CNS
Assignment-5

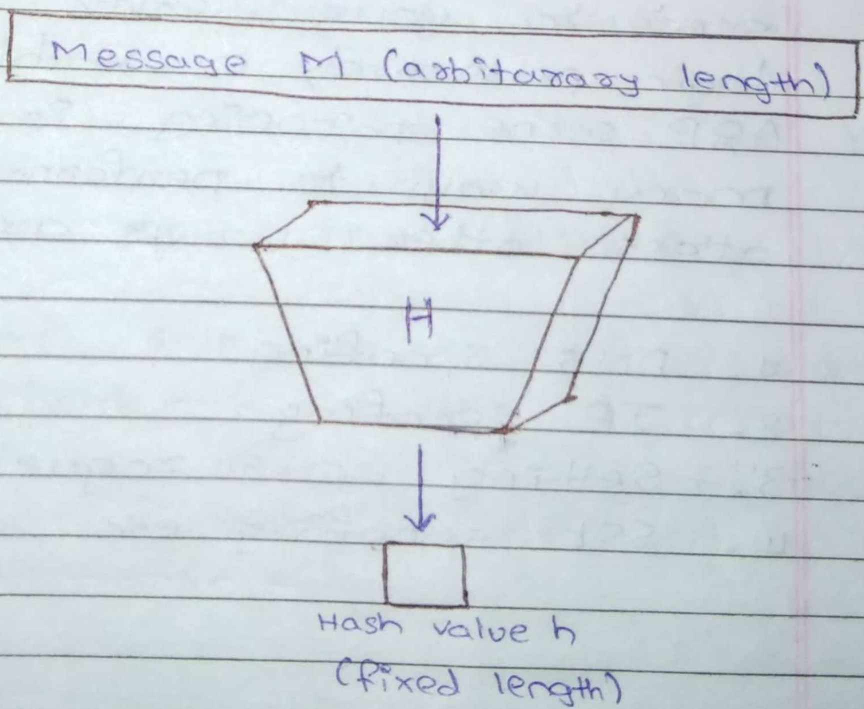
181240116001
Vishwas Acharya

1) Write about Cryptographic Hash Functions in detail.

Ans - Hash functions are extremely useful and appear in almost all information security applications.

- A hash functions is a mathematical function that converts a numerical input value into another compressed numerical value.
- The input to the hash function is of arbitary length but output is always of fixed length.
- Values returend by a hash function are called message digest or simply hash values.

• Figure :-



- **Features :-**

↳ Fixed Length Output (Hash Value)

- Hash function converts data of arbitrary length to a fixed length. This process is often referred to as hasing the data.
- In general, the hash is much smaller than the input data, hence hash functions are sometimes called compression functions
- Since a hash is a smaller representation of a larger data, it is also referred to as a digest.

↳ Efficiency of Operation

- Generally for any hash function h with input x, computation of h(x) is a fast operation.
- Computation hash functions are much faster than a symmetric encryption.

- **Properties :-**

↳ Pre-Image Resistance
↳ Second Pre-Image Resistance
↳ Collision Resistance

- **Applications :-**

- There are two direct applications of hash function based on its cryptographic propertie

↳ Password Storage
↳ Hash functions provide protection to password storage

↳ Data Integrity Check.
↳ It checks the most common application of the hash functions.

