(0) Will give 4 bits for hint 7. (We announced) later today. (Tell me your group.)

(1) ElGamal Digital Signature

- Prove authenticity of the sender that the
- Slow WAY - 2 levels of RSA on the whole msg.

\[ E \left( E \left( M \right) \right) \xrightarrow{\text{Pr-Alice}} E \left( M \right) \xrightarrow{\text{Pr-Bob}} \text{2nd signature} \]

Usually to sign faster, we'll use a hash function output of a message because this is shorter.

Public Components: 
- \( q \) = prime (large)
- \( \alpha \) = generator / primitive root
- \( Y_A \) = Alice's public key

Private component: 
- \( 1 < X_A < q - 1 \)
- \( Y_A = \alpha^{X_A} \mod q \)

For Alice to sign her message \( M \), she'll do this:

0. \( m = H(M), \ 0 \leq m \leq q - 1 \)

1. \( 1 \leq K \leq q - 1, \ \gcd(K, q - 1) = 1 \)

2. \( S_1 = \alpha^K \mod q \) (same as \( C \) in ElGamal Encryption)

3. Compute \( K^{-1} \mod q - 1 \).

4. \( S_2 = K^{-1}(m - X_A S_1) \mod q - 1 \)
Bob receives both $m$ and $(S_1, S_2)$ from Alice.

1. $V_1 = \lambda^m \mod q$ (Bob can calculate $m$ via $H(m)$.)

2. $V_2 = (V^A)^{S_1}(S_i)^{S_2} \mod q$

Test if $V_1 = V_2$, the signature is valid. Otherwise it is not.

$V_2 = (V^A)^{S_1}(S_i)^{S_2} \mod q$

$= \lambda^{xAS_1} (S_i)^{k^{-1}(m-xAS_i)} \mod q$

$= \lambda^{xAS_1 + k \cdot k^{-1}(m-xAS_i) \mod q-1}

= \lambda^{xAS_1 + m - xAS_i} \mod q$

$= \lambda^m \mod q$