

Digital Signature Algorithm

- In order to ensure the security of data transmission, we have to take a series of security technologies, such as encryption technology, digital signature, Identity authentication, Key management, firewall and so on.
- Digital signature is the core technology to realize the security of online transactions. It can ensure the confidentiality of information transmission, Integrity of data exchange.

Digital Signature Algorithm

DSA is another public key algorithm, which is a more advanced way of validation, it can not be used as encryption, only for digital signature .

The digital signature, can perform these functions:
(1) to confirm the information is sent by the signer; (2) to confirm the information from the signature to receive so far, has not been altered; the signer cannot deny that information is sent by myself.

Digital Signature Algorithm

- DSA uses a public key to verify the integrity of the data and the identity of the sender for the recipient.
- It can also be used by the third party to determine the security of the signature and the authenticity of the data.