CIS 3362 11/27/23

0) Will give 4 bits for Hmk 7. (WC announcement) later today. (Tell me your group.)

1) El Gamal Digital Signature

- Prove authenticity of the sender's ~~that the~~

Slow WAY - 2 levels of RSA on the whole msg.

$$E_{Pr-Alice}(E_{Pu-Bob}(M)) \rightarrow \begin{array}{l} 1^{st} \text{ encryption} \\ 2^{nd} \text{ signature} \end{array}$$

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

Public Components: q = prime (large)

α = generator / primitive root

Y_A = Alice's public key

Private component: $1 < X_A < q-1$,

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

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

0. $m = H(M)$, $0 \le m \le q-1$
1. $1 \le K \le q-1$, $\gcd(K, \underline{q-1}) = 1$
2. $S_1 = \alpha^K \bmod q$ (same as C_1 in El Gamal Cryptosys)
3. Compute $K^{-1} \bmod q-1$.
4. $S_2 = K^{-1}(m - X_A S_1) \bmod q-1$

Bob receives both M and $\underline{(S_1, S_2)}$ from Alice.

(Bob can calculate m via $H(M)$.)

1. $V_1 = \alpha^m \mod q$

2. $V_2 = (Y_A)^{S_1}(S_1)^{S_2} \mod q$

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

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

$$= \alpha^{X_A S_1} S_1^{K^{-1}(m - X_A S_1) \mod q-1} \mod q$$

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

$$= \alpha^{X_A S_1 + \underline{K \cdot K^{-1}}(m - X_A S_1) \mod q-1} \mod q$$

$$= \alpha^{\underline{X_A S_1} + m - \underline{X_A S_1}} \mod q$$

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