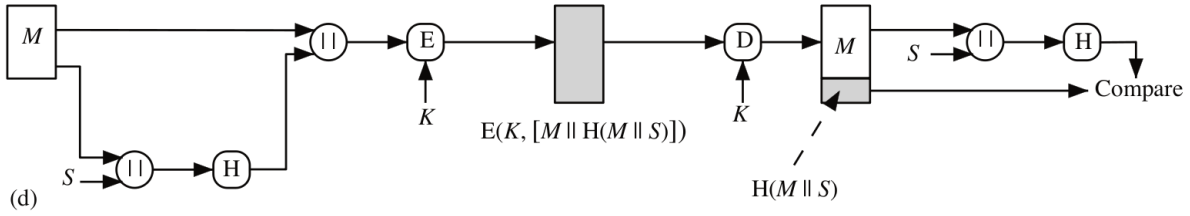
CSS322 – Quiz 5

Name: _____ ID: _____ Marks: ____ (10)

Question 1 [3 marks]

Consider the mechanism illustrated below and the six security services: confidentiality, authentication, non-repudiation, data integrity, access control and availability.

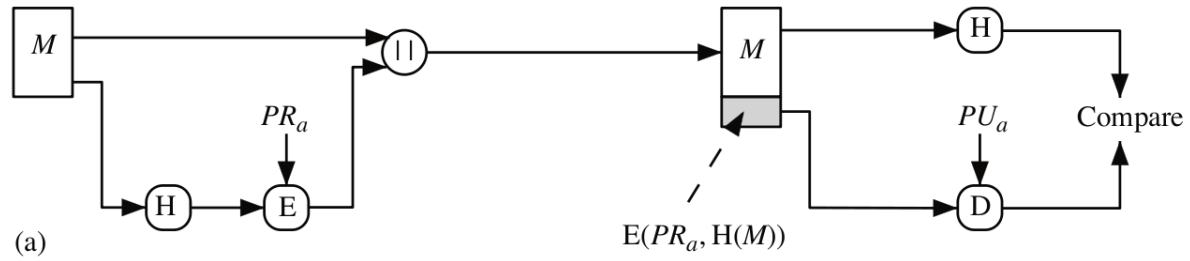


(a) What security service(s) does the mechanism provide? [1 mark]

(b) If encryption was not used (i.e. E() and D() operations not applied) in the above mechanism, then explain what an attacker needs to do to break the mechanism. [2 marks]

Question 2 [3 marks]

Consider the mechanism illustrated below.

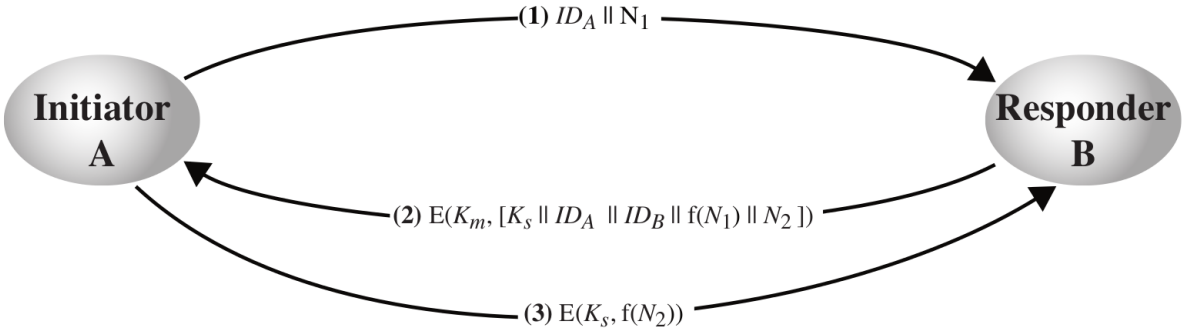


(a) The mechanism is a special case of authentication. What is its name? [1 mark]

(b) An example of E()/D() in the above mechanisms may be RSA. Explain why if 3DES was used as E()/D() instead, then the above mechanism would not provide the same service as when RSA was used. [2 marks]

Question 3 [4 marks]

Considered the key distribution scheme below.



(a) For this scheme to work, what keys are known by A and B before the 3 steps are taken? [1 mark]

(b) Assume an attacker sent message 1 pretending to by A (instead of A sending message 1). Explain how either A or B would detect this attack. [2 marks]

(c) Describe an disadvantage of the above scheme. [1 mark]