# Cryptomen key gen example

1. Use Calculator at <https://andrea.corbellini.name/ecc/interactive/modk-mul.html>
2. Use curve A = 5, B = 3  y2 = x3 + 5x + 3
3. Use Field p = 211
4. Use Base point P: x = 17, y = 123

Alice  
Select n \_\_\_\_\_93\_\_\_\_\_\_ Alice’s private key  
Compute Q \_17, 123\_\_\_\_\_\_\_ Q = nP Alice’s public key  
Alice gives public key to Bob, keeps private key secret

Bob  
Select n \_\_107\_\_\_\_\_\_\_\_ Bob’s private key  
Compute Q \_\_17, 88\_\_\_\_\_\_ Q = nP Bob’s public key  
Bob gives public key to Alice, keeps private key secret

Alice’s shared key \_\_\_17, 88\_\_\_\_\_\_\_\_\_

N = 93, P = 17, 88

Bob’s shared key \_\_17, 88\_\_\_\_\_\_\_\_\_\_

N = 107, P = 17, 123