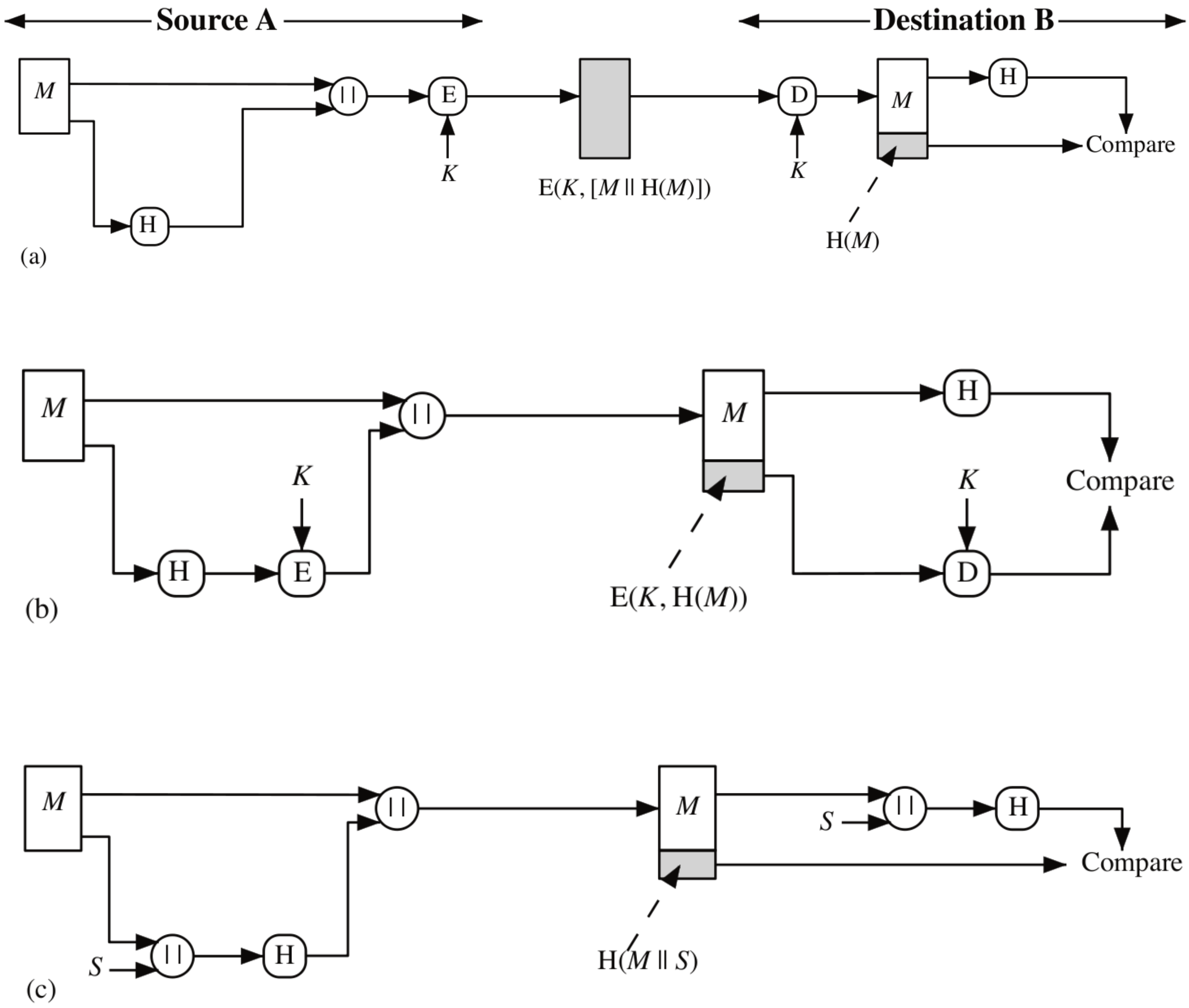
CSS322 – Quiz 5

Security and Cryptography, Semester 2, 2010

Prepared by Steven Gordon on 30 January 2011
CSS322Y10S2Q05, Steve/Courses/CSS322/Assessment/Quiz5.tex, r1651

Question 1 [3 marks]

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

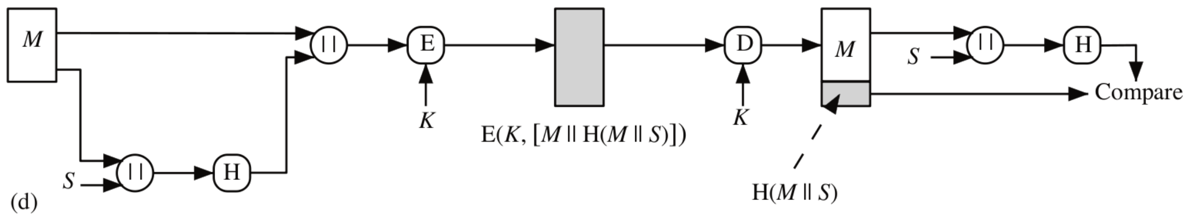


(a) What security service(s) does the mechanism provide? [1 mark]

Answer.

i. Confidentiality, Authentication, Data Integrity

ii. Authentication, Data Integrity



iii. Authentication, Data Integrity

iv. Confidentiality, Authentication, Data Integrity

(b) Assuming it is impossible for an attacker to discover K or break E() or D(), explain what an attacker needs to do break the above mechanism (that is, so one of the security services is compromised). [2 marks]

(c) 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]

Answer.

i. *Both M and $\mathrm{H}(M)$ are sent in the clear. The attacker modifies M and also recalculates the hash, and forwards to B. B cannot detect the modification.*

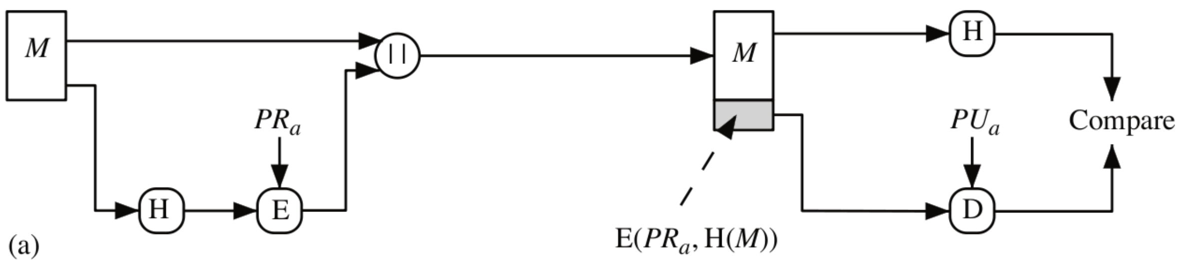
ii. *If attacker can find another message M' that has the same hash value as M, i.e. $\mathrm{H}(M') = \mathrm{H}(M)$, then attacker can create modified message without being identified.*

iii. *If attacker can discover the input of the hash function from the hash value, i.e. given h, where $h = \mathrm{H}(M||S)$, find $M||S$, then the attacker can find the secret S.*

iv. *Same as (iii).*

Question 2 [3 marks]

Consider the mechanism illustrated below.



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

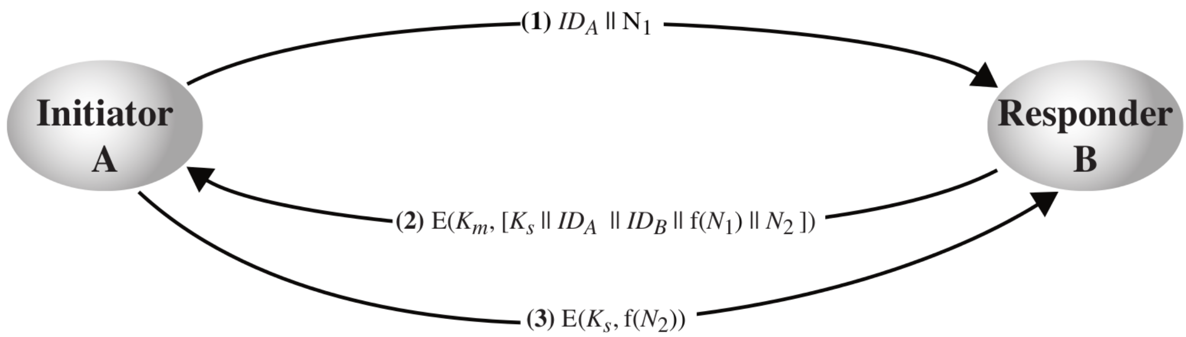
Answer. *Digital Signature*

(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]

Answer. *Using symmetric key encryption (e.g. 3DES) means both A and B have the shared secret key. The message could have been encrypted by either A or B, meaning the message could have originated at either A or B. Using public key encryption (e.g. RSA) means only A could have encrypted the message, confirming that the message originated at A.*

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]

Answer. *A and B both must know* K_m.

(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]

Answer. *B responds. If A receives the response unaltered, then it is decrypted with* K_m *and A will recognise that it did not send the initial request with nonce* N_1*, hence identifying the attack. If attacker interecpted message (2) before it arrived at A, then the attacker cannot decrypt (doesn't know* K_m*), and therefore does not know* N_2 *or* K_s*. If attacker tries to respond with message 3, B will detect the attack because it will contain the wrong value and encrypted with wrong key. If attacker does not send message 3 then B will detect an attack (because it expects to receive message 3).*

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

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

Answer. *An advantage is that it doesn't rely on a trusted third party (KDC). This is useful of you do not trust a central party or the third party is slow. A disadvantage is that for large number of users, many master keys must be manually distribted beforehand.*