Global Public Key Components

p prime number where $2^{L-1} < p < 2^L$
for $512 \le L \le 1024$ and L a multiple of 64
i.e., bit length of between 512 and 1024 bits in increments of 64 bits

q prime divisor of $(p - 1)$, where $2^{159} < q < 2^{160}$
i.e., bit length of 160 bits

g $= h^{(p-1)/q} \bmod p$
where h is any integer with $1 < h < (p - 1)$
such that $h^{(p-1)/q} \bmod p > 1$

User's Private Key

x random or pseudorandom integer with $0 < x < q$

User's Public Key

y $= g^x \bmod p$

User's Per-Message Secret Number

k = random or pseudorandom integer with $0 < k < q$

Signing

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

$$s = \left[k^{-1}\left(\mathrm{H}(M) + xr\right)\right] \bmod q$$

Signature = (r, s)

Verifying

$w = (s')^{-1} \bmod q$

$$u1 = \left[\mathrm{H}(M')w\right] \bmod q$$

$u2 = (r')w \bmod q$

$$v = \left[\left(g^{u1}y^{u2}\right) \bmod p\right] \bmod q$$

TEST: $v = r'$

M = message to be signed
H(M) = hash of M using SHA-1
M', r', s' = received versions of M, r, s

Figure 13.4 The Digital Signature Algorithm (DSS)