Cryptography

Assignment 6

DSS / DSA:

Implementation of Digital signature Standard / Digital signature algorithm

NAME:

SNEHA MAGHNAHALLI RAJENDRANATH

ROLL NO:

CS21M522

Algorithm:

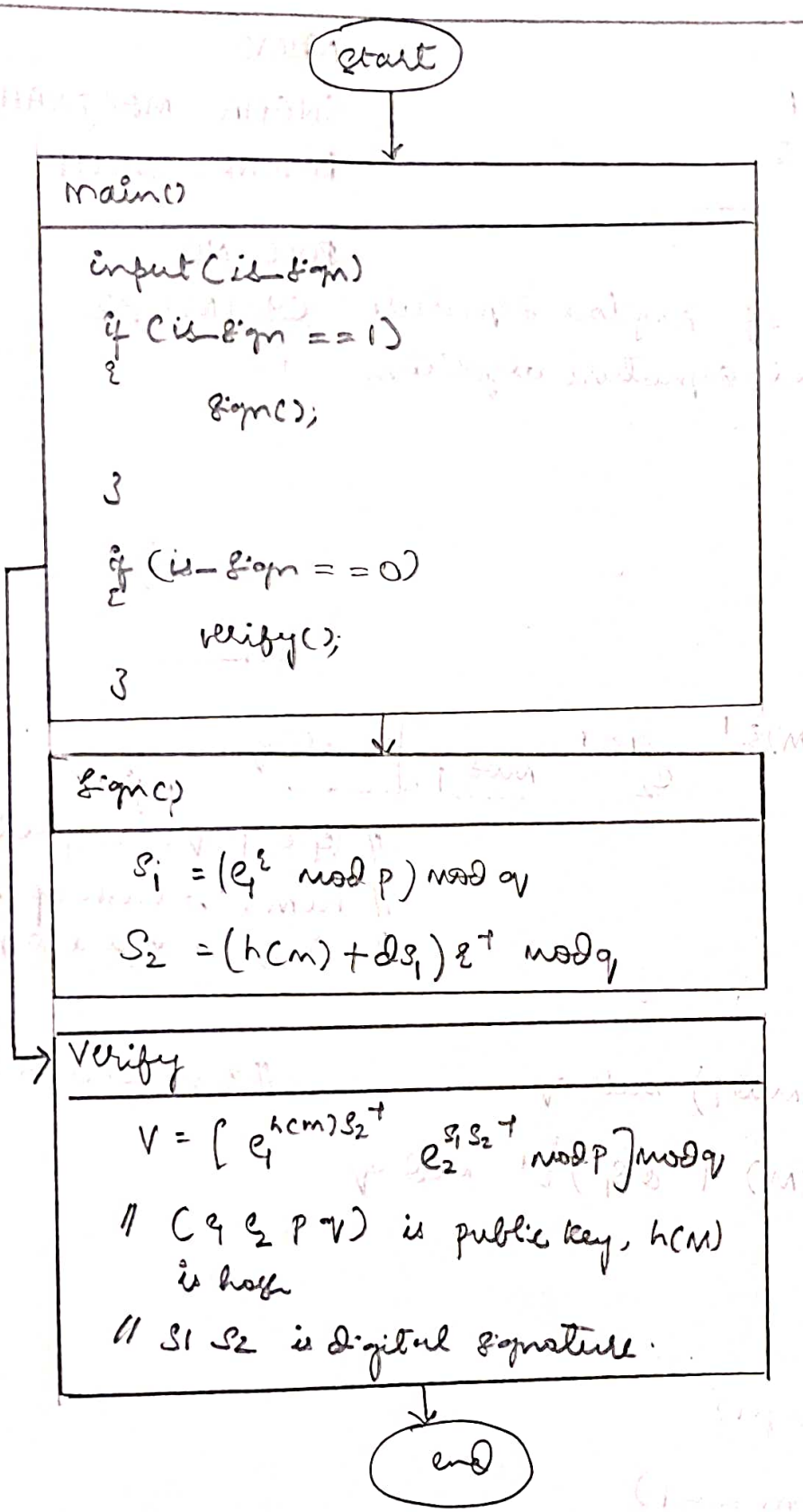
```
Void verify()
{
    V = [ e1^(h(M)S2^-1)  e2^(SIS2^-1)  mod p ] mod q
}

Void sign()
{
    S1 = (e1^z mod p) mod q
    S2 = (h(M) + xS1) z^-1 mod q
}

Main()
{
    input_issign)
    if (is_sign == 1)
    {
        sign();
    }
    if (is_sign == 0)
        verify();
    }
}
```

// (e1 e2 p q) is public key
// h(m) is hash of message
// S1, S2 is digital signature.

// z is random integer


start
main()
input(is_sign)
if (is_sign == 1)
{
sign();
}
if (is_sign == 0)
{
verify();
}
sign()
$S_1 = (g^k \bmod p) \bmod q$
$S_2 = (h(m) + dS_1) k^{-1} \bmod q$
Verify
$V = [g^{h(m)S_2^{-1}} \; e_2^{S_1 S_2^{-1}} \bmod p] \bmod q$
// (q g2 p v) is public key, h(M) is hash
// S1 S2 is digital signature.
end

Example :

Alice / Signer :

$p = 8001$

$q = 101$

$e_0 = 3$

$e_1 = e_0^{(p-1)/q} \mod p$

$= 3^{(8001-1)/101} \mod 8001$

$e_1 = 6968$

$d = 61$ // private key

$e_2 = e_1^{d} \mod p$

$= 6968^{61} \mod 8001$

$e_2 = 2038$

Let $h(M) = 5000$

$k = 61$

Send (M, S1, S2)

$S1 = (e_1^{k} \mod p) \mod q$

$= [6968^{61} \mod 8081] \mod 101$

$= 51$

$S2 = ((h(M) + dS_1) k^{-1}) \mod q$

$= (5000 + 61 \times 51) 61^{-1} \mod 101$

$= 40$.

Bob / verifier :

$V = [[e_1^{h(M) S_2^{-1}} \; e_2^{S1 S_2^{-1}}) \mod p] \mod q$

$= [(6968^{5000 \times 48} \times 2038^{51 \times 48}) \mod 8081] \mod 101$

$= 51$

$S1 = V$

∴ It is verified that Alice is the sender

—X—