Cryptography and Network Security

AKASH KUMAR GANGWAR(20CS60R31)

12-nov-2020

1 Introduction

In this scribe we will learn about "Cryptographic Hash Function".These hash functions are used for integrity of information rather than confidentiality of information. In this scribe we are going to learn about build hash function and to analyse hash function.

2 Hash Function for Data Integrity

Cryptographic hash function are used for integrity of information. hash create a fingerprint of data means unique code which is said as "message digest" generally. message digest is generaly used for a large amount of data bits let's says x. and message digest is short binary strings of 160 bits which is shorter tha x.

If hash function of a data x is h(x) lets assueme y=h(x). now if we change x to x' means here we are altering x and it can be totally changed or a slight change. Then h(x) and h(x') will be not same (assume) and then alteration of data can be find by comparing y and y' where y'= h(x'). So by this way Hash function is used for data integrity/

These hash functions are used in "Digital Signature" and "Message Authentication Code (MAC)".

Here Data integrity and Digital Signature is showed using figure 1 and 2 respectively.

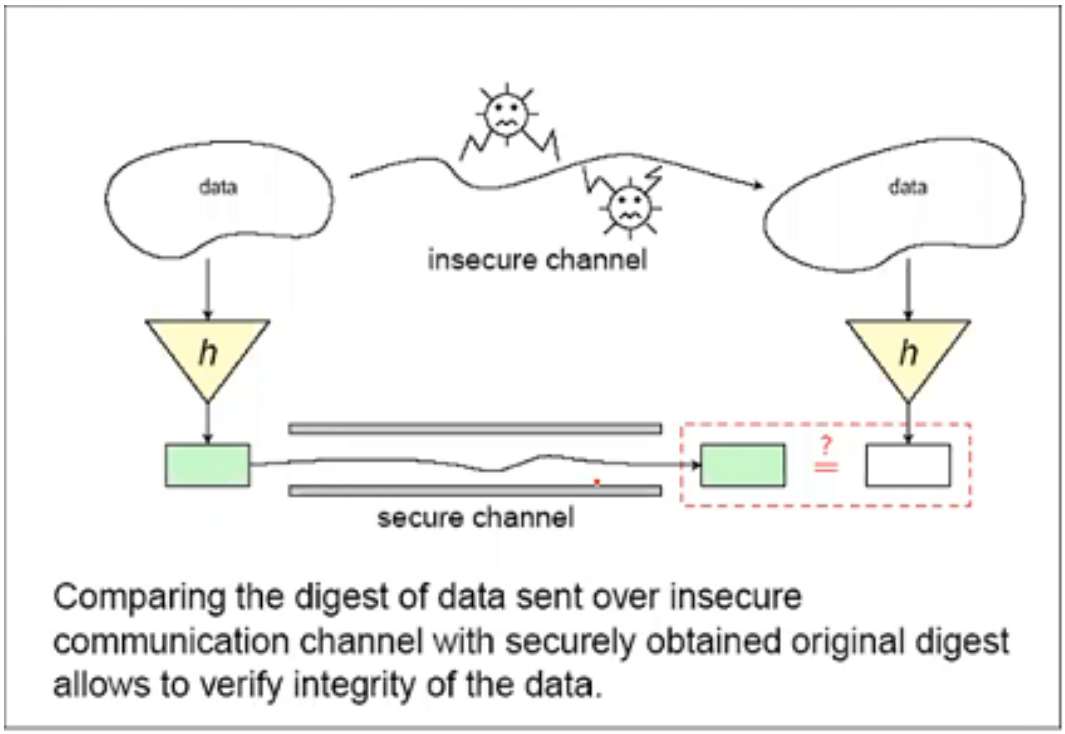

Figure 1: Application Data Integrity

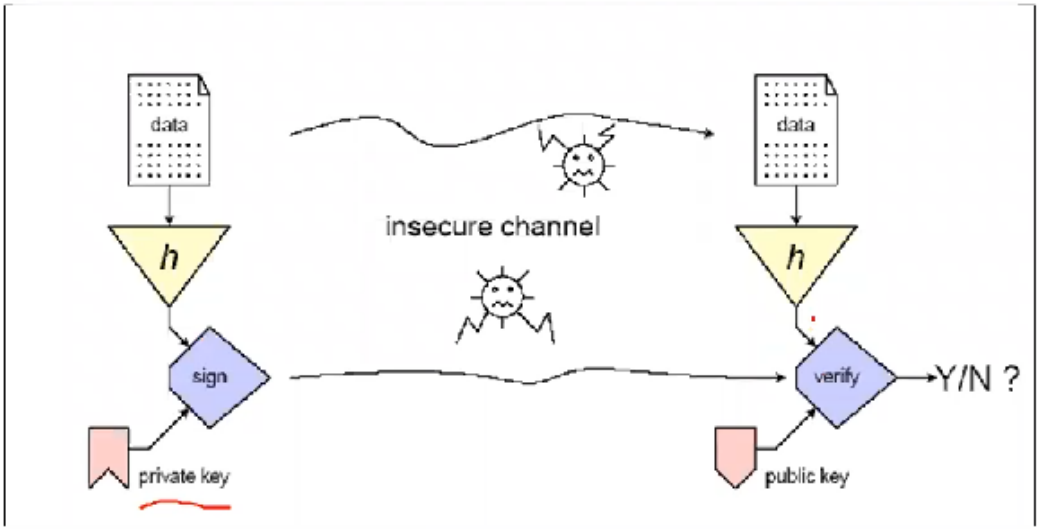

Figure 2: Application Digital Signature

3 A keyed Hash Function

In this hash function a secret k is used for computation of hash function.
y = $h_k(x)$

- Alice and Bob share secret key k
- Alice computes y on x using key k and sends to Bob
- Bob receives x' and compute y' on x' uskin same key k
- if y and y' are same then message is unaltered

4 Cryptographic Hash Family

A hash family is four-tuple (X, Y, K, H) where :-

- X is a set of possible messages
- Y is a finite sets of possible message digests.
- K is a key space which is finite set of possible keys.
- H is a set of hash function in which every $h_k : X \to Y$

Here X can be finite or infinite but Y is finite . If —X— = N and —Y—= M then there will be M^N possible functions from X to Y. And here any hash family $F \subseteq F^{X,Y}$ is known as (N, M) hash family.

5 Security of Hash Functions

There are three properties which are must for security of hash functions .

1. Preimage
2. Second Preimage
3. Collision

5.1 Preimage

In preimage property our goal is to find data x from a given hash function and hash . here h : $X \to Y$ and $y \in Y$ is given. and we have to find a x such that $x \in X$ and $h(x) = y$.

If we can find such x then (x,y) will be valid pair. otherwise h will be preimage resistant.

5.2 Second Preimage

In Second preimage property our goal is to find $x' \in X$ which is different from x and h(x) = h(x') from a given hash function h : $X \to Y$ and an element $x \in X$

If we can find such x' then (x' , h(x)) is valid otherwise hash is known as second preimage resistant.

5.3 Collision

In this property our goal is to find out two data elements x and x' which both belongs to X such that $x \neq x'$ and h(x) = h(x') where h is a given hash function from X to Y means h : $X \to Y$.

If such x and x' can be find then both (x, y) and (x', y) will be valid pair otherwise such hash function h is known as collision resistant.

Collision is defferent from Second preimage because there x was given and we have to find only x' but here we have to find both x and x' where x is random.

6 The Random Oracle Model

This is a model to analyse Hash function. It captures the concept of ideal hash function.

6.1 Ideal Hash Function

If a hash function h is ideal then the only way to compute the hash of a given value is by actually computing it even if many previous values are known.

6.2 A Non-Ideal Hash Function

If a hash function, h is computed the new hash value from pre-computed values without actually computing the hash value of given input then this is not what is an ideal hash function according to RO model.

- Oracle
  - This is not an algorithm nor any formula
  - We can imagine this as a giant book of random numbers and each page is is a value x and the nuumber written on that page is h(x)

7 Algorithms in The Random Oracle Model

These algorithms can be applied on all the hash functions as these are in Ro model so these will not depend on detains of hashing method. These algorithm makes random choice so these are randomized algorthms.

These algorithm may not work in all the cases but if these will work then there will will be correct computation and working and gives correct result. so these are example of **Las Vegas Algorithms**

Performance of these algorithm can be measured in two term ϵ and Q, where Q is the number of hash queries that are being used in hash computation and ϵ is the average case success probability that is averaged over all the problem instances.

7.1 Algorithm-Find Preimage

Algorithm 1: Find- Preimage(h,y,Q)

```
for each x ∈ x_0 do
    If h(x)=y then return(x)
returnFAILURE
```

- **Theorem** : for any $x_0 \in x$ with $|x_0| = Q$, the average case succees probability of above algorithm is ϵ = 1 - $(1 - 1/M)^Q$

Above theorem can be summarized as till $Q^t h$ there will be no match then probability will be $(1 - 1/M)^Q$ accoding to independence theorem. then probability that there will be atleast one match will be 1 - $(1 - 1/M)^Q$

8 Conclusion

In this scribe we study about cryptographic hash function and analysis of hash function with RO model and properties of hash function that it should follow to provide security i.e. preimage, second-preimage and collision. We also see how preimage algorithm works and any data x can be find by given hash function and hash value.