Digital Signature Algorithm

Prerequisites:

$$(ab) \bmod p = (a \bmod p)(b \bmod p) \bmod p$$
$$g^{xy} \bmod p = (g^x \bmod p)^y \bmod p$$

Public Parameters:

$$\text{Generate large primes: } p, q$$
$$(q \mid p-1, |p| = 2048, |q| = 256)$$
$$\text{Choose random } h$$
$$h \in (2, \cdots, p-2)$$
$$\text{Calculate } g = h^{\frac{p-1}{q}} \bmod p$$
$$\because p, q \text{ are primes,}$$
$$\therefore h^{p-1} \bmod p = 1$$
$$g^q \bmod p = (h^{\frac{p-1}{q}} \bmod p)^q \bmod p = h^{p-1} \bmod p = 1$$
$$\text{let k be any integer,}$$
$$g^{x+kq} \bmod p = (g^x g^{kq}) \bmod p$$
$$= (g^x \bmod p \cdot g^{kq} \bmod p) \bmod p$$
$$g^{kq} \bmod p = (g^q \bmod p)^k \bmod p = 1$$
$$\therefore g^{x+kq} \bmod p = g^x \bmod p$$
$$\text{If k is negative, multiple q can be takne out from x,}$$
$$\therefore g^x \bmod p = g^{x \bmod q} \bmod p$$

Key Generation:

$$\text{Choose random x (private key)}$$
$$x \in (1, \cdots, q-1)$$
$$\text{Calculate y} = g^x \bmod p \text{ (public key)}$$

Signing:

$$\text{Choose random k}$$
$$k \in (1,\cdots,q-1)$$
$$\text{Calculate } r = (g^k \bmod p) \bmod q$$
$$\text{Calculate } s = (k^{-1}(H(m)+xr)) \bmod q$$
$$((k^{-1}k) \bmod q = 1)$$
$$S(r,s)$$

Verification:

$$\text{Check } 0 < r < q, 0 < s < q$$
$$\text{Calculate } w = s^{-1} \bmod q$$
$$\text{Calculate } u_1 = (H(m)w) \bmod q$$
$$\text{Calculate } u_2 = (rw) \bmod q$$
$$\text{Calculate v} = (g^{u_1} y^{u_2} \bmod p) \bmod q$$
$$\text{If v} = r,\ \text{signature validated,}$$
$$\text{otherwiese, rejected.}$$

Correctness:

$$g^{u_1} y^{u_2} \bmod p$$
$$= g^{(H(m)w) \bmod q} y^{(rw) \bmod q} \bmod p$$
$$= (g^{(H(m)w) \bmod q} \bmod p) \cdot (y^{(rw) \bmod q} \bmod p) \bmod p$$
$$\because g^x \bmod p = g^{x \bmod q} \bmod p$$
$$\therefore g^{u_1} y^{u_2} \bmod p = (g^{H(m)w} y^{rw}) \bmod p$$
$$= g^{H(m)w+rwx} \bmod p$$
$$= g^{w(H(m)+rx)} \bmod p$$
$$= g^{s^{-1}(H(m)+rx)} \bmod p$$
$$= g^{k(H(m)+rx)^{-1}(H(m)+rx)} \bmod p$$
$$= g^{k(mq+1)} \bmod p$$
$$= (g^{kmq} g^k) \bmod p$$
$$= (g^{qkm} \bmod p) \cdot (g^k \bmod p) \bmod p$$
$$= g^k \bmod p \bmod p$$
$$= g^k \bmod p$$

Utility:

For modular inverse with respect to p:

$aa^{-1} \bmod p = 1$

If $a = cd^{-1}, a^{-1} = c^{-1}d$

(c^{-1}, d^{-1} are modular inverses WRT p respectively)

Proof:

$aa^{-1} = cd^{-1}c^{-1}d = (cc^{-1})(dd^{-1})$

$\because cc^{-1} \bmod p = 1, dd^{-1} \bmod p = 1,$

$\therefore cc^{-1} = mp+1, dd^{-1} = np+1 (m, n \in Z^{+})$

$aa^{-1} = mpn^{2} + mp + np + 1,$

$aa^{-1} \bmod p = 1$

Correct