**Exercise 6**

**Student ID: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Student Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

1. In RSA, a ciphertext sent from Alice to Bob is C=2. Bob’s public key is e=7, n=55. Determine the private key d and decrypt the ciphertext C=2.

2. Alice and Bob exchange a secret key using the Diffie-Hellman key agreement. They agree to use the modulus q = 353 and g = 3 as the generator. Assume Alice uses the secret value a = 97 and Bob the secret value b = 233. Compute the intermediate values and the final key that Alice and Bob exchange and explain the man-in-the-middle attack to the protocol.