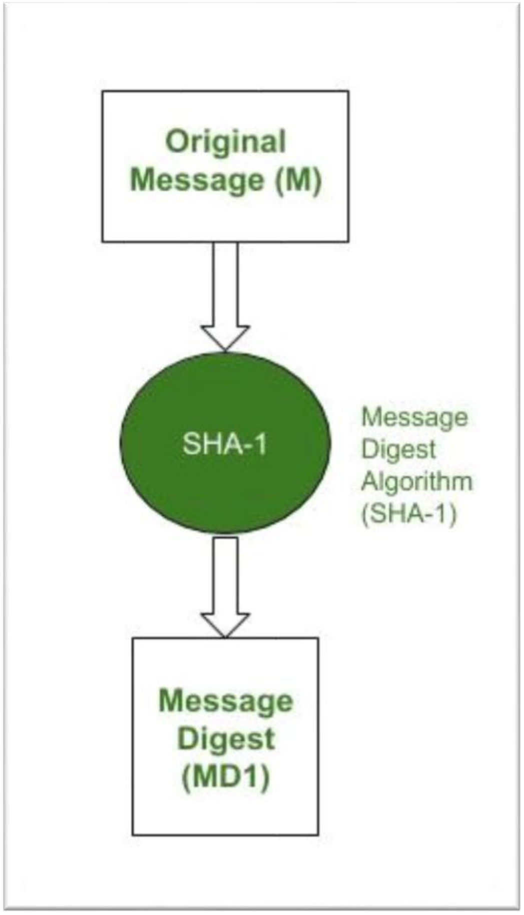
RSA and Digital Signatures

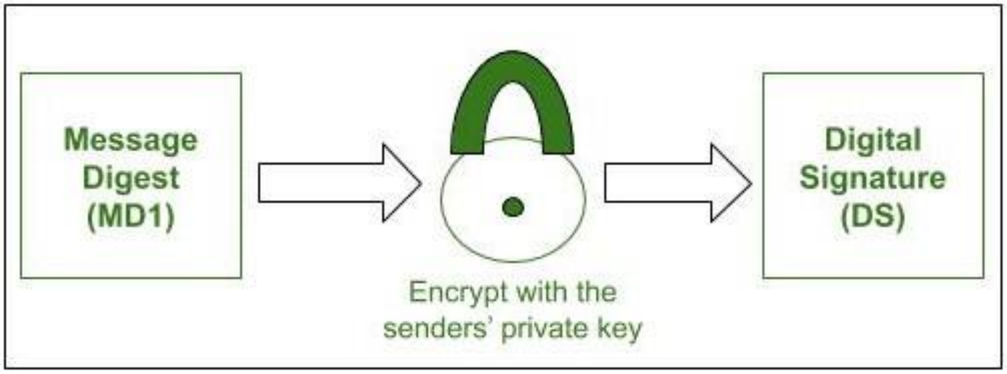
Digital Signature : As the name suggests are the new alternative to sign a document digitally. It ensures that the message is sent by the intended user without any tampering by any third party (attacker). In simple words, digital signatures are used to verify the authenticity of the message sent electronically.

RSA : It is the most popular asymmetric cryptographic algorithm. It is primarily used for encrypting message s but can also be used for performing digital signature over a message. Let us understand how RSA can be used for performing digital signatures step-by-step. Assume that there is a sender (A) and a receiver (B). A wants to send a message (M) to B along with the digital signature (DS) calculated over the message. **Step-1 :** Sender A uses SHA-1 Message Digest Algorithm to calculate the message digest (MD1) over the original message M.