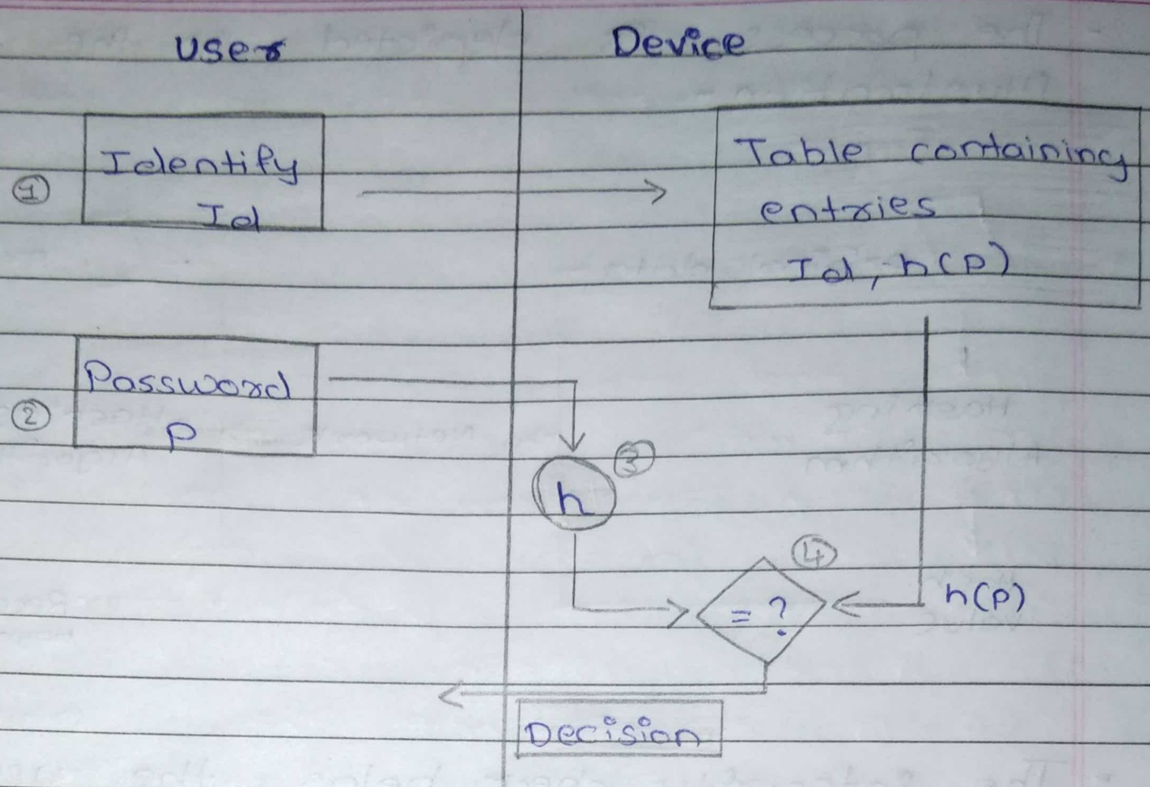
2) Explain Hash functions applications in detail.

Ans - There are two direct applications of hash fuction based on it's cryptographic properties.

- Password Storage

↳ Hash functions provide protection to password storage.

- Instead of storing password in clear, mostly all logon processes store the hash values of passwords in the file.
- The Password file consists of a table of pairs which are in the form (user id, h(p))
- The process of logon is depicted in the following illustration -



- An intruder can only see the hashes of passwords, even if he accessed the passwod.
- He can neither logon using hash nor can he derive the password from hash value since & hash function possesses the property of pre-image resistance.

