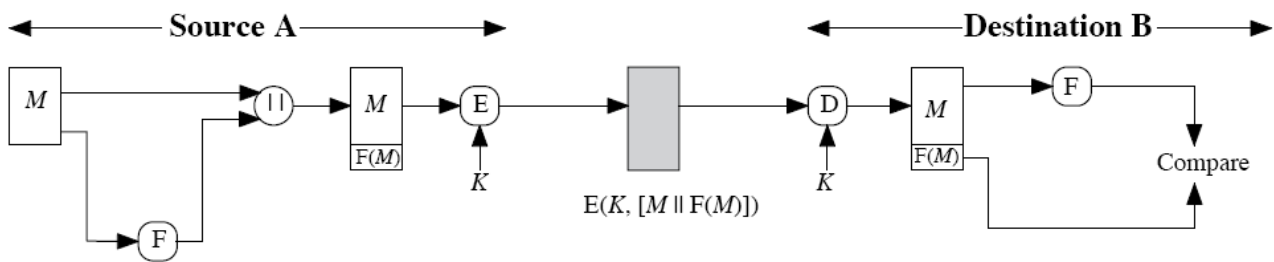# CSS322 – Quiz 5

Name: _____

ID: _____   Mark: _____ (out of 8)

Question 1 [5 marks]

Consider the scheme in the figure below.

a) Fill in the blank: This scheme uses _____ cryptography. [1 mark]

b) Of the 6 general security services, list the services that this scheme provides. For each service, explain why/how the scheme provides it. [3 marks]

c) If you assume the message M was binary data (such as portion of an image), explain the purpose of F(M). [1 mark]

Question 2 [3 marks]

a) Draw a diagram in the same format as above (in Question 1) that illustrates a MAC being used without the original message being encrypted.

b) Explain why you might want to use the approach from part (a) of this question, instead of the approach from Question 1.