Digital Signature Algorithms

DSA-Digital Signature Algorithm is a variant of Schnorr and ElGamal signature algorithms, and it is DSS (DigitalSignature Standard) by NIST in the United States

Digital Signature

Digital signature is a common physical signature similar to that written on paper, but it is implemented in the field of public key cryptography, and is used to identify digital information.

Digital signature is a digital string which can not be forged by others only. It is also an effective proof of the authenticity of information sent by the sender of the information.

A set of digital signatures usually defines two complementary operations, one for signature and the other for verification.

Digital Signature Algorithms

- ✓ DSA is based on RSA algorithm.
- ✓ The private key X and the public key y are called a pair of keys (x, y). The private key can only be held solely by the signer himself, and the public key can be published publicly. Key pairs can be used continuously over a period of time.
- ✓ It follows the principle of "to signature with the private key and to verify with the public key"

Function of DSA

The integrity of the digital signature file is easy to verify, and the digital signature has non repudiation

Guarantee the integrity of information transmission, the identity authentication of sender, and the repudiation of transactions

Digital signature is an encryption process, and digital signature verification is a decryption process.