CIS 3362 Quiz #5 Review Questions

1) In an RSA system, n = 391 and e = 137, what is d?

Team #: _____ Answer: _____

2) In a Diffie-Hellman Key Exchange, Alice and Bob agree upon the public keys p = 17 and g= 3. Alice picks the secret key a = 4 and Bob picks the secret key b = 7. What value does Alice send Bob? What value does Bob send Alice? What is their shared secret key?

Team #: _____ Answer: _____

3) Consider the Elliptic Curve$_{29}$(3, 11). Let p be the point (8, 5) on this curve and q be the point (20, 26) on this curve. Determine P + Q.

Team #: _____ Answer: _____

4) Consider the Elliptic Curve$_{29}$(3, 11). Let P be the point (8, 5) on this curve. Determine 2P.

Team #: _____ Answer: _____

5) Alice's Public El Gamal keys are q = 31, and $\alpha = 11$. Alice's secret key $X_A = 9$. Bob has sent a message to Alice. The ciphertext he has sent to Alice is $C_1 = 3$, $C_2 = 18$. What is the plaintext?

Team #: _____ Answer: _____