DSA
(Digital Signature Algorithms)

WISE Zhu Jia

27720151153580

The digital signature algorithm (DSA) is a federal information processing standard for digital signatures. In august 1991 the national institute of standards and technology (NIST) proposed DSA for use in their digital signature standard (DSS) and adopted it as FIPS 186 in 1993.

——From Wikipedia

DSA consists of 2 parts:

① Generation of a pair of public key and private key;

② Generation and verification of digital signature.

Key generation has two phases:

- The first phase is a choice of algorithm parameters which may be shared between different users of the system,
- The second phase computes public and private keys for a single user.

Reference

- https://en.wikipedia.org/wiki/Digital_Signature_Algorithm
- http://www.herongyang.com/Cryptography/DSA-Introduction-What-Is-DSA-Digital-Signature-Algorithm.html