DIGITAL SIGNATURE

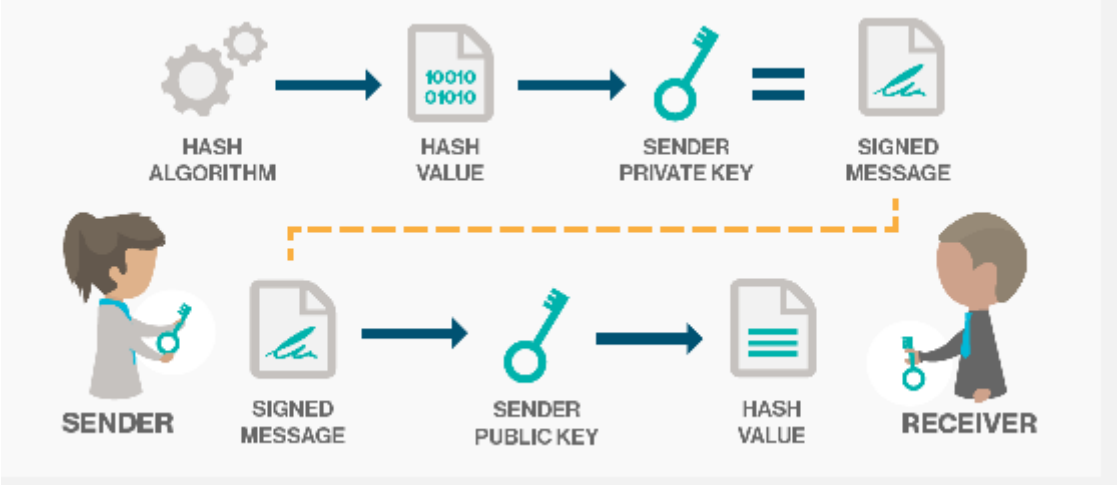
DIGI PAGE

Subject - Computer

Date of Release - 05-NOV-2017

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

The digital equivalent of a handwritten signature or stamped seal, but offering far more inherent security, a digital signature is intended to solve the problem of tampering and impersonation in digital communications.



Digital signatures can provide the added assurances of evidence to origin, identity and status of an electronic document, transaction or message, as well as acknowledging informed consent by the signer.

Digital signatures are based on public key cryptography, also known as asymmetric cryptography.

Using a public key algorithm such as RSA, one can generate two keys that are mathematically linked: one private and one public.

To create a digital signature, signing software (such as an email program) creates a one-way hash of the electronic data to be signed. The private key is then used to encrypt the hash. The encrypted hash -- along with other information, such as the hashing algorithm -- is the digital signature.

The reason for encrypting the hash instead of the entire message or document is that a hash function can convert an arbitrary input into a fixed length value, which is usually much shorter. This saves time since hashing is much faster than signing.