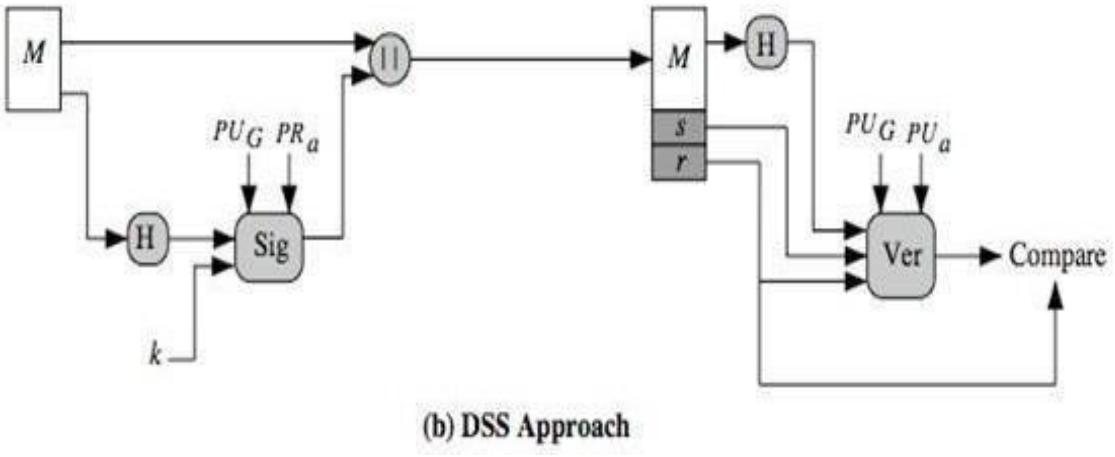
DSS APPROACH

DSS uses an algorithm that is designed to provide only digital signature function. Unlike RSA, it cannot be used for encryption or key exchange.

The DSS approach makes use of a hash function. The hash code is provided as input to a signature function along with a random number k generated for this particular signature. The signature function also depends on the sender's private key (PRa) and the global public key (PUG) The result is a signature consisting of two components, labeled *s* and *r*. At the receiving end, the hash code of the incoming message is generated. This plus the signature is



(b) DSS Approach

input to a verification function.

The verification function also depends on the global public key as well as the sender's public key (PUa), which is paired with the sender's private key. The output of the verification function is a value that is equal to the signature component if the signature is valid. The signature function is such that only the sender, with knowledge of the private key, could have produced the valid signature.

THE DIGITAL SIGNATURE ALGORITHM

1. Global Public key Components

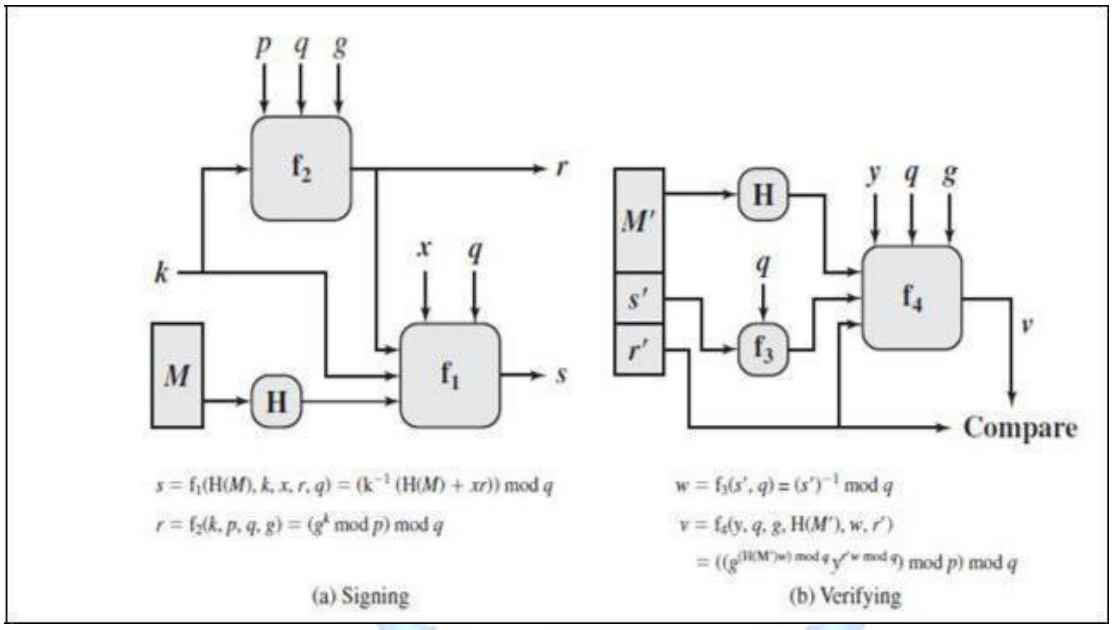
p- prime no. where $2^{L-1} < p < 2^{L}$ for

$512 \leq L \leq 1024$ q –prime divisor of (p-1

) where 2

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

where h is any integer with $1 < h < (p-1)$ such that $h^{(p-1)/q} \bmod p > 12\ 160$



2. User's Private key

x - random or pseudo random integer with $0 < x < q$

3. User's

Public key

$y = g^{x} \bmod p$

4. User's Per Message Secret Number

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

DSA Signature Creation

To sign a message M the sender: the sender generates a random signature key k, k<qComputes signature pair:

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

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

Signature = (r,s)

DSA Signature Verification

After received M & signature (r,s)

Verify a signature, recipient computes: $w = (s')^{-1} \bmod q$

u1= [H(M')w

]mod q u2=

(r'w)mod q

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

If v=r then signature is verified.