CIS 3362 - 11/29/2021

Digital Signature (proof that someone wrote something)

Alice → Bob

$E(E(M))$ — Decrypt using Alice's Public key; Decrypt using his Private key

Pr-Alice Pu-Bob

SLOW!!!

Today: El Gamel Signature Scheme

Public keys: q (prime), α (primitive root)

1. $1 < X_A < q-1$, Private key

2. $Y_A = \alpha^{X_A} \bmod q$ (public key)

hash func.

To sign message M, first calculate $m = H(m)$.
$0 \le m \le q-1$.

1. Pick a value K, $1 \le K \le q-1$, $\gcd(K, q-1) = 1$.

2. $S_1 = \alpha^K \bmod q$

3. Calculate $K^{-1} \bmod q-1$.

4. $S_2 = K^{-1}(m - X_A S_1) \bmod q-1$

Sig: (S_1, S_2)

Receive M (after I decrypt it)
(S_1, S_2).

① Calculate $H(m) = m$.

② $V_1 = \alpha^m \bmod q$

③ $V_2 = (V_A)^{S_1} (S_1)^{S_2} \bmod q$

Iff $V_1 = V_2$ is the signature valid.

$$V_2 = (\alpha^{X_A})^{S_1} S_1^{S_2}$$

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

$$= \alpha^{X_A \cdot \alpha^k} \cdot \alpha^{\underline{k \cdot k^{-1}}(m - X_A S_1) \bmod q-1} \bmod q$$

$$= \alpha^{X_A \cdot S_1} \cdot \alpha^{(m - X_A S_1) \bmod q-1} \bmod q$$

$$= \boxed{\alpha^{X_A S_1 \bmod q-1}} \cdot \alpha^{m \pmod{q-1}} \cdot \boxed{\alpha^{-X_A S_1 \bmod q-1}}$$

$$= \boxed{\alpha^m \bmod q}$$