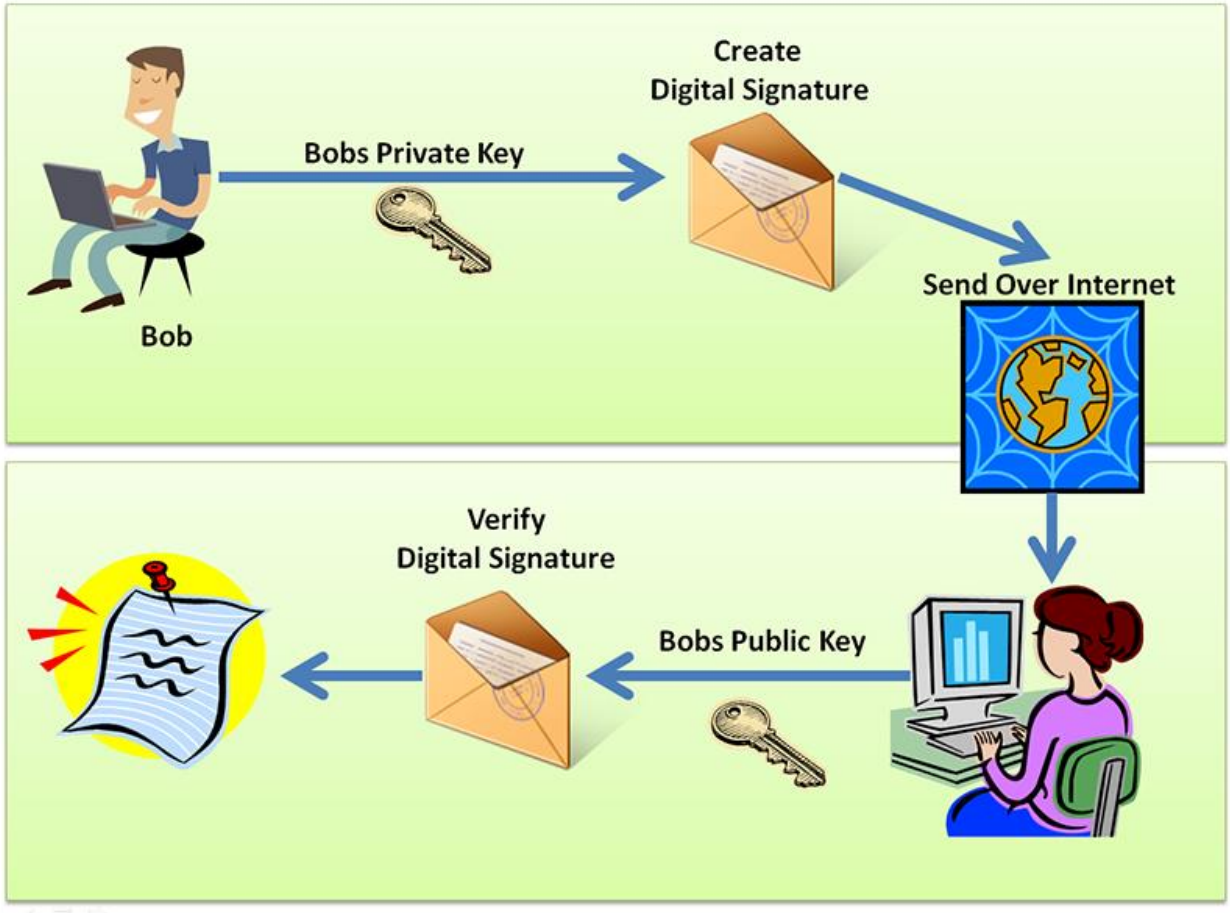
Basics of Digital Signature

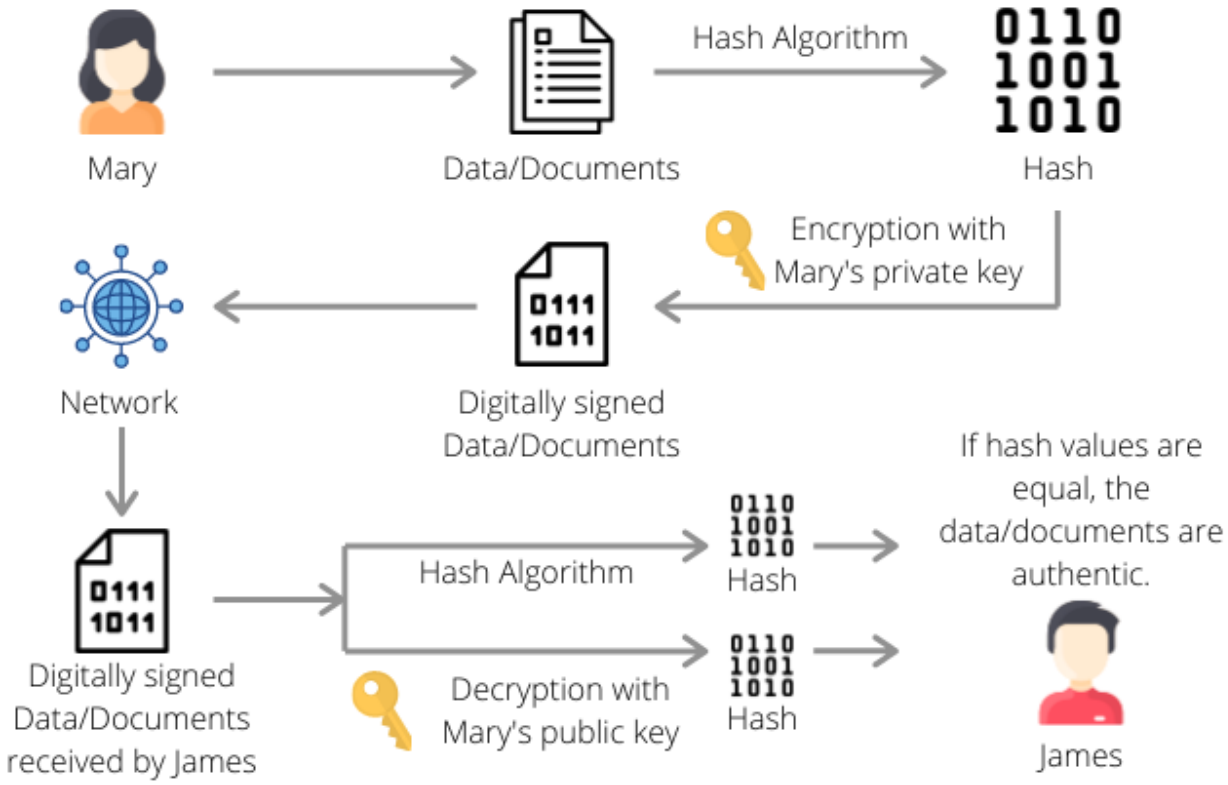


Digital Signature is a type of electronic signature that encrypts documents with digital codes that are particularly difficult to duplicate. **In case of digital signature**, message is encrypted with the private key and decrypted with the public key.

A digital signature is a mathematical method for confirming the veracity and consistency of a digital message, document, or piece of software. It gives much more intrinsic security than a handwritten signature or stamped seal, yet it is the digital version of them. The issue of tampering and impersonation in digital communications is addressed by a digital signature.

Public key cryptography, commonly referred to as asymmetric cryptography, is the foundation of digital signatures. Two keys are generated, one private and one public, using a public key algorithm like RSA. This results in a pair of keys that are mathematically connected. Public key cryptography's two mutually authenticating cryptographic keys are how digital signatures function. The person who generates the

digital signature uses a private key to encrypt the data associated with the signature for encryption and decryption. With the signer's public key, that data can only be decrypted. The signature or the document may be flawed if the recipient is unable to open the file using the signer's public key. Digital signatures are verified in this way.



To create a digital signature, signing software is used to provide a one-way hash of the electronic data to be signed.

A hash is a fixed-length string of letters and numbers generated by an algorithm. The digital signature creator's private key is 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 because a hash function can convert an arbitrary input into a fixed-length value, which is usually much shorter. This saves time, as hashing is much faster than signing.

The value of a hash is unique to the hashed data. Any change in the data, even a modification to a single character, results in a different value. This attribute enables

others to use the signer's public key to decrypt the hash to validate the integrity of the data.

If the decrypted hash matches a second computed hash of the same data, it proves that the data hasn't changed since it was signed. But, if the two hashes don't match, the data has either been tampered with in some way and is compromised or the signature was created with a private key that doesn't correspond to the public key presented by the signer. This signals an issue with authentication.

Digital certificates, also called public key certificates, are used to verify that the public key belongs to the issuer. Digital certificates contain the public key, information about its owner, expiration dates and the digital signature of the certificate's issuer. Digital certificates are issued by trusted third-party certificate authorities (CAs). The party sending the document and the person signing it must agree to use a given CA.