Directions: Solve the following problems. All written work must be your own. See the course syllabus for detailed rules.

1. Alice and Bob wish to share a secret using Elliptic Curve-based Diffie–Hellman. They agree on the curve E given by $y^2 = x^3 + 14x + 2$ over $\mathbb{F}_{31}$ and the base element $g = (12, 10)$.
   (a) Bob picks $b = 10$ as his private exponent. What should Bob send to Alice?
   (b) Alice sends $A = (18, 17)$ to Bob. Compute Alice and Bob's shared secret.
   (c) **[Challenge (optional)]** Find Alice's private exponent a. In other words, find a such that $g^a = A$. This is an instance of the Elliptic Curve Discrete Logarithm Problem (ECDLP).

2. *Programming with elliptic curves.* In the following, we write code to multiply points and compute powers of points in the elliptic curve group E over $\mathbb{F}_p$, where p is prime and E is given by $y^2 = x^3 + Ax + B$. We assume that $B \neq 0$ so that we may represent the identity element in E as the special pair $(0, 0)$.
   (a) Write code for a function `ec_mult`$(p, A, B, x_1, y_1, x_2, y_2)$ that multiplies the points (x_1, y_1) and (x_2, y_2) in the elliptic curve group E over $\mathbb{F}_p$, where E is given by $y^2 = x^3 + Ax + B$. Be sure to handle the cases where the inputs or output are the identity point. For example, `ec_mult`$(p, A, B, x_1, y_1, 0, 0)$ should return (x_1, y_1) (modulo p) and `ec_mult`$(p, A, B, x, y, x, -y)$ should return $(0, 0)$. Submit your code.
   (b) Implement the fast power algorithm in a routine `ec_fast_power`(p, A, B, x, y, n) that computes $(x, y)^n$ where within the elliptic curve group E over $\mathbb{F}_p$. Submit your code.

3. Alice and Bob use Elliptic Curve ElGamal to send an encrypted message. They use the curve E over $\mathbb{F}_p$, where $p = 942857$ and E is given by $y^2 = x^3 + 152654x + 95765$. They agree to use base point $g = (395876, 217218)$, which happens to have prime order $q = 470749$ in E.
   (a) Check your code from problem #2 by verifying the following:
      i. $g^{500} = (485216, 167677)$
      ii. $g^q = (0, 0)$, our representation for the identity element in E, and
      iii. $g^{q+1} = g$.
   (b) Alice selects $a = 199481$ as her secret exponent. What should Alice send to Bob?
   (c) Bob wants to send the message $m = (358621, 245390)$ to Alice. He picks random element $k = 304364$. What is the corresponding ciphertext (c_1, c_2) that he should send to Alice?
   (d) Later, Alice receives a second encrypted message (c_1, c_2) from Bob, where $c_1 = (21125, 331345)$ and $c_2 = (448432, 307568)$. Decrypt the message.