CSS 322 – QUIZ 3

First name: ______________________________ Last name: ___________________________

ID: _____________________________ Total Marks: ____________
out of 10

- Write your name and ID in the space provided at the top of the sheet.
- Answer the questions on this sheet(s) only, using the space given.

Question 1 [3 marks]

Explain (in 2-3 sentences) why Cipher Block Chaining mode of operation for block ciphers is better than Electronic Code Book when long messages must be encrypted.

Question 2 [2 marks]

Give an advantage and disadvantage of using link-level encryption (as opposed to end-to-end encryption) in the Internet.

Advantage:

Disadvantage:

Question 3 [3 marks]

Assume you are using a centralised Key Distribution Centre (KDC) in your symmetric key cryptosystem.

a) List the keys that are used if A wants to communicate with B. Give each key a meaningful name or short description.

b) For each key from part (a), list which of the three hosts (A, B, KDC) have access to the key.

Question 4 [2 marks]

Assume you are using the linear congruential generator (see equation below) to generate random numbers.

$$X_{n+1} = (aX_n + c) \bmod m$$

a) If the input is X_0=1, c=0 and m=9, and the first three output numbers are X_1 to X_3 = {7, 4, 1}, then what is X_4?

b) A desirable property of a random number sequence is a long period. What parameter can be modified to potentially produce a sequence of more than 10 different random numbers?