Digital Signature Algorithm (DSA)

Hanjun Hua
27720161153020

Introduction of DSA

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.

Key generation

Key generation included parameter generation and per-user keys.

Key generation 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.

Signing

- Let *H* be the hashing function and *m* the message:
- Generate a random per-message value *k* where $1<k<q$
- Calculate $r=(g^k \bmod p) \bmod q$
- In the unlikely case that $r=0$, start again with a different random *k*
- Calculate $s=k^{-1}(H(m)+xr) \bmod q$
- In the unlikely case that $s=0$, start again with a different random *k*
- The signature is *(r,s)*

Verifying

- Reject the signature if $0<r<q$ or $0<s<q$ is not satisfied
- Calculate $w=s^{-1} \bmod q$
- Calculate $u_1=H(m)\cdot w \bmod q$
- Calculate $u_2=r\cdot w \bmod q$
- Calculate $v=(g^{u1}y^{u2} \bmod p) \bmod q$
- The signature is invalid unless $v=r$

DSA is similar to the ElGamal signature scheme.

Sensitvity

With DSA, the entropy, secrecy, and uniqueness of the random signature value k are critical. It is so critical that violating any one of those three requirements can reveal the entire private key to an attacker. Using the same value twice (even while keeping k secret), using a predictable value, or leaking even a few bits of k in each of several signatures, is enough to reveal the private key x.