SHOW ALL WORK AND STEPS AND CITE SOURCES

1. Suppose the prime p=251 and base g=53 are published. Alice and Bob want to use the Diffie-Hellman key exchange protocol to establish a key. Alice selects the random number a=63 as her secret and Bob selects the random number b=55 as his secret. What is the key they agree on?
2. Suppose that the published Diffie-Hellman prime is p=37 with base g=6. If Alice sends Bob the number Ya=36 and Bob sends Alice Yb=31, find the key on which they have agreed. What makes the recovery of this key so easy? [Hint: Look at a table of values of 6x mod 37.] From Bob and Alice’s viewpoint, what would be a better choice of s?
3. Suppose the prime p=571 and base g=5 are published. Alice and Bob are engaging in a Diffie-Hellman public key exchange protocol. Eve the eavesdropper captures their public communication. Alice sent Bob Ya = 223 and Bob sent Alice Yb = 503. Use the divide and conquer method from class to break one of their discrete log problems and find the key. Show all steps.