Lecture 4 🪴

> **Class**: Implementing Integrity and Message Authentication
>
> **Date**: 9.14 AM , 11 Nov
>
> **Author**: Lasal Hettiarachchi

Key learnings:

- Cryptographic hash functions
- How authenticity and integrity with hash functions
- Attacks possible in hashing

Integrity

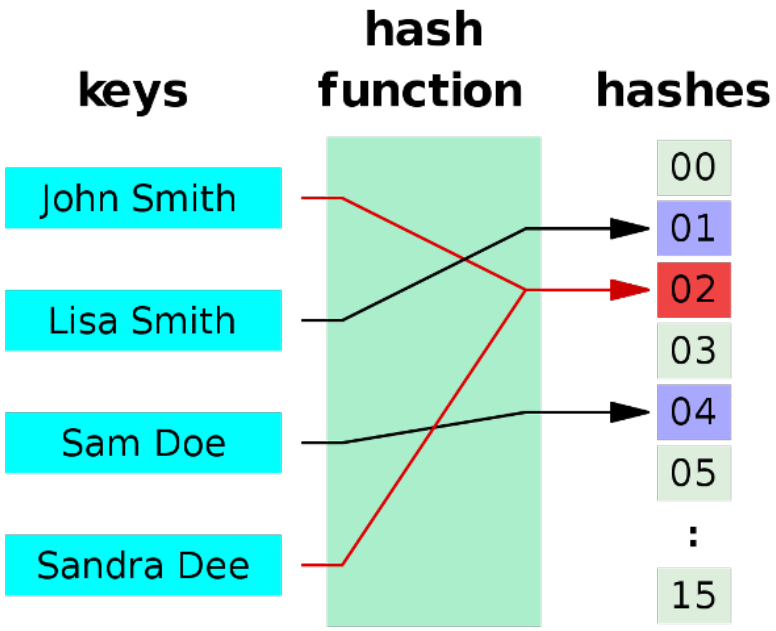
- Data are not modified without proper autherization.
- Accidental or malicious
- Two main areas for data compramise:
  - Accuracy - data changed
  - Completeness - data is not changed but the entire dataset is not recieved and has errors in the packets
- attack on integrity is much more severe than confidentiality and availability

What can be done to ensure integrity over a network

- We cannot ensure that a message is not tampred with in a network
- Threrefore integrity in a network is ensured not through prevention but through detection and retransmission

Hash Functions

- Cryptographic primitive: low-level cryptographic algorithms that are used to build more complex security systems.
- Mathematical algorithm that maps data of arbitrary size ("message") to a bit string of a fixed size ("hash value" or "message digest").
  - Ex: CRC in ethernet
  - Many inputs may map to one digest.
  - We can go from message→ Hash
  - But the other way is not possible
  - in encryption we can go both ways



John and Sandra maps to the same hash

Cryptographic Hash Functions

1. Deterministic: Input only should determine the output (Same message a million times should give one output)
2. Averlanch effect: Small change to the message should change the hash drastically
3. Efficient : One way hashes are used since it is computational heavy
4. Pre-image resistance: it is difficult to generate a message that yields a given hash value
5. Second Pre-image resistance: It is also difficult to find a message that matches a given messages hash (Second Pre-image resistance)
6. Collision resistance: it is difficult to find two different messages with the same hash value

Degree of difficulty

In cryptographic practice "difficult" generally means "almost certainly beyond the reach of any adversary who must be prevented from breaking the system for as long as the security of the system is deemed important"

Uses of hash functions

- Can be used to verify the integrity of messages and files
- Digital Signature generations for non rupidiation
- Password verification
- Proof of work in clock chains

Examples

- MD2 (Message Digest)

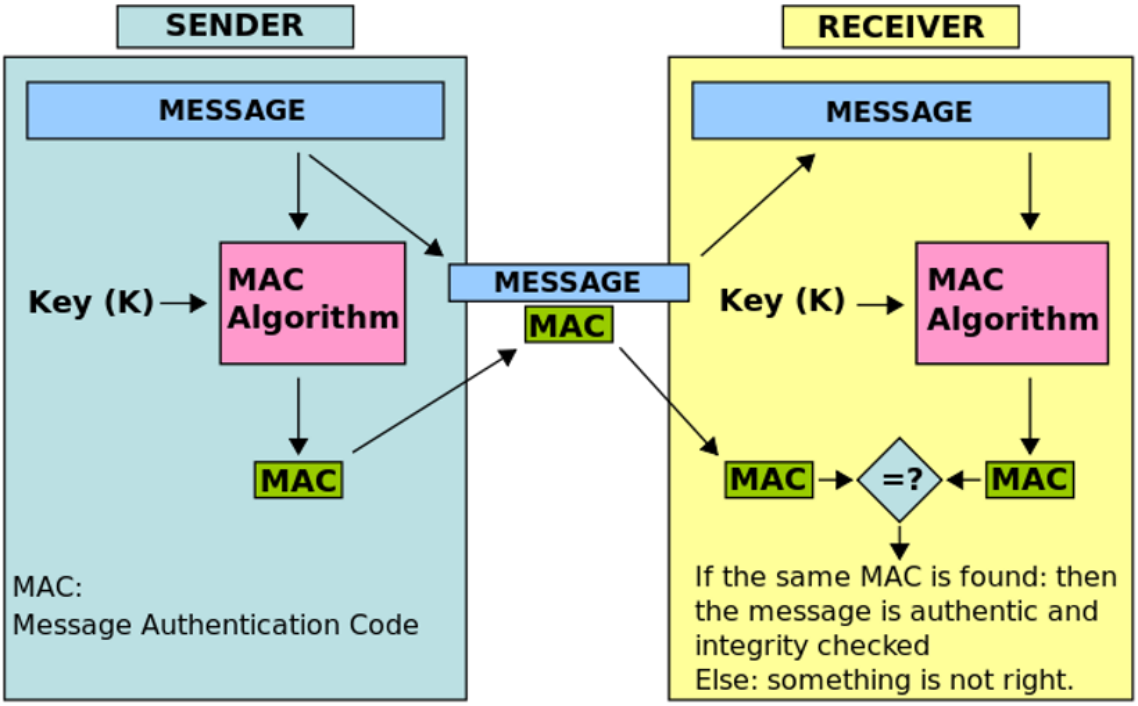
    - works on a message of 16 bits and create a digest of 128 bits
- MD4 (Message Digest)
    - message length can be (512)N -64 and create a 128 bit hash.
    - No longer secure
- MD5
    - also prcesses 512 bit block input
    - Chained blocked hash
    - Was proven to be subjected to collision(2 messages can be found matching the same hash)
- SHA - 1
    - NIST developed
    - Similar to MD 5
- SHA - 2
    - block length and tha hash length are higher
    - But algorithm is same
- SHA - 3
    - Only algorithm that is secured for cryptographic use

