Assignment 3

Consider the elliptic curve E: $y^2 = x^3 - 2x + 2 \pmod{23}$ and P = (4, 9).

a. Calculate the value of 2P and 3P. (Show inverse calculation part).

b. Suppose this E and P = (4, 9) are used in an ECC Diffie-Hellman key exchange, where Alice chooses the secret value a = 3 and Bob chooses the secret value b = 6. What is the shared key among Alice and Bob?

** You need to find online tools to collect the values of 2P, 3P....etc. (In exam it will be provided)
https://graui.de/code/elliptic2/