Digital Signature: proof ~~A~~ for recipient and a third party that A sent a particular message to B at a particular time.

El Gamal Signature Scheme

Public Keys: q - prime number
α - primitive root / generator

Pick X_A $(1 < X_A < q-1)$ - secret key
$Y_A = \alpha^{X_A}$ (Third public key)

To sign a message M do this:

(1) compute $m = H(M)$ → hash func $0 \le m \le q-1$.
(2) Choose a random K, $1 \le K \le q-1$ $\gcd(K, q-1) = 1$.
(3) Compute $S_1 = \alpha^K \bmod q$ (Different generator!)
(4) Compute $K^{-1} \bmod (q-1)$
(5) Compute $S_2 = K^{-1}(m - X_A S_1) \bmod (q-1)$
(6) Signature is (S_1, S_2).

Verify

User B to verify
1. Compute $V_1 = \alpha^m \bmod q$
$V_2 = (Y_A)^{S_1} S_1^{S_2} \bmod q$ } Valid iff $V_1 == V_2$?

$$V_2 = \left(V_{1A}\right)^{S_1} \alpha^{S_2} \mod q$$

$$= \left(\alpha^{X_A S_1}\right)\left(\alpha^{K S_2}\right) \mod q$$

$$= \alpha^{X_A S_1 + K S_2} \mod q$$

Remember $V_1 = \alpha^m \mod q$

$V_1 == V_2$ if AND only if

$$X_A S_1 + K S_2 \equiv m \mod (q-1)$$

The idea is that modular exponentiation of α cycles every $q-1$ times hitting each value in $\{1, 2, \ldots, q-1\}$ exactly once. Both cycles must land on the exact same spot. Since the cycle length is $q-1$, that means that the 2 land at the same place iff the mod $q-1$ is the same.

$$X_A S_1 + K S_2 \equiv X_A \alpha^K + K\left(K^{-1}\left(m - X_A S_1\right)\right) \mod q-1$$

$$\equiv X_A \alpha^K + m - X_A \alpha^K \mod q-1$$

$$\equiv m \mod q-1.$$

PUBLIC $q = 19$

$\alpha = 2$

$X_A = 6$, $V_{1A} = 2^6 = 64 \equiv 7 \mod 19$

$m = 10$, $K = 5$

Compute $S_1 = \alpha^K = 2^5 \equiv 32 \mod 19 = \boxed{13}$

Compute $k^{-1} \bmod q-1 = 5^{-1} \bmod 18$ $\quad 5^{-1} \equiv 11 \bmod 18$

$k^{-1} \equiv 11 \bmod 18$

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

$= 11(10 - 6 \cdot 13) \bmod 18$

$= 11(10 - 78) \bmod 18$

$= 11(-68) \bmod 18$

$\equiv 11 \cdot 4 \bmod 18$

$\equiv \boxed{8 \bmod 18}$

Recipient gets $(S_1, S_2) = (13, 8)$.

= calculates $H(m) = 10$

$V_1 = \alpha^m = 2^{10} = 2^5 \times 2^5 = 32 \times 32 \equiv (-6) \times (-6) \bmod 19$

$\equiv 36 \bmod 19$

$\equiv \boxed{17}$

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

$= 7^{13}\, 13^{8} \bmod 19$

$= (7^2)^6 \cdot 7 \cdot (-6)^8$ → because $(-6)^2 \equiv 17 \bmod 19$

$\equiv 49^6 \cdot 7 \cdot 17^4$

$\equiv 11^6 \cdot 7\,(-2)^4$

$\equiv 11^6 \cdot 7\,(16) \bmod 19$

$\equiv (-8)^6 \cdot (-21) \bmod 19$

$\equiv 7^3 \cdot (-2) \bmod 19$

$\equiv 11 \cdot 7 \cdot (-2) \bmod 19$

$\equiv (-8) \cdot 7 \cdot (-2) \bmod 19$

$\equiv -21$

$\equiv \boxed{17 \bmod 19}$

64
-57
49