Network Security

- SCSA1603

Name: Mohnish Devaraj

Reg No: 39110636

Assignment-II

PART-A

1. Traffic Analysis
2. Message Authentication
3. Encrypted
4. his or her own private key
5. 160 bits

PART-B

6. Hash function requirements:

- H can be applied to a block of data of any size
- H produces a fixed length output
- H(x) is relatively easy to compute
- For any given code h, it is computational infeasible to find x such that H(x)=h
- For any given block x, it is completely infeasible to find y x with H(y)=H(x).
- It is computationally infeasible to find any pair (x,y) such that H(x) = H(y).

⑦ Message Authentication Code

A message authentication code (MAC) or tag, is a security code that is typed in by the user of a computer to ~~ates~~ access accounts or portals. The code is attached to the message or request sent by the user.

⑧ Hash function is a function that has a huge role in making a System secure as it converts normal data given to it as an irregular value of fixed length. ~~[illegible]~~ when we put data into this function it outputs an irregular value. The irregular value it outputs is known as "Hash Value". Hash values are simple numbers but are often written in Hexadecimal.

⑨ The two applications of authentication functions are:

→ Multi factor Authentication

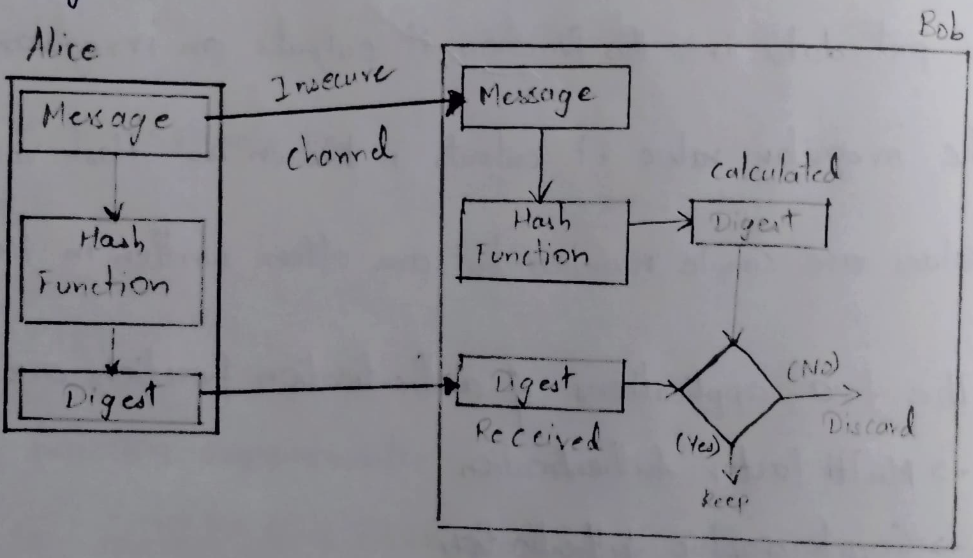
→ Cryptographic Authentication

⑩ Destination repudiation:

Danial of receipt of message by destination. Message authentication is a procedure to verify that received messages come from the alleged source and have not been altered. Message authentication may also verify sequencing and time liners.

PART-C

(11) Message Digest is used to ensure the integrity of a message transmitted over an insecure channel (where the content of the message can be changed). The message is passed through Crypotographic hash function. This function creates a compressed image of the message called Digest



This message and digest pair is equivalent to a physical document and finger print of a person on that document. Unlike the physical document and the finger print, the message and the digest can be sent seperatly:

- Most importantly, the digest should be unchanged during the transmission.
- The cryptographic hash function is a one way function, that is, a function which is practically in feasible to invert. This cryptographic hash

function takes a message of variable length as input and creates a digest/hash/finger print of fixed length, which is used to verify the integrity of the message.

- Message digest ensures the integrity of the document. To provide authenticity of the message, digest is encrypted with sender's private key. Now this digest is called digital signature, which can be only decrypted by the receiver who has sender's public key. Now the receivers can authenticate the sender and also verify the integrity of the sent message.