CIS 3362 11/21/25

1) Papers - come to office after or office hrs

2) El Gamal Digital Signature Scheme - instead

Alice M to Bob
she wants to prove she wrote it.
Alice has to have her own El Gamal keys for (regular crypto scheme).

q = prime #
α = primitive root
X_A = Alice's secret #
$Y_A = \alpha^{X_A} \bmod q$ (Alice's public key)

To sign she wants to prove that used her private key w/o divulging any info about it.
Alice → M → Bob (encryption is independent/ Separate of signature)

HOW ALICE SIGNS M, (S1, S2)

1) Calculate $m = H(M)$ using some agreed upon hash function, m is fixed size output
2) Choose random, K, $\gcd(K, q-1) = 1$. (If this gcd = 1, then α^K is also a primitive root.)
3) $S1 = \alpha^K \bmod q$

4) Compute $K^{-1} \pmod{q-1}$, can only exist iff $\gcd(K, q-1) = 1$.

5) $S2 = K^{-1}(m - X_a \cdot S1) \pmod{(q-1)}$

Bob received m, $(S1, S2)$, wants to verify Alice's signature.

1) Bob calculates $m = H(m)$

2) To verify Bob calculates

$$V1 = \alpha^m \bmod q$$

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

Message is verified as a valid signature ONLY IF $V1 = V2$,

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

$$= (\alpha^{X_a \cdot S1}) \times \alpha^{K \cdot S2} \bmod q$$

$$= \alpha^{X_a S1 + K \cdot S2} \bmod q \quad \rightarrow \text{find this mod } q-1$$

$$\equiv \alpha^{m \bmod q-1} \bmod q$$

$$\equiv \alpha^m \bmod q \equiv V_1 \checkmark$$

V_1 was this

Via Fermat's Thm

$$\alpha^{B} \equiv \alpha^{B \bmod q-1} \bmod q$$

$$\alpha^{B_1} \equiv \alpha^{B_2} \bmod q \quad \text{if}$$

if $B_1 \equiv B_2 \bmod q-1$, then

$$\alpha^{B_1} \equiv \alpha^{B_2} \bmod q$$

$$X_a \cdot S_1 + k \cdot S_2 = X_a \cdot \alpha^{K} + \underbrace{k \cdot k^{-1}(m - X_a \cdot S_1)}_{\bmod q-1}$$

$$\equiv X_a \cdot \alpha^{k} + m - X_a \cdot \alpha^{k} \bmod q-1$$

$$\equiv \boxed{m \bmod q-1}$$

$$y^2 \equiv x^3 + ax + b \pmod{p}$$

Find (x, y) that works

$C \equiv x^3 + ax + b$

→ Compute this.

$$y^2 \equiv c \pmod{p}$$

Has 2 solutions iff

$$c^{\frac{p-1}{2}} \equiv 1 \bmod p$$

has 1 solution iff

$$c^{\frac{p-1}{2}} \equiv 0 \bmod p$$

else has 0 solutions

→ Ans $c^{\frac{p+1}{4}} \bmod p$

Reason

$$\left(c^{\frac{p+1}{4}}\right)^2 = c^{\frac{p+1}{2}} = c^{\frac{p-1}{2}+1}$$

$$\equiv c^{\frac{p-1}{2}} \times c \pmod{p}$$

$$\equiv 1 \times c \pmod{p}$$