Semester : VI Subject : CSS Academic Year: 2023-2024

DIGITAL SIGNATURE STANDARD :-

→ Generation of public key and private key for user A.
→ Creation of Digital Signature by user A for an message M.
→ User B verifying the Digital Signature

Step 1: Key Generation:

User should generate:
Global public key components → (p,q,g) } It is published in public domain
Sender public key = y
Sender private key = x.

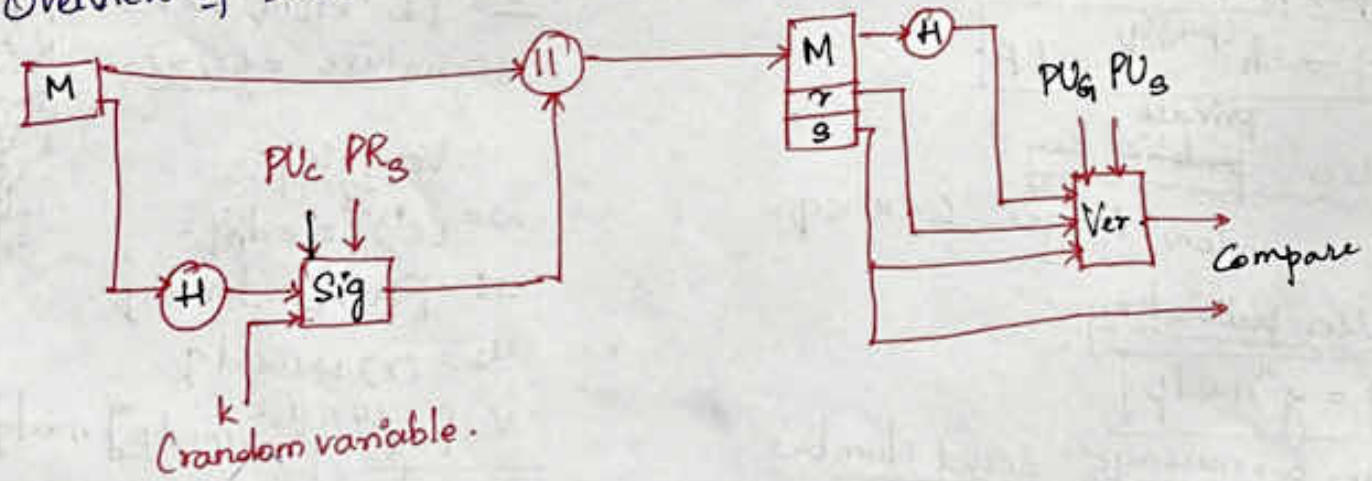
Step 2: Creation of Digital Signature

Signature is generated → (r,s).
Message M + (r,s) is send to Receiver.
Signature

Step 3: Verification of Signature

The Receiver validate the signature (r,s) using the global public key components → (p,q,g) and public key y.

Overview of DSS :-



Semester: VI Subject: CSS Academic Year: 2023 - 2024

Step 1: The sender generates hash value of the message to be send using hash algorithm.

Step 2: The sender generates the signature (r,s) using H[M], PU_c → public key components, P_s → Private key of sender and k → random variable.

Step 3: The sender sends message M and signature (r,s) to the receiver.

Step 4: The Receiver generates hash of the message.

Step 5: The receiver computes the value using PU_G → Public key Components and PU_s → public key of sender.

Step 6: If the computed value and r is same then the message is not modified.

Global public key components:

p → prime number

q → prime divisor.

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

User private public key:

X → random integer $0 < x < q$.

User public key.

$y = g^x \bmod p$.

User per message secret Number:

k = random integer $0 < k < q$.

Signing.

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

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

Signature = (r,s).

Verifying.

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

$u_1 = [H[M] w] \bmod q$.

$u_2 = (r) w \bmod q$.

$V = [(g^{u_1} \cdot y^{u_2}) \bmod p] \bmod q$

TEST: $V = r$.