Elliptic Curve Cryptography

Monday, November 9, 2020 11:35 AM

1. Go over an Elliptic Curve Cryptography Scheme
2. Look at Sample ECC code.
3. Quickly Talk about the Quiz on Friday

Public Elements - Global

$E_q(a, b)$
G - a point with a large order on the curve, let n be the order of this point on the curve.

Private and Public key generation for a single user

Each user generates a private key
User A Private key: n_A, $n_A < n$
User A Public key: $P_A = n_A \times G$

Now, to send a message to user A:

1. Pick a random integer, $k < n$.
2. Calculate $k \times G$.
3. Let the message to encrypt be the point P_m.
4. Calculate $P_m + k \times P_A$
5. Send $(k \times G, P_m + k \times P_A)$

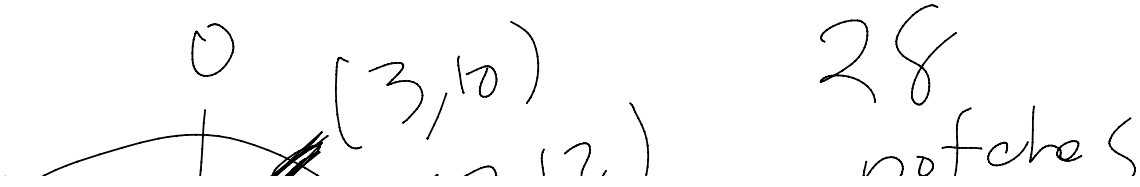
So Alice receives

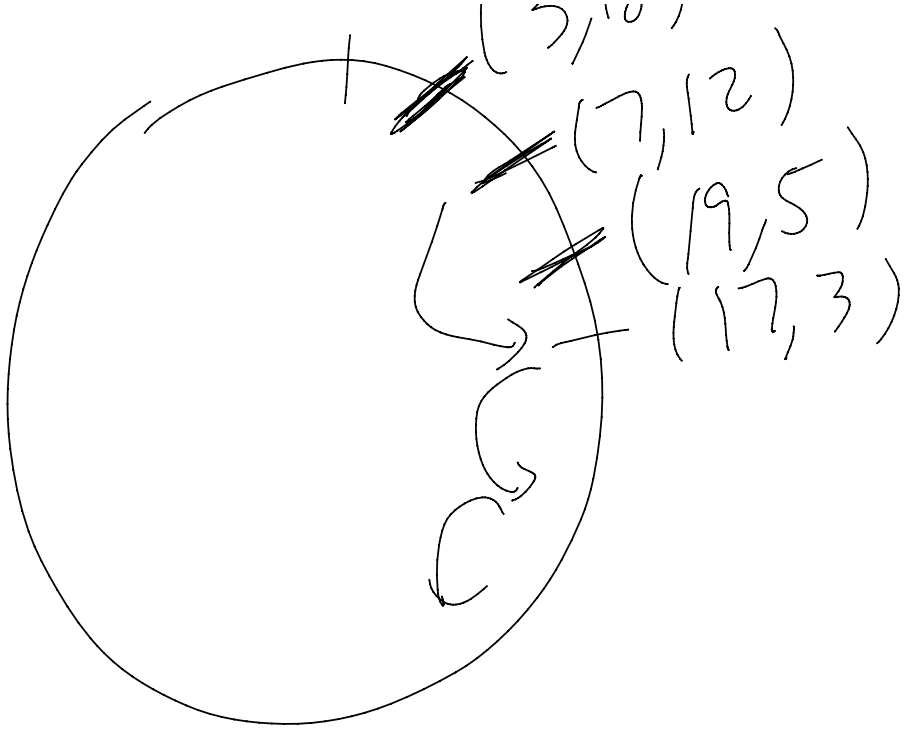
1) $k \times G$
2) $P_m + k \times P_A = P_m + k \times n_A \times G$
   $= P_m + n_A \times k \times G$
   $= P_m + n_A \times (k \times G)$

So, to decrypt, Alice takes the second ciphertext value, and subtracts from it, $n_A \times C_1 = n_A \times (k \times G)$

Note: Subtraction is addition of the negative.

A - B = A + (-B)





Cycle for a point kG is going to be order(G)/gcd(k, orderG).

Remember: No class on Wednesday.
Homework Due Soon.
Homework Solutions will be posted after homework is due, but homework won't be graded before the quiz.
I will have my office hours on Wednesday but TA s will not!

Format Same AS all the other quizzes.
25 minutes for each section, 10 minutes to turn in.
Typing preferred.

Topics

Diffie-Hellman (Part A)
RSA (Part A)
El Gamal (Part B)
ECC (Part B)