Application

- Message authentication
    - Hash and the message are both sent and they are seperated.
    - Sender authentication
    - Message Authentication Code (MAC)

Message Authentication Code (MAC)

- MAC uses a keyed hash
- A symmetric key is input in addition to the message when generating the hashes
- The key must be shared in secret between the sender and receiver
- This does not provide Confidentiality

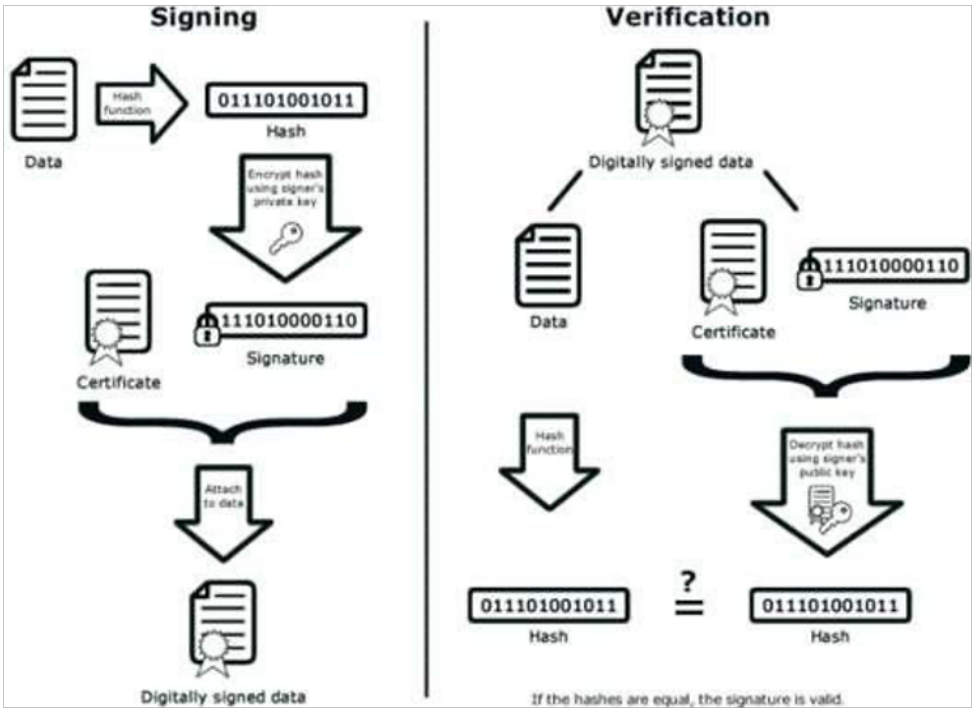


- Non Rupidiation
  - Used to create trust between communicators
  - Original sender cannot deny sending the message
  - Digital signature:
    - Uses assymertric key encryption

Digital signatures

Classes of digital signatures

- Class 1: . Signatures provide a basic level of security and are used in environments with a low risk of data compromise.
- Class 2: e-filing , tax documents. Authenticate a signees signature against a preverified database.Class 1 signatures provide a basic level of security and are used in environments with a low risk of data compromise.
- Class 3: The highest level of digital signatures. Class 3 signatures require a person or organization to present in front of a certifying authority to prove their identity before signing. Class 3 digital signatures are used for e-auctions, e-tendering, e-ticketing, court filings and in other environments where threats to data or the consequences of a security failure are high. Lika an IAM system



- Data is encrypted with a hash (Not a keyed hash but cryptographic hash)
- Then encrypt with your private key (Signature: Hash encrypted with the private key)
- Certificate has the public key issued by the company that checks

- decompose the message to data certificate and the signature
- certificate and signature decrypted from the public key of the reciever
- compare the hashes

For this to happen we need an organization trusted by both parties to issue the certificate.

Public Key Infrastructure

- Allows unknown people to authenticate and their messages to each other
- Provides
  - integrity
  - Confidentiality
  - Authentication (message and sender)
  - Non repudiation

  Disadvantages
  - Requires the considerably more resource intensive asymmetric key encryption
  - Requires a robust digital key infrastructure
  - Requires a trusted third party to act as key/certificate authority