Digital Signature Algorithms

Yuan Sun

The Digital Signature Algorithm (DSA) is a Federal Information Processing Standard for digital signatures.for the key generation, it has two phases. The first phase is a choice of algorithm parameters which may be shared between different users of the system, while the second phase computes public and private keys for a single user.

For the Parameter generation, the steps are: Choose an approved cryptographic hash function *H*; Decide on a key length L and N which is the primary measure of the cryptographic strength of the key; Choose an N-bit prime q; Choose an L-bit prime p such that p − 1 is a multiple of q; Choose g, a number whose multiplicative order modulo p is q.

The algorithm parameters (p, q, g) may be shared between different users of the system.

Per-user keys: Given a set of parameters, the second phase computes private and public keys for a single user.

Apart from these, we also need signing and verifying process, then check the Correctness of the algorithm

THANKS