**QUIZ 4**

**CHAPTER 8 and Chapter 10**

**30 Minute Quiz**

1. **Write the answers on a blank sheet of paper.**
2. **Make sure you write your name on every page.**
3. **Mark each page with Quiz 4.**
4. **Write legibly.**
5. **Must show steps for any credit.**
6. Consider the cyclic group denoted by Z19\*.
   1. State the size of the elements in the group.
   2. How many generators does it have?
   3. What are the possible element orders of the elements in Z19\*?
   4. What is the order of the element 4? Is 4 a generator? Why or why not?
7. Verify the RSA based digital signature that has been received as follows. Use square and multiply algorithm for exponentiation.

Given n = 143, public Exponent, e = 11, message x = 2, signature s = 46

1. a) Describe the process of creating DIFFE-HELLMAN Key Exchange. What parameters are chosen and state the conditions of each parameter chosen.

b) Compute the two public keys A and B and the Common Key, KAB in a Diffe-Hellman key exchange, given the parameters: p= 467, α = 2, a = 3 and b = 7

