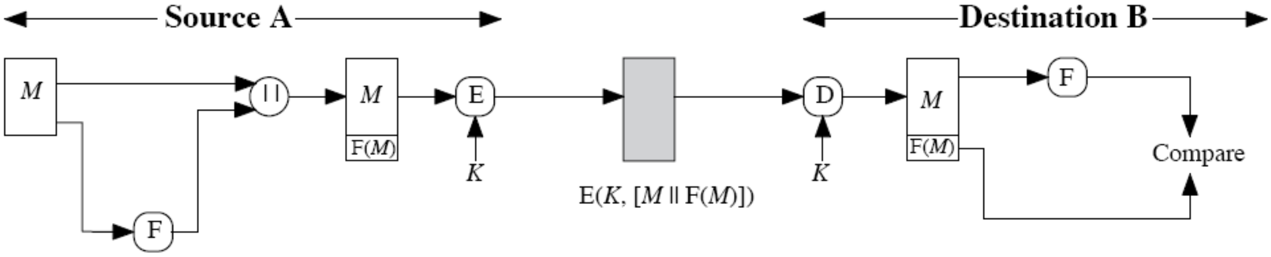
CSS322 – Quiz 5 Answers

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]

Answers

a. Symmetric Key Cryptography (because the keys used by both sides are the same, K).

b. The message is encrypted, hence it provides Confidentiality. Symmetric key encryption also provides Authentication because only A and B have the secret key K (hence B knows it came from A). If the message was modified then B would detect it because decrypting with K would produce unexpected results. Hence this also provides Data Integrity.

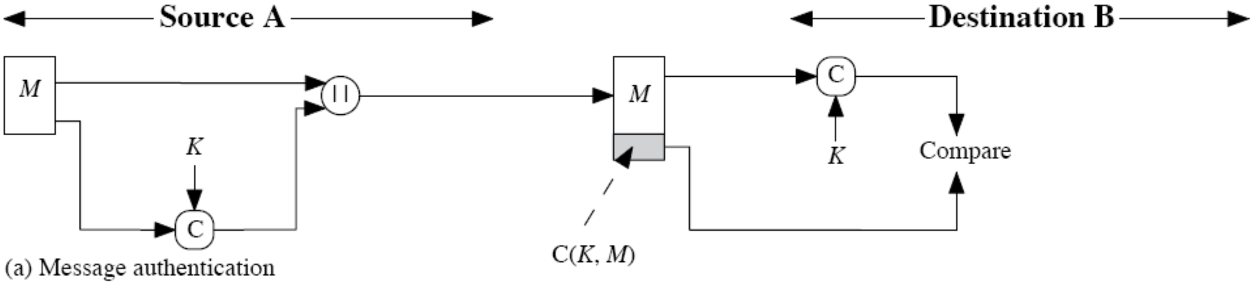
c. F(M) adds structure to the message so that B can recognise whether or not the ciphertext received is in fact from A: if apply F() on the decrypted plaintext M does not match the received F(M) then it indicates the ciphertext was encrypted with a key other than K.

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.

Answer



(a) Message authentication

b. The top approach provides Confidentiality as well as Authentication and Data Integrity. Some cases when you don't need/want Confidentiality include: cost (computational, financial) of encrypting entire message is too much; message does not need to be confidential.