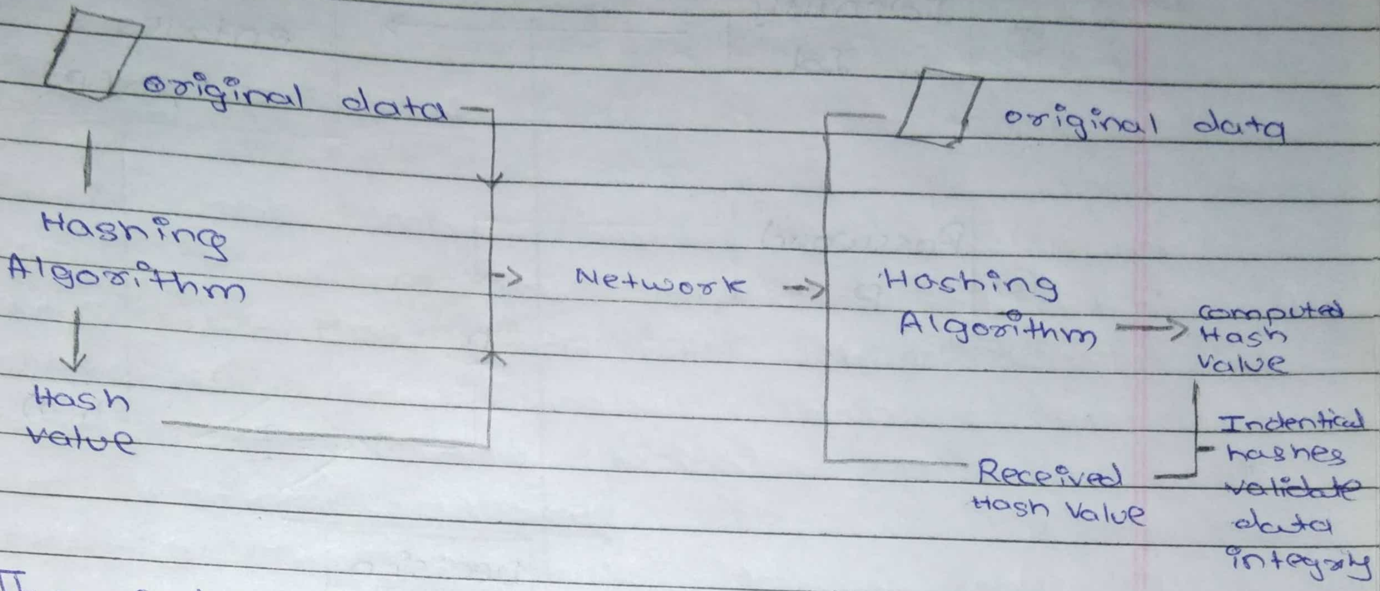
- **Data Integrity Check**

↳ Data Integrity check is a most common application of the hash functions.

↳ It is used to generate the checksums on data files.

↳ This application provides assurance to the user about correctness of the data.

- The process is depicted in the following illustration-

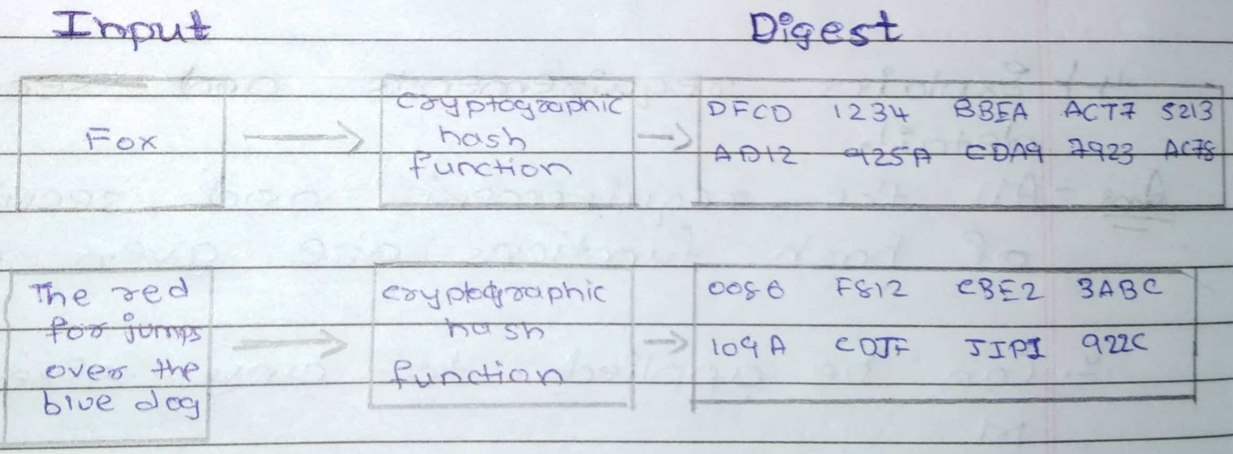


- The integrity check helps the user to detect any changes made ~~th~~ to original file.
- It however, does not provide any assurame about originalty.
- The attacker, instead of modifying file data, can change the entire file and compute all together new hash and send to the receiver.
- This integrity check application is useful only if the user is sure about the originality of files.

3) Explain SHA algorithm in detail.

Ans - A Secure Hash Algorithm is actually a set of algorithms developed by the National Institutes of standars and Technology (NIST) and other goverment and private parties. These secure encryption or "file check" functions have arisen have arisen to meet some of the top cybersecurity challengs of the 21st century, as a number of public servic groups work with federal goverment agencies to provide better online security standards for organizations and the pubic

- Figure:



- Characteristics:

- Cryptographic hash functions are utilized in order to keep data secured by providing three fundamental of characteristes which is consist of : pre-image resistance, second pre-image resistance, and collision resistance.

- Types of SHA

- There are many types of SHA, some of those family are SHA-0, SHA-1, SHA-2, SHA-3 and SHA-256, each of which was succeded increasingly stronger encryption and still being updated in response to hacker attack.
- SHA-0, for example, this is now absoloute due to widely exposed to the world.
- Because there are too many types of SHA algorithms, in this article I will just point out few of those types

4) Explain requirements and security in detail.

Ans - All the requirements and security ~~in~~ of hash functions are given further.

1. Can be applied to any sized message M
2. Produces fixed-length output h.
3. It is easy to compute h=H(M) for any message M.
4. Given hash value h is infeasible to find y such that (H(y)=h)
   - One way property.

5. For given block x, it is computational infeasible to find $y \neq x$ with $H(y) = H(x)$
   - weak collision resistance
6. It is computationally infeasible to find messages m1 and m2 with $H(m1) = H(m2)$
   - strong collision resistance.