Hash function H(x) : (x +3) mod 10

message = H(2) : 5 mod 10

= 5

Encryption :

private keys : 11, public key : 5, Modulus : 14

p,q : random primes

modulus n =pq = 14= 2,7

λ(n) means Carmichael’s totient for the value of n

λ(n) = lcm (p − 1, q − 1)

λ(14) = lcm(2 -1, 7-1)

λ(14) = lcm(1,6)

λ(14) = 6

since public key = 5 , Since the public key is freely shared, the value for e doesn’t have to be a secret.

let private key be d

d =1/e mod λ(n)

***m* (*c*) = *cd* mod *n***

When it comes to digital signatures:

The value of m (c) will be the signature.

The value of c is the hash of the message (10).

The value of d is part of the sender’s private key

*m* (*c*) = *cd* mod *n :*  5 power 11 mod 14

= 48828125mod 14

= 3

So the digital signature for the hash of the message is **3**

**Verifying digital signatures**

c(m) = mraise to power e mod n

c(m) = hash value

The value of e is part of the sender’s public key : 4

The value of m is the digital signature : 3

Value of n = 14

3 to power 5 mod 14

c(m) senders hash value = 243 mod 14

c(m) = 5

hash value = 5