash value. However, it will be difficult task.

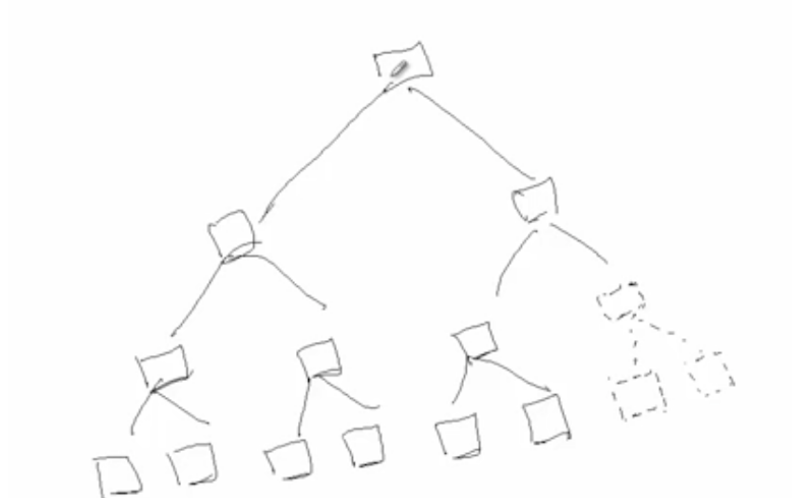
Q2)



Q3) What if the number of nodes in Merkel's hash tree are odd?

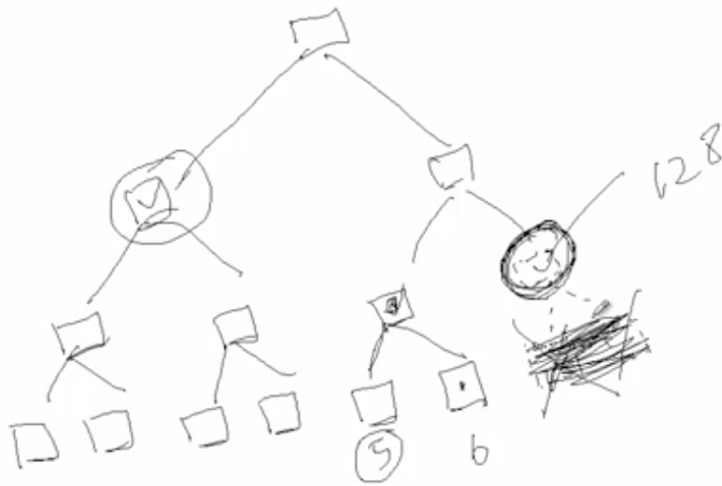


1. Generate Fake nodes.



Here we are adding two fake leaf nodes.

2. Generate the fake node only when required.



#### 4.2 Q & A part 2

Q1) We have 128 hash result.  
We have  $2^{128}$  possible hash values?  
How can two messages have same hash results?

Ans: Yes there are files with same hash values that is the reason we increase bit size.

Q2) How is it possible that a block cipher, that should have matching plain text and a cipher text blocks have a cipher text that is longer than the plaintext?

It is possible that cipher text is longer than plain text.

Q3) Question about Merkle's hash tree.

There are two approaches.

1. Generate two fake nodes.