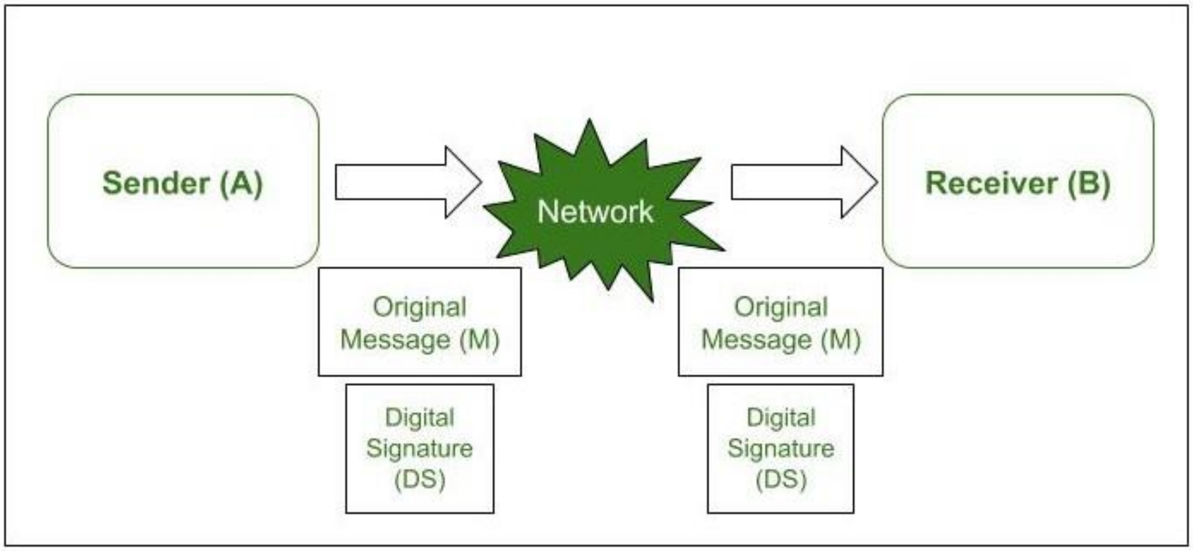
Message digest calculation

Step-2 : A now encrypts the message digest with its private key. The output of this process is called Digital Signature (DS) of A.



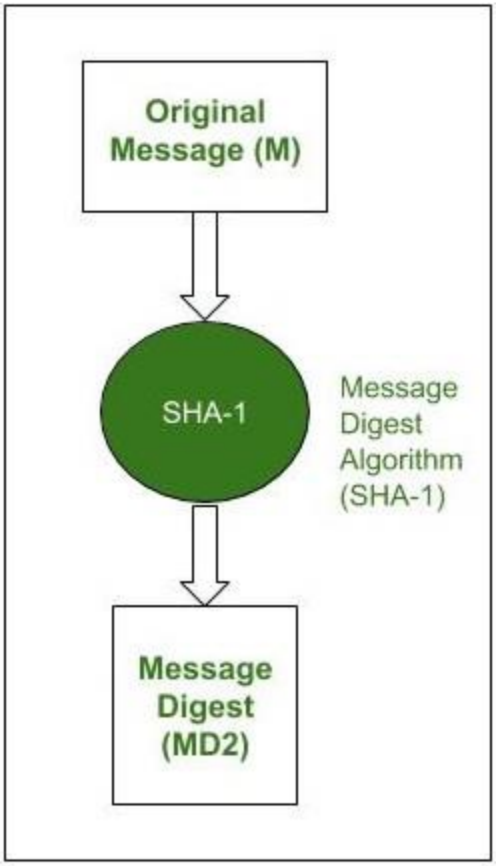
Digital signature creation

Step-3 : Now sender A sends the digital signature (DS) along with the original message (M) to B.



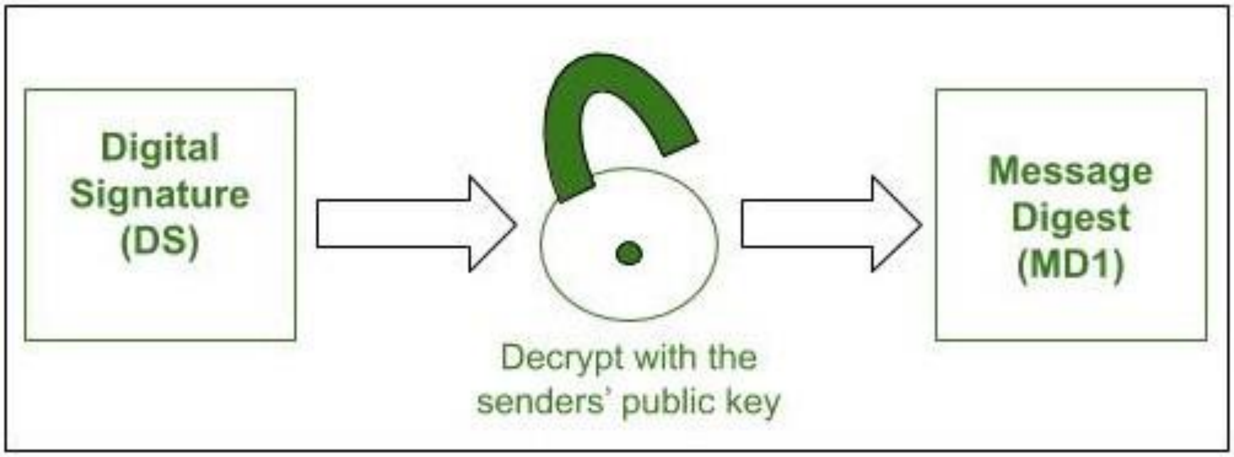
Transmission of original message and digital signature simultaneously

Step-4 : When B receives the Original Message(M) and the Digital Signature(DS) from A, it first uses the same message-digest algorithm as was used by A and calculates its own Message Digest (MD2) for M.



Receiver calculates its own message digest

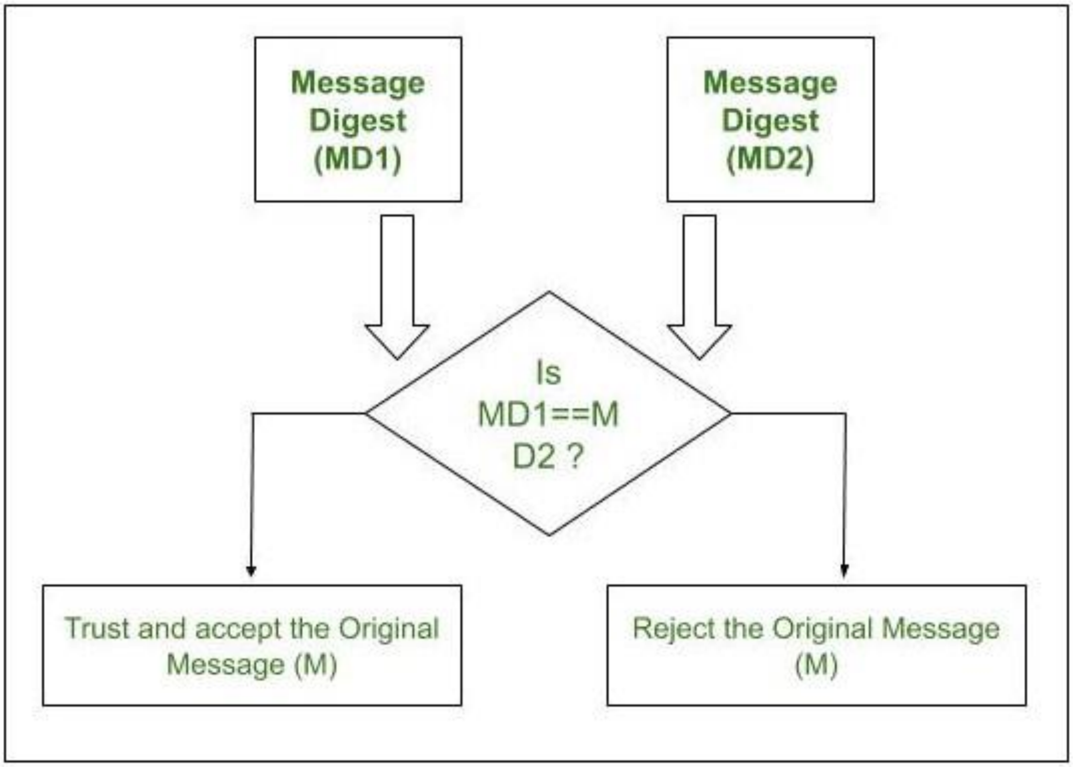
Step-5 : Now B uses A’s public key to decrypt the digital signature because it was encrypted by A’s private key. The result of this process is the original Message Digest (MD1) which was calculated by A.



Receiver retrieves sender’s message digest

Step-6 : If MD1==MD2, the following facts are established as follows.

- B accepts the original message M as the correct, unaltered message from A.
- It also ensures that the message came from A and not someone posing as A.


Message Digest (MD1)
Message Digest (MD2)
Is MD1==MD2 ?
Trust and accept the Original Message (M)
Reject the Original Message (M)

Digital signature verification