ELGAMAL DIGITAL SIGNATURES

Elgamal signature scheme involves the use of private key for encryption and public key for decryption

The global elements of Elgamal digital signature are prime number q and a, which is the primitive root of q.

1. **Global Public key Components**

q - prime no.

a – primitive root of q

2. **User A signs a message M to B by computing**

- Generate a random integer XA, such that 1 < XA < q-1
- Compute **Y**A= a^{XA} mod q
- A's Private key is XA
- A's Public key is YA

To sign a message M, user A first computes the hash m=H(M), such that m is an integer in the range 0≤ m ≤ (q-1)

3. **User A generates the digital signature**

- Choose a random integer K, such that 1≤ K≤(q-1) and gcd(K,q-1) = 1. That is, K is relatively prime to q-1.
- Compute, S1 = a K mod q
- Compute K -1 mod q-1
- Compute, S2 = K-1(m-xAS1) mod (q-1)
- The signature consists of a pair (S1,S2)

2. **User B verifies the Signature**

$V1 = a^{m} \bmod q$

$V2= (YA)^{S1} (S1)^{S2} \bmod q$

The signature is valid if V1 = V2.

<u>Example I</u>

Global Element

q=19 and a=10

Alice computes the private and public key

- Alice computes her key:
  - Alice chooses Private key, X_A=16
  - Computes Public Key, $Y_A=10^{16} \bmod 19 = 4$
- Alice signs message with hash m=14
  - Alice chooses K=5 which is relatively prime to q-1=18
  - Compute $S_1 = 10^5 \bmod 19 = 3$
  - Compute $K^{-1} \bmod (q-1) = 5^{-1} \bmod 18 = 11$
  - Compute $S_2 = 11(14-16*3) \bmod 18 = -374 \bmod 18=4$ {-374 mod 18=18-374%18}
- B can verify the signature by computing
  - $V_1 = 10^{14} \bmod 19 = 16$
  - $V_2 = 4^3.3^4 = 5184 = 16 \bmod 19$
  - Since 16 = 16 signature is verified and valid.

Any other user can verify the signature as follows.

1. Compute $x' = a^y v^e \bmod p$.
2. Verify that $e = H(M \| x')$.

To see that the verification works, observe that $x' \equiv a^y ve \equiv a^y a^{-se} \equiv a^{y-se} \equiv a^r \equiv x \pmod p$

Hence, $H(M\| x`) = H(M\|x)$