Name:
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 $E: y^{2}=x^{3}+a x+b(\bmod p)$. 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 $p=23, E: y^{2}=x^{3}+5 x+1$ 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: $\qquad$
(3) You wish to compute $r P$ ( $P$ added to itself $r$ times.) We compute this using repeated doubling. Work out the values in the table. Recall to add $P_{1}=\left(x_{1}, y_{1}\right)$ to $P_{2}=\left(x_{2}, y_{2}\right)$, and get $P_{3}=\left(x_{3}, y_{3}\right)=P_{1}+P_{2}$ we compute

$$
m=\left\{\begin{array}{lll}
\left(y_{2}-y_{1}\right)\left(x_{2}-x_{1}\right)^{-1} \quad(\bmod p) & P_{1} \neq P_{2} \\
\left(3 x_{1}^{2}+a\right)\left(2 y_{1}\right)^{-1} & (\bmod p) & P_{1}=P_{2}
\end{array}\right.
$$

| $x_{3}=m^{2}-x_{1}-x_{2}$ | $(\bmod p)$ |
| :---: | :---: |
| $P$ | $(5,6)$ |
| $2 P=P+P$ |  |
| $4 P=2 P+2 P$ |  |
| $8 P=4 P+4 P$ |  |

(4) Now add together the relevant entries to produce your $r P$.
(5) Exchange this number with your partner and write down the number they send you $Q$ :

| in the table: |  |
| :---: | :---: |
| Q |  |
| 2Q |  |
| 4Q |  |
| 8Q |  |

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

