

Exercise 2: (1) Compute all points on  $y^2 = x^3 + 8$   
with  $(x, y) \in \mathbb{F}_5^2$ .

just check every possibility.

(actually, plug-in  $x$  then solve for  $y$ ).

(2) Use ECC to establish a shared secret w/ partner.

Use  $E: y^2 = x^3 + 8$  over  $\mathbb{F}_5$ , pick a point  $P$

Alice picks  $a \in \mathbb{Z}_p$ , sends  $aP$  } To compute multiple, - we

Bob picks  $b$  integer, sends  $bP$  | the formulas  
from Ex. 1.

Shared secret:  $a(bP) = b(aP)$

