Digital Signature Standard

Public

prime p: 512 to 1024 bits
$2^{L-1} < p < 2^L$ with $512 \leq L \leq 1024$

prime q: $q \mid (p-1)$, q is 160 bits.

→ Step 1 create 160 bit prime q.
Step 2 multiply q by random large #, add 1, check if prime.

prim/generator: $g = h^{\frac{p-1}{q}} \bmod p$
where $1 < h < p-1$.

To SIGN

for all msg:
1) Pick random private value x, $0 < x < q$.
2) User's public key $y = g^x \bmod p$.

3) Each message has its own k, random $0 < k < q$.

Signature: $r = (g^k \bmod p) \bmod q$.
$s = [k^{-1}(H(m) + xr)] \bmod q$.

TO VERIFY

1) $w = (s')^{-1} \bmod q$.
2) $u_1 = [H(m')w] \bmod q$
3) $u_2 = r'w \bmod q$
4) $v = (g^{u_1} y^{u_2} \bmod p) \bmod q$

$v = r'$ is test

$$g^{u1} y^{u2} = g^{[H(m')w] \bmod q} (g^{x})^{u2}$$

$$= g^{[H(m')w] \bmod q} \, g^{x r' w \bmod q}$$

$$= g^{(H(m')w + x r' w) \bmod q}$$

$$= g^{w(H(m') + x r') \bmod q}$$

$$= g^{k(H(m)+xr)^{-1}(H(m')+xr') \bmod q}$$

$$= g^{k \bmod q}$$

$$= \left(g^{k \bmod q}\right) \bmod p \bmod q$$