CSS322 – Quiz 5 Answers

Name: ____

ID: ____________________________ Mark: _________ (out of 10)

Question 1 [4 marks]

Three properties of hash functions for practical implementations are: Hash function can be applied on any size input message; fixed length output message is produced; Hash function is easy to calculate.

Three properties of hash functions for security are: one way property; weak collision resistance; strong collision resistance.

a) Which Hash function property is the easiest for a malicious user to attack? [1 mark]

Answer

Strong collision resistance. It is easier for an attacker to find a pair of messages with the same hash value than finding a message with the same hash value as a given message (weak collision resistance). It is also easier than finding the message from a hash value (one way property).

b) Referring to the properties, explain why collisions will occur in practical Hash functions. [1 mark]

Answer

As the input can be any size, but the output must be fixed, that means the input can be longer than the output. Hence there are more possible inputs than outputs, and hence some inputs must map to the same output, i.e. collision.

c) Explain (or define) the *one way property* for Hash functions. [1 mark]

Answer

It is computationally hard to find the original message given its hash value.

d) Explain (or define) the property of weak collision resistance for Hash functions. [1 mark]

Answer

It is computationally hard to find a message which has the same hash value of another, given message.

e) Explain (or define) the property of strong collision resistance for Hash functions. [1 mark]

Answer

It is computationally hard to find any pair of messages that have the same hash value.

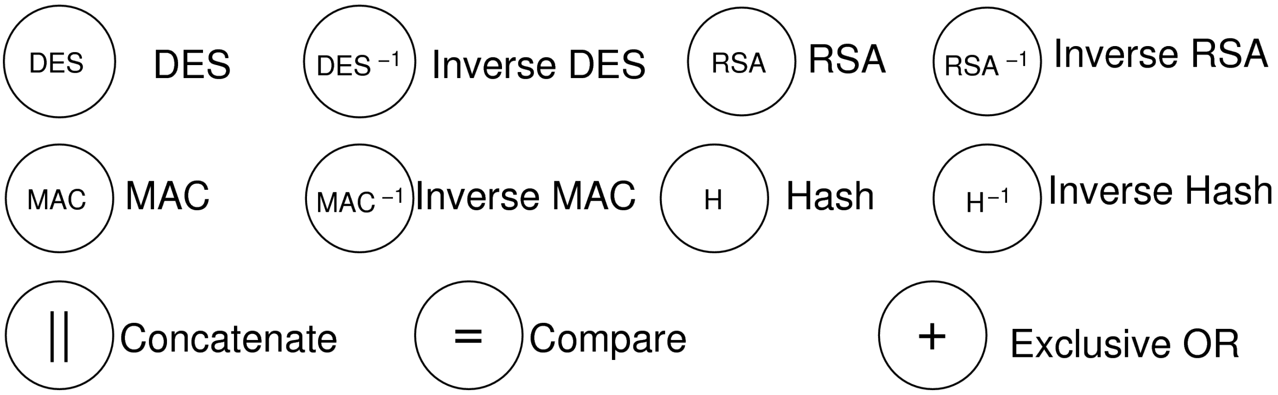
f) Explain a security benefit of using Hash functions with Public Key Cryptography to provide authentication and confidentiality (compared to using Hash functions with Symmetric Key Cryptography to provide authentication and confidentiality). [1 mark]

Answer

With Public Key Cryptography only one person could have encrypted the hash – that is the person with the private key. With Symmetric Key Cryptography two possible people could have encrypted the hash – the two users that share the secret key. Hence Public Key Cryptography provides a *digital signature* service, which guarantees to everyone who the message came from.

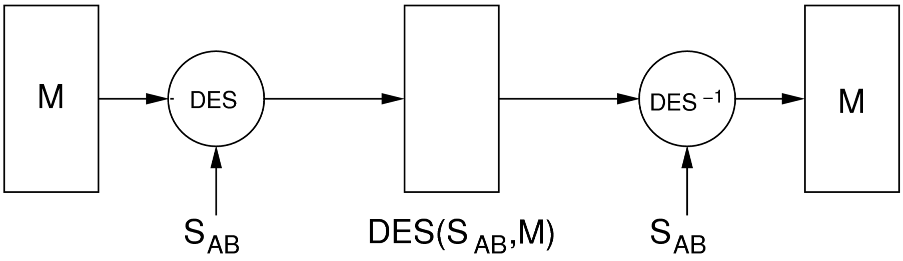
Question 2 [6 marks]

In the following questions you need to draw a diagram illustrating the mechanism used when sending information from A to B. In your answer you can use the following operations:

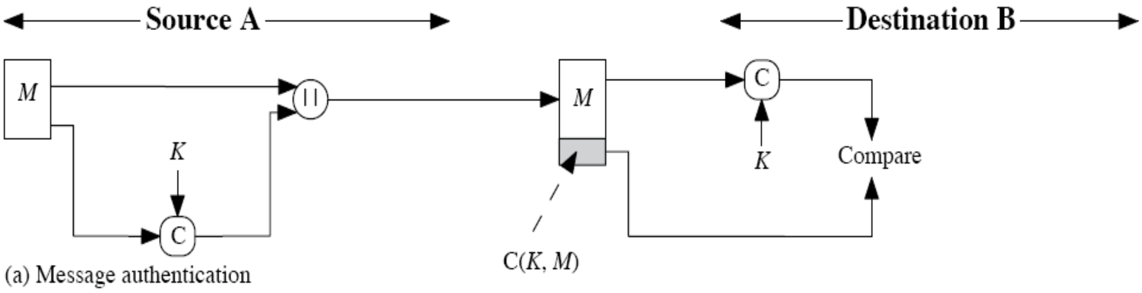


as well as the following keys: S_{AB}, PU_A, PR_A, PU_B, PR_B.

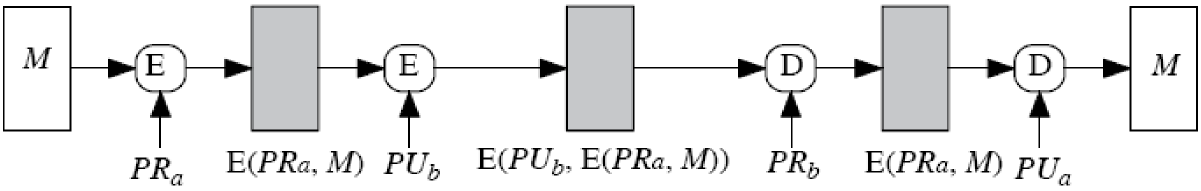
As an example, the following diagram illustrates DES symmetric key encryption for confidentiality.



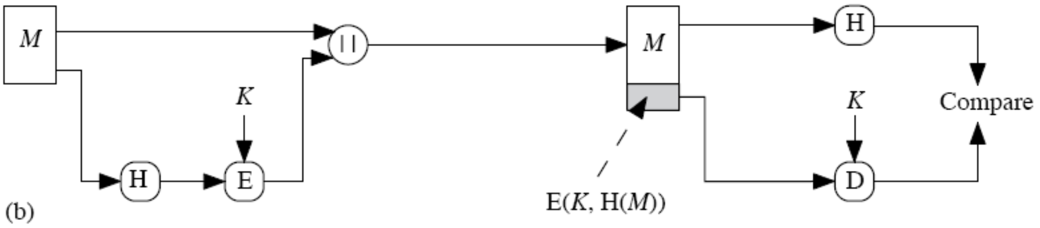
a) Authentication only (no confidentiality), using a Message Authentication Code [3 marks]



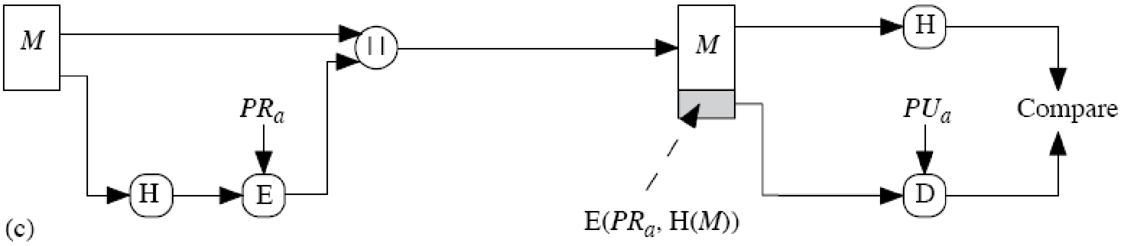
b) Confidentiality using RSA and authentication using RSA [3 marks]



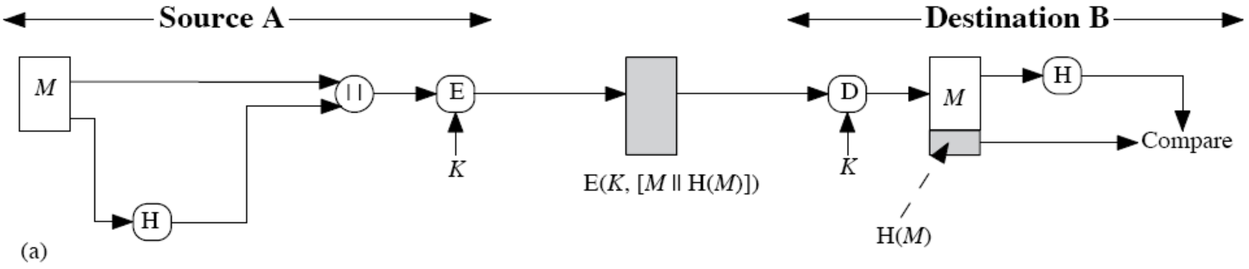
c) Authentication only (no confidentiality), using a Hash function and DES [3 marks]



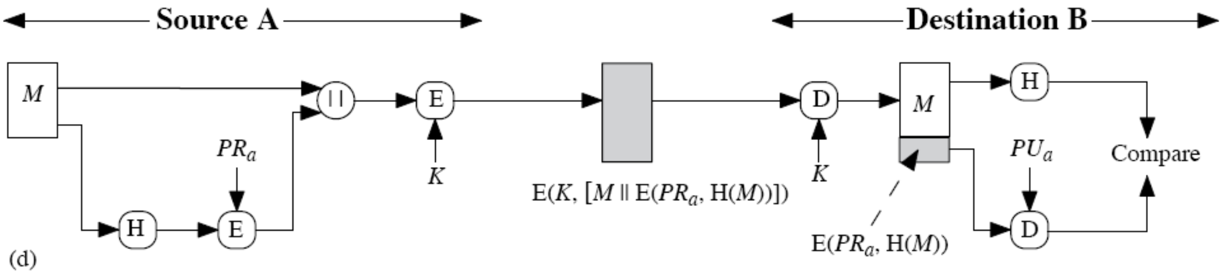
d) Authentication only (no confidentiality), using a Hash function and RSA [3 marks]



