CIS 475 - Introduction to Cryptography Quiz 5

Name:

1. Alice and Bob are communicating using the ElGamal cryptosystem with prime p = 23 and generator g = 7.

   A. Bob creates his public key by choosing the exponent b = 5. What is Bob's public key?

   B. Alice wants to send the message, say x to Bob. Demonstrate how Alice encrypts the message. Let Alice secret exponent a = 4

   C. Bob receives the encrypted message $(H_A, C) = (9, 6)$ from Alice. What is his plaintext message?