Elgamal Digital Signature Scheme

1. Select a Prime number (q)
2. Select a Primitive root (α) of q
3. Generate a random integer (X_A)

   $1 < X_A < q-1$
4. Compute $Y_A = (\alpha)^{X_A} \bmod q$
5. Generate Keys for user (A)

   Private Key = X_A

   Public Key = $\{q, \alpha, Y_A\}$
6. Generate hashcode(m) for the plain Text (M)

   $m = H(M) \quad 0 \le m \le q-1$
7. Generate a random Integer (K)

   $1 \le k \le q-1$ and $\gcd(k, q-1) = 1$
8. Now Calculate S_1 and S_2

   $S_1 = \alpha^k \bmod q$

   $S_2 = k^{-1}(m - X_A S_1) \bmod q-1$
9. Now we get the Signature Pair. (S_1, S_2)

B's Side

Calculate V_1 and V_2

$V_1 = \alpha^m \bmod q$

$V_2 = (Y_A)^{S_1} (S_1)^{S_2} \bmod q$

If $V_1 = V_2$

Signature is Valid.

$V_1 \neq V_2$

Signature is not valid

Example

let $q = 19$

Primitive root

$(\alpha^1 \bmod q \;\; \alpha^2 \bmod q \;\ldots\; \alpha^{q-1} \bmod q)$ should have values $\{1, 2, 3 \ldots q-1\}$

$\boxed{\alpha = 10}$

Random Integer X_A $(1 < X_A < q-1)$

$1 < X_A < 18$

$\boxed{X_A = 16}$

$Y_A = \alpha^{X_A} \bmod q$

$= (10)^{16} \bmod 19$

$\boxed{Y_A = 4}$

A – Keys: Private key $\Rightarrow X_A = 16$

Public key $= \{q, \alpha, Y_A\} = (19, 10, 4)$

Generate hash code (m)

$m = H(M) \quad 0 \le m \le q-1$

$0 \le m \le 18$

$\boxed{m = 14}$

Therefore $k = 11$ $0 \le k \le q-1$ and $\gcd(k, q-1) = 1$

$0 \le k \le 15$ and $\gcd(k, 14) = 1$

$k = 11$

Calculate $S_1 = \alpha^k \bmod q$

$= (6)^{11} \bmod 17$

$S_1 = 3$

$S_2 = k^{-1} (m - x_a S_1) \bmod q-1$

$= k^{-1} \bmod q-1$

$= 5^{-1} \bmod q-1$

$5x = 1 \pmod{16}$

$\frac{5x}{16} = 1$

$16 \overline{)\,55\,(3}$

$\underline{50}$

5

$\underline{5}$

0

$k^{-1} = 11$

$S_2 = 11\,(14 - 16 \times 3) \bmod 16$

$= 11\,(14 - 48) \bmod 16$

$= 11\,(-34) \bmod 16$

$= -374 \bmod 16$

$S_2 = 4$

$S_1, S_2 = 3, 4$

B's side

$$v_1 = \alpha^m \bmod q$$

$$= 10^{14} \bmod 19$$

$$\boxed{v_1 = 16}$$

$$v_2 = (y_A)^{s_1} (s_1)^{s_2} \bmod q$$

$$= 4^3 \times 3^4 \bmod 19$$

$$= 5184 \bmod 19$$

$$\boxed{v_2 = 16}$$

Now $v_1 = v_2$

Signature is valid.