

## DSS and DSA

The Digital Signature Standard uses the Digital Signature Algorithm to sign hash functions. Compare with signing a hash function with RSA.

DSA is a variation of signature schemes of ElGamal and Schnorr.

Notation:

$p$  is a prime of  $L$  bits ( $2^{L-1} < p < 2^L$ ),  $512 \leq L \leq 1024$ ,  $64|L$ .

$q$  is a prime of 160 bits,  $q|p-1$ .

$h$  is an integer,  $1 < h < p-1$ ,  $h^{(p-1)/q} \pmod{p} > 1$ , that is,  $h^{(p-1)/q} \not\equiv 1 \pmod{p}$ .

$g = h^{(p-1)/q} \pmod{p}$ . ( $g$  has order  $q$  modulo  $p$ .)

$p, q, g$  are a global public key used by several people.

Each user of the DSS chooses a secret private key  $x$  in  $1 < x < q$  and publishes a public key  $y = g^x \pmod{p}$ .

This assumes that discrete logarithms are hard to compute.

Each time a user wants to sign a message  $M$ , he chooses a secret random number  $k$  in  $1 < k < q$  and computes SHA of  $M$ , called  $H(M)$  below.

Alice signs message  $M$  with the pair  $r, s$ , where

$$r = (g^k \bmod p) \bmod q, \text{ and}$$
$$s = [k^{-1}(H(M) + xr)] \bmod q.$$

If Bob receives the message  $M'$  with signature  $r', s'$  from Alice, he verifies her signature by computing:

$$w = (s')^{-1} \bmod q,$$
$$u_1 = [H(M')w] \bmod q,$$
$$u_2 = (r')w \bmod q,$$
$$v = [(g^{u_1}y^{u_2}) \bmod p] \bmod q,$$

and making the test " $v = r'?$ "

If this equality holds, then Bob accepts that  $M' = M$  is a message actually sent to him by Alice.

Note that  $y$  is Alice's public key.

Why does the DSA work? That is, assuming that the message and signature are received correctly (so  $M' = M$ ,  $r' = r$  and  $s' = s$ ), why should  $v = r$ ?

Note that  $r$  doesn't even depend on  $M$ .

**Lemma 1:** If  $a \equiv b \pmod{q}$ , then  $g^a \equiv g^b \pmod{p}$ .

*Proof:* Write  $a = b + qt$ , where  $t$  is an integer. Then

$$g^a = g^{b+qt} = g^b g^{qt} \equiv g^b \cdot 1 = g^b \pmod{p}$$

because

$$g^q \equiv (h^{(p-1)/q})^q = h^{p-1} \equiv 1 \pmod{p}$$

by Fermat's Little Theorem.

**Lemma 2:**  $y^{((rw) \bmod q)} \equiv g^{((xrw) \bmod q)} \pmod{p}$ .

*Proof:* By definition,  $y = g^x \bmod p$ , so

$$y^{((rw) \bmod q)} \equiv g^{x((rw) \bmod q)} \pmod{p}.$$

Lemma 2 follows from Lemma 1 and the fact that

$$x((rw) \bmod q) \equiv ((xrw) \bmod q) \pmod{q}.$$

**Lemma 3:**  $((H(M) + xr)w) \bmod q = k$ .

*Proof:* By definition,  $w = s^{-1} \bmod q$  and  $s = [k^{-1}(H(M) + xr)] \bmod q$ . Therefore,

$$1 \equiv ws \equiv wk^{-1}(H(M) + xr) \bmod q \quad (\bmod q).$$

Since  $q$  is prime and  $q \nmid k$ ,

$$k \equiv w(H(M) + xr) \quad (\bmod q).$$

The lemma follows because  $1 < k < q$ .

**Theorem:** If  $M$  is unchanged and really came from Alice, then  $v = r$ .

*Proof:* Using the definition of  $v$  and then those of  $u_1$  and  $u_2$ , we find

$$v = ((g^{u_1} y^{u_2}) \bmod p) \bmod q$$
$$v = (g^{(H(M)w) \bmod q} \cdot y^{(rw) \bmod q} \bmod p) \bmod q.$$

Lemma 2 allows us to replace  $y$  by  $g$ :

$$v = (g^{(H(M)w) \bmod q} \cdot g^{(xrw) \bmod q} \bmod p) \bmod q$$
$$v = (g^{(H(M)w) \bmod q + (xrw) \bmod q} \bmod p) \bmod q.$$

Lemma 1 lets us combine terms in the exponent:

$$v = (g^{(H(M)w + xrw) \bmod q} \bmod p) \bmod q$$
$$v = (g^{((H(M) + xr)w) \bmod q} \bmod p) \bmod q.$$

Now use Lemma 3 and the definition of  $r$ :

$$v = (g^k \bmod p) \bmod q = r.$$