DS Digital Signature

A digital signature is an electronic signature that is used to authenticate the identity of the sender of a message or document and to ensure that the original content of the message or document that has been sent is unchanged. It functions as a way of confirming the authenticity and integrity of a digital message or document, similar to a handwritten signature on a physical document. Digital signatures use encryption and authentication algorithms to secure the signature and can be verified using public key infrastructure (PKI).

DS use of hash function in Digital signature

Hash functions play a critical role in digital signatures. A hash function is a one-way mathematical function that takes an input (i.e., a message or document) and produces a fixed-length output, called a hash or digest. In the context of digital signatures, the hash function is used to generate a unique representation of the original message or document, which is then encrypted with the sender's private key to create the digital signature.

When the recipient receives the signed message, they use the sender's public key to decrypt the signature and retrieve the original hash value. They then generate their own hash of the received message and compare it to the original hash value. If the two hashes match, it indicates that the message has not been tampered with and came from the sender whose public key was used to verify the signature.

In this way, the use of hash functions in digital signatures helps to ensure the integrity and authenticity of the message being sent.