Diffie-Hellman Exercises

Basic DH Computations. Consider a Diffie-Hellman scheme with system parameters $q = 11$ and $\alpha = 2$.

1. If Alice has public key $Y_A = 4$, what is her private key X_A?
2. If Bob has public key $Y_B = 6$, what is his private key X_B?

"Real" DH Computations. Recall that in a real Diffie-Hellman protocol, there are *three* system parameters: a prime q, a prime p that is much bigger than q, and an element α of order q mod p. For an actual implementation of the DH protocol, q would be at least 160 bits and p would be at least 1024 bits. Consider a small example of a DH protocol with the following system parameters:

$q = 866279$
$p = 764058079$
$\alpha = 19482865$

Complete a key exchange between Alice and Bob using these parameters. That is, generate random secret keys X_A and X_B, calculate the public keys Y_A and Y_B, and perform Alice and Bob's computations to derive the shared secret K. This is easily done in Python.