CS2910 Paper Quiz 5 Name:

1. (2 points) Flow control and congestion control both reduce the rate at which information is sent. ***Describe*** the difference in the physical constraints that each control algorithm tries to meet.

2. (2 points) The sender in a TCP connection sends a message with a sequence number of 150, and 25 bytes of data. If all of the data is received, ***write*** what the acknowledgement number from the receiver will be.

3. (3 points) Suppose Bob encrypts a message M with his public key K_B^+, yielding the ciphertext $C = K_B^+(M)$.
   a. ***Circle one***. This message is secure/insecure. (An insecure message is accessible in plaintext to Trudy)
   b. ***Circle one***. This message is accessible/inaccessible to Alice.
   c. ***Circle one***. Assuming that Alice knows that the public key K_B^+ really is Bob's, Alice can/cannot confirm that the message comes from Bob.

4. (2 points) ***Describe*** the problem with a plain cipher-block encryption algorithm that cipher-block chaining overcomes.

5. (1 point) ***Select*** the equation that the public exponent d must satisfy in RSA, assuming the primes p and q are used, and prime exponent e is provided.
   a. $(pq)^d \bmod (p-1)(q-1) = e$
   b. $((p-1)(q-1))^d \bmod pq = e$
   c. $(de) \bmod (p-1)(q-1) = 1$
   d. $(de) \bmod pq = 1$