CIS 3362 : 11/21/22

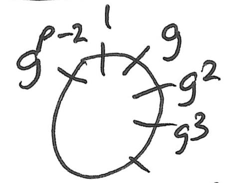
ECC

Day 1: Went over arithmetic

Day 2: Went over code

Day 3: How to apply to cryptography

Analog to Diffie Hellman Key Exchange



p prime

g gen

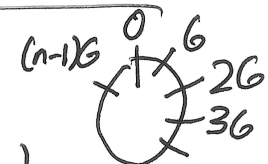
Given g^a, g and p

a is hard to find

Alice → g^a → Bob $(g^a)^b$

Bob → g^b → Alice $(g^b)^a$

Public elements



Curve $E_p(a,b)$

Point G on Curve

Order of G is large.

Let n be order of G.

Alice chooses $n_A < n$

Sends Bob $n_A \times G$.

Bob chooses $n_B < n$

Sends Alice $n_B \times G$.

Alice take $n_A \times (n_B \times G) = (n_A \times n_B) \times G$

Bob take $n_B \times (n_A \times G) = \underline{(n_A \times n_B) \times G}$

Shared Key

Public Key Crypto via Elliptic Curves
Similar to El Gamal

Alice pick a curve $E_p(a,b)$ — Public keys

She picks a secret value n_A — Private key

She ~~calculate point P =~~ chooses a point G with a high order n] — Public key

Post Public key $P_A = n_A \times G$ — Public

Bob send MSG ⇒ Alice

1. Bob's Plaintext is P_m (a pt on curve)
2. Picks secret $k < n$
3. $C1 = k \times \cancel{P_A}\, G$ $\cancel{((k \times n_A) \times G)}$
4. $C2 = P_m + k \times P_A$ $(P_m + (k \times n_A) \times G)$

When Alice receives this, she does

1. temp $= n_A \times C_1$ $(n_A \times k) \times G$
2. $P_m = C2 -$ temp

$$P_m + k \times P_A - n_A \times C_1$$

$$P_m + \underline{k \times n_A} \times G - \underline{n_A \times k} \times G$$

$$P_m$$