Sunil
DATE
PAGE
"Rough 'n' Fair"

Message Authentication & Hash Functions

Message Authentication Requirements

Revelation
It means releasing the content of the message to someone who does not have an appropriate cryptographic key.

Analysis of Traffic
Determination of the pattern of traffic through the duration of connection and frequency of connections between different parties

Deception
Adding out of context messages from a fraudulent source into a communication network. This will lead to mistrust between the parties communicating and may also cause loss of critical data.

Modification in the Content
Changing the content of a messages between parties. This includes insertion, deletion and reordering of messages.

Modification in the timings
This includes replay and delay of messages

sent between different parties. This way session tracking is also disrupted.

Repudiation
- Source Refusal
  When the source denies being the originator of a message
- Destination Refusal
  When the receiver of the message denies the reception

(8) Authentication Functions
(9) Message authentication is a procedure to verify that received message come from the alleged source and have not been altered. Message authentication may also verify sequencing and timeliness.
A digital signature is an authentication technique that also includes measures to counter repudiation by either source or destination.

All message authentication and digital signature mechanisms are based on two functionality levels

Lower Level: At this level, there is a need for a function that produces an authenticator, which is the value that will further help in the authentication of a message.

Higher Level: The lower level function is used here in order to help receivers verify the authenticity of messages.

These messages authentication functions are divided into three classes

1) Message Encryption
While sending data over the internet there is always a risk of a Man in the Middle (MITM) attack. A possible solution for this is to use message encryption. In Message encryption data is first converted to a ciphertext and then sent any further. Message Encryption can be done in two ways
Symmetric Encryption
Public Key Encryption

2) Message Authentication Code (MAC)
A message authentication code is a security code that the users of a computer has to type in order to access any account or portal. These codes are recognized by

the system so that it can grant access to the right users. These codes help in maintaining information integrity. It also confirms the authenticity of the message.

3) Hash function

A hash function is nothing but a mathematical function that can convert a numeric value into another numeric value that is compressed. The input to this hash function can be of any length but the output is always of fixed length. The values that a hash function returns are called the Message digest or hash values.

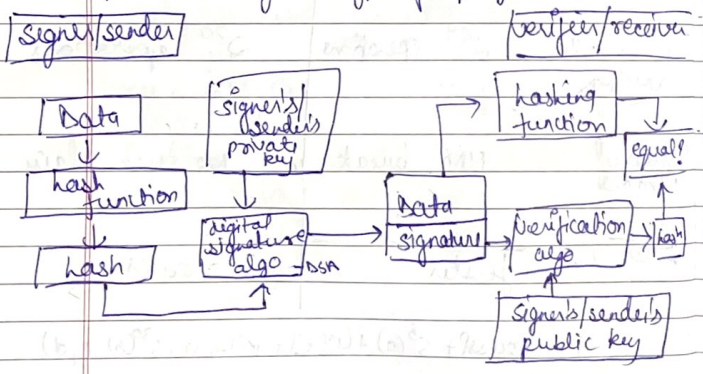
Digital Signature

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software, or digital document

Digital signature is the cryptographic value that is calculated from the data and a secret key known only by the ~~receiver~~ signer.

The receiver of msg needs assurance that the msg belongs to the sender and he should not be able to repudiate the origination of that message.

The digital signature is based on public key cryptography.



- private key used for signing is called signature key
- public key used is called verification key
- Sender gives the data to hash function and generates hash of data (digest)
- hash value and signature key are then given to DSA to produce digital signature. signature is appended to the data and sent to the receiver
- receiver gives the digital signature and verification key to verification algo which gives some value as output
- receiver uses hash function on received data to produce hash value

if the hash value and output of the verification are equal then the digital signature is valid. else not

Note: signing a hash is more efficient than signing the entire data.

Sunil
DATE
PAGE
"Rough 'n' Fair"

Digital signature has the ability to provide non-repudiation of message it also provide message authentication and data integrity.

① Message authentication
When the receiver validates the digital signature using public key of a sender he is assured that the signature has been created only by sender who posses the corresponding private key and no one else

② Data integrity
In case an attacker has the access to data and modifies it, the digital signature verification at receiver end will fail.
The hash of modified data and output by verification algo will not match
∴ receiver can deny the req assuring the data integrity has been breached.

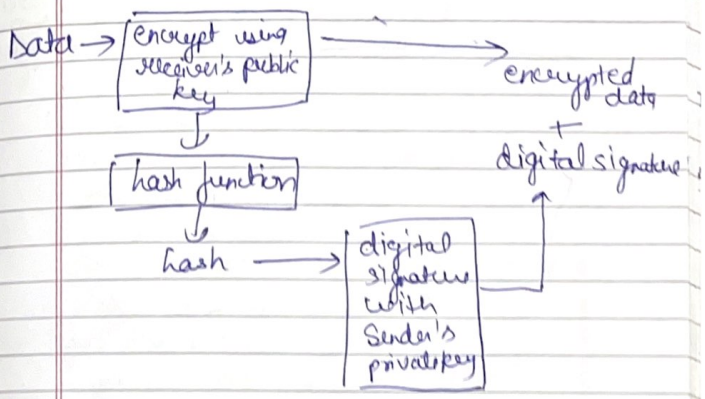
③ Non-repudiation
receiver can present data and digital signature to the third party if any dispute arises in the future as an evidence

encryption with digital sign

Sunil
DATE
PAGE
"Rough 'n' Fair"

To achieve confidentiality encrypted messages are to be exchanged rather than plain text.

sender's side



receiver first validates the signature, after ensuring the validity of the signature, he then retrives the data through the decryption using his private key