Sai Ram
20181CSE0621

02/06/2021

20181CSE0621
Sai Ram. K
6-CSE-10

Part-B

Q.4) **Hash Function:-**

An hash function is an algorithm that takes an arbitrary amount of data input, - a credential and produces a fixed sized output of enciphered text called 'Hash'. The enciphered text can be stored instead of the password itself & can be used to verify the user.

- Condenses message to fixed size $h = H(M)$
- Usually assume hash function is public
- Hash used to detect changes to message.
- Want a cryptographic hash function
  - Computationally infeasible to find data mapping to specific hash [one-way property]
  - Computationally infeasible to find two data to same hash [~~two way property~~]. which is collision free property.

—> Properties of Hash function:-

(1) Pre-Image resistance: It means that it should be hard to reverse a hash function

(2) Second Pre-Image resistance: It means that it should be hard to find different input with the same hash.

(3) Collision resistance: It should be hard to find any two different inputs x & y such that $h(x) = h(y)$