Math 400 Fall 2017
Cryptology HW 8
Due Thursday, October 26

1. Find every point :
   (a) $E : y^2 = x^3 + 3x + 2$ over $\mathbb{F}_7$.
   (b) $E : y^2 = x^3 + 2x + 7$ over $\mathbb{F}_{11}$.
2. Let $E : y^2 = x^3 + x + 1$ over $\mathbb{F}_{23}$ and let $P = (0, 22)$.
   (a) Compute $\log_P(18, 20)$. Show the results of each point addition you compute.
   (b) Compute $17P$. Show the results of each point addition you compute.
3. Suppose Alice and Bob want to communicate using a Elliptic Curve Diffie-Hellman scheme. They have chosen the curve $E : y^2 = x^3 + 23x + 13$, the field $\mathbb{F}_{83}$, and the point $P = (3, 21)$.
   (a) Bob chooses a secret number $n_B = 10$. What information should he send to Alice?
   (b) Bob receives the point $Q_A = (71, 82)$ from Alice. What is the shared secret key?
4. Now Alice and Bob communicate using an Elliptic Curve ElGamal scheme. They use the same curve and point as in the previous problem.
   (a) Alice chooses a private key $n_A = 17$. What is her public key?
   (b) Suppose Bob's public key is $Q_B = (68, 32)$. Alice wishes to send the message $M = (75, 8)$ using the ephemeral key $k = 5$. What ciphertext does Alice send?
   (c) Alice receives the ciphertext $(C_1, C_2) = ((30, 8), (71, 82))$ from Bob. What message does she decrypt?