DIGITAL SIGNATURE ALGORITHMS(DSA)

A Federal Information Processing Standard for digital signatures. It is a variant of the ElGamal signature scheme

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.

Four revisions to the initial specification to DSA

1. FIPS 186-1 in 1996
2. FIPS 186-2 in 2000
3. FIPS 186-3 in 2009
4. FIPS 186-4 in 2013

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.