El Gamal Digital Signature Scheme

Alice is sending a message M to Bob, and she wants Bob to know that it was definitely her, who wrote the message.

1. Calculate H(M) for the message let m = H(M) and m is a fixed size.

Alice has to create both her private and public keys → SAME exact items as regular El Gamal.

q = prime number

a = primitive root

XA = Alice's secret key, $1 < XA < q-1$ (1 or q-1 is allowed but not good)

YA = a^{XA} mod q, this is Alice's Public key

To sign, we want to use our private key because that proves it's us, but we don't want to divulge any information about its value.

Alice is going to sign her message so that Bob knows that it's really her and not a scam!

<u>For Alice to Sign (ordered pair (S1, S2))</u>

1. Calculate H(M) for the message let m = H(M) and m is a fixed size.
2. Choose a random value of K, gcd(K, q – 1) = 1.
3. S1 = a^K mod q (If a is primitive root (which it is), then S1 is also a primitive root)
4. Compute K^{-1} (mod q-1).
5. S2 = K^{-1}(m – XA*S1) (mod (q-1))

Alice is going to send this ordered to Bob, along with the message.

Bob receives M, (S1, S2).

If Bob gets the message, M, he can also calculate m = H(M).

To verify, here is what Bob does (he calculates two values V1, V2):

V1 = a^m mod q

V2 = $(YA)^{S1}*(S1)^{S2}$ mod q

Message is verified if and only if V1 = V2.

V2 = $YA^{S1} \times S1^{S2} \pmod q$

$= (a^{XA})^{S1} \times (a^{K})^{S2} \pmod q$

$= (a^{XA})^{S1} \times (a^{K})^{((K^{-1} \pmod{q-1})(m-XA*S1))} \pmod q$

$= (a^{XA})^{S1} \times (a)^{((q-1)c+1)(m-XA*S1))} \pmod q$, since K * K^{-1} is 1 mod (q-1), we can rewrite This product as a int times (q-1) plus 1.

$= (a^{XA})^{S1} \times (a^{(q-1)c}a^{1})^{(m-XA*S1)} \pmod q$, by Fermat's Theorem a^{q-1} is 1 mod q

$= (a^{XA})^{S1} \times (1^{c}a^{1})^{(m-XA*S1)} \pmod q$,

$= (a^{XA})^{S1} \times (a)^{(m-XA*S1)} \pmod q$,

$= (a)^{XA*S1+m-XA*S1} \pmod q$,

$= (a)^{m} \pmod q$ = V1