## Elliptic Curve Diffie Hellman Key Exchange

Let  $E: y^2 = x^3 + ax + b$  be an elliptic curve. If Alice and Bob wish to exchange a key they can follow the following steps.

They agree on a prime p and an elliptic curve, and a point P on this curve. Let's say they choose p = 23,  $E: y^2 = x^3 + 5x + 1$  and P = (4, 4).

(1) Check that P is a point on their curve.

- (2) To exchange a key using ECDHA with your partner, pick a secret number a :\_\_\_\_\_\_(For this exercise, pick a number between 9 and 15, make sure you don't pick the same number as your partner.)
  Write a in binary: \_\_\_\_\_\_.
- (3) You wish to compute *aP*. We compute this using repeated doubling. Work out the values in the table: (Recall from your notes or book the rules for adding points on a curve. You can use sage to do the arithmetic modulo 23.)

Р	
$2\mathbf{P}$	
4P	
8P	

(4) Now add together the relevant entries to produce your aP.

(5) Exchange this number with your partner and write down the number they send you Q: \_\_\_\_\_\_. Now compute aQ, again using repeated doubling. Work out the values in the table:

Q	
2Q	
4Q	
8Q	

(6) Finally add together the relevant entries to produce aQ. Do you and your partner get the same point? This point (or one of its coordinates, say the x-coordinate) is your secret key.

## Elliptic Curve El Gamal

Let  $E: y^2 = x^3 + ax + b$  be an elliptic curve. Alice wishes to create a public key so that others can send her messages securely using an Elliptic curve version of the El Gamal system.

To do this she does the following. She picks a large prime p. (Let's say she picks p = 8675309) and an elliptic curve (Let's say she picks  $E : y^2 = x^3 + 2x + 1$ .)

- (1) Define this curve in sage using E = EllipticCurve(GF(8675309),[2,1])
- (2) Use sage to pick a random point α on this curve using
  alpha = E.random\_point() and a secret integer a using
  a = ZZ.random\_element(1000000). a is the private key, which should not be shared. Write it here a : \_\_\_\_\_\_
- (3) Compute  $\beta = a \times \alpha$ . Alice's public key is  $(E, p, \alpha, \beta)$ . Write it here:
- (4) Exchange public keys with your partner. Write their key  $(E, p, \alpha', \beta')$  here: (Note, they will have the same curve and prime, but different  $\alpha$  and  $\beta$ .
- (5) Now, send a message to your partner. Use m = E.random\_point() to pick a point on the curve which will be your message and write it here: m:\_\_\_\_\_

(Note: There are various ways to encode a message as a point on a curve, we won't talk about them here.)

- (6) Use sage to pick a random integer k. k = ZZ.random\_element(1000000) Write it here k : \_\_\_\_\_\_
- (7) Compute:  $y_1 = k \times \alpha' =$ \_\_\_\_\_\_  $y_2 = m + k \times \beta' =$ \_\_\_\_\_\_
- (8) Exchange these numbers with your partner, write their values here:  $y'_1 =$ \_\_\_\_\_\_ $y'_2 =$ \_\_\_\_\_\_
- (9) Decrypt their message by computing  $m' = y'_2 - a \times y'_1$ : \_\_\_\_\_\_
- (10) Check: Did you successfully decrypt their message? (Is your m' equal to their m?)