Problem 1:

Users A and B use the Diffie-Hellman exchange technique with a common prime q = 71 and a primitive root α = 7.

a. If user A has a private key X_A = 5, then what is it’s public key Y_A?
b. If user B has a private key X_B = 12, then what is it’s public key Y_B?
c. What is the shared secret key?

Problem 2:

Consider a Diffie-Hellman scheme with a common prime q = 11 and a primitive root α = 2.

a. Show that 2 is a primitive root of 11.
b. If user A has a public key Y_A = 9, then what is it’s private key X_A?
c. If user B has a public key Y_B = 3, then what is the secret key K shared with A?

Problem 3:

Is 2 a primitive root of 7? Is 3 a primitive root of 7? Show your work.

Problem 4:

Write code to prove that 7 is a primitive root of 71.