Elgamal Digital Signature:

1. Select global elements q(prime number),α(primitive root of q)
2. Select private key Xa
3. Calculate public key Ya= α Xa mod q
4. Message is converted in hash code
5. Random integer K[gcd(q-1,k)=1]
6. S1= αk mod q
7. Inverse of k-1 mod {q-1}
8. S2=k-1(m- Xa. S1) mod {q-1}
9. S1=S2

Example:

1. q=19 , α=10

Xa=16

Ya=1016 mod 19

101 mod 19=10

102 mod 19=100 mod 19=5

104 mod 19=5.5 mod 19=25 mod 19=6

108 mod 19=36 mod 19=17

1016 mod 19=289 mod 19=4

Message m=14====h(m)

Random integer k=? gcd(q-1,k)=1

Gcd(18,?)=1

Gcd(18,5)=1

K=5

6.s1=105  mod 19

=3

7.k-1 mod {q-1}=5-1 mod 18

18=5\*3+3----[3=18-5\*3]

5=3\*1+2-----[2=5-3]

3=2\*1+1

1=3-2

1=3- (5-3)

1=(18-5\*3)-(5-(18-5\*3)

1=-5\*3 -5 -5\*3 [18 mod 18=0]

1=-7(5) mod 18

-x mod y=y-(x mod y)

18-(7 mod 18)

=18-7

=11 mod 18

k-1 =11

s2= 11(14-16.3) mod 18

=11.14- 11.16.3 mod 18

=154-528 mod 18

=-374 mod 18

-x mod 18 =18-(374 mod 18)

=18-14

=4

s1:s2=(3,4)

signature completed

verification process:

v1=αm mod q

= 1014 mod 19

= 108. 104.102 mod 19

=17.16.5 mod 19

=510 mod 19

=16

V2=Yas1 s1s2 mod q

=43.34 mod 19

=5184 mod 19

=16

V1=V2