

4.1 - Q and A about Hash and Symmetric Encryption: Part 1

Q1) Is it possible that you hash the same message twice and get different results?

Ans: If the hash function and message are same, then we get same result whenever we hash.

Q2)

hash more than 2^{128} files



3. 1, 6, 5, 5, 4, 2, 1, 6, 5

find a file (\hat{F})

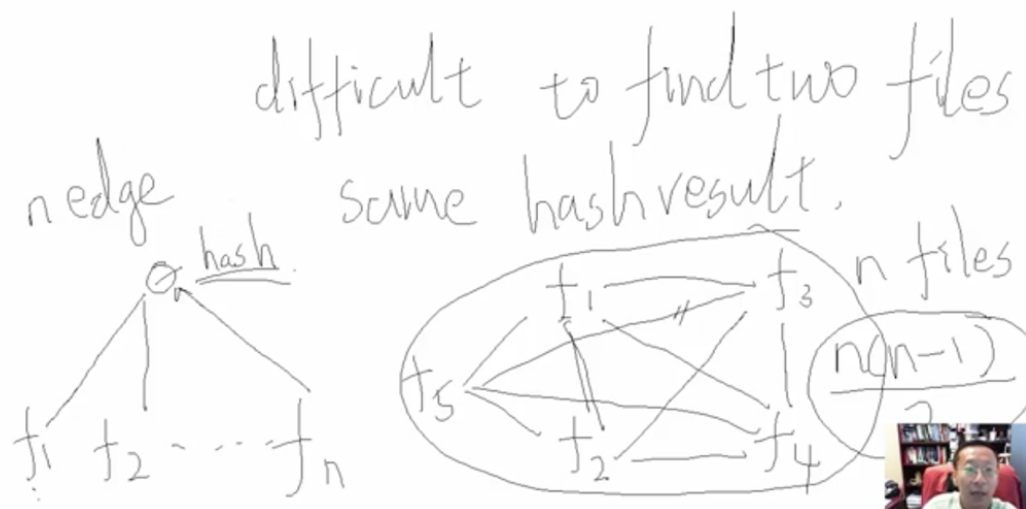
hash(F) = value I gave you.

128 bit

x, y, z, x,

There is no guarantee that we will find the hash value in 2^{128} files. However, we may find two some files have same results. However, that value is not we want.



4.1 Q and A Part 1

we have
Q2) 128 bit hash result.
∴ 2^{128} different hash result (possible hash values)
I give you hash result (128 bit) is it possible to find a file 'f' where
 $\text{hash}(f) = \text{given 128 bit hash}$.
Q:- How can it possible that to find such files we need to hash more than 2^{128} files?

Ans:- Remember Dice problem.

First Property of Hash Fun.	Second prop of hash Fun.
For a given hash you can't find file having same hash.	You can't find two files having same hash value. Two arbitrary files.

This makes a star shape. Comparing hash with every file.

This forms Network. edges

$$n \text{ files} = \frac{n(n-1)}{2}$$

Hash-collision

→ This is more demanding than star shape.