# Digital Signature Algorithm (DSA)

The Digital Signature Algorithm (DSA) is a Federal Information Processing Standard for digital signatures.

- A digital signature algorithm is a subset of the digital signature standard that represents a specific public key algorithm that is used only as a digital signature.
- The key runs on the message hash generated by SHA-1: To verify a signature, recalculate the message's hash, use the public key to decrypt the signature and then compare the results.

- The implementation of a digital signature is usually done by the sender of the message through a one-way function to process the message to be transmitted to produce a string of digits that can not be forged by another person to authenticate the source of the message and to detect whether the message has been modified.
- The message receiver decrypts the received message encrypted with the sender's private key with the sender's public key, and determines the source and integrity of the message, and the sender can not deny the signature.