Math 314 - Spring 2018	Name:
Worksheet 3 May 15th, 2018	Partner:

Elliptic Curve Diffie Hellman Key Exchange

If Alice and Bob wish to exchange a key using ECDHE they do the following:

- They choose a prime p and an elliptic curve $E: y^2 = x^3 + ax + b \pmod{p}$. They pick a point P on the curve. (The analogue of the primitive root in the regular Diffie-Hellman exchange).
 - Let's say they choose p = 23, $E : y^2 = x^3 + 5x + 1$ and P = (5, 6).
 - (1) Check that P is a point on their curve.

- (2) To exchange a key using ECDHA with your partner, pick a secret number r :______ (Pick a number between 9 and 15, don't pick the same number as your partner.) Write r in binary: ______.
- (3) You wish to compute rP (P added to itself r times.) We compute this using repeated doubling. Work out the values in the table. Recall to add $P_1 = (x_1, y_1)$ to $P_2 = (x_2, y_2)$, and get $P_3 = (x_3, y_3) = P_1 + P_2$ we compute

$$m = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1} \pmod{p} & P_1 \neq P_2 \\ (3x_1^2 + a)(2y_1)^{-1} \pmod{p} & P_1 = P_2 \end{cases}$$

$$x_3 = m^2 - x_1 - x_2 \pmod{p}$$

$y_3 = m$	$(x_1 - x_1)$	$(x_3) - (x_3)$	y_1 ((mod	p)	1
-----------	---------------	-----------------	---------	------	----	---

P	(5,6)
2P = P + P	
4P = 2P + 2P	
8P = 4P + 4P	

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

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

<u>in th</u>	e table:
Q	
2Q	
4Q	
8Q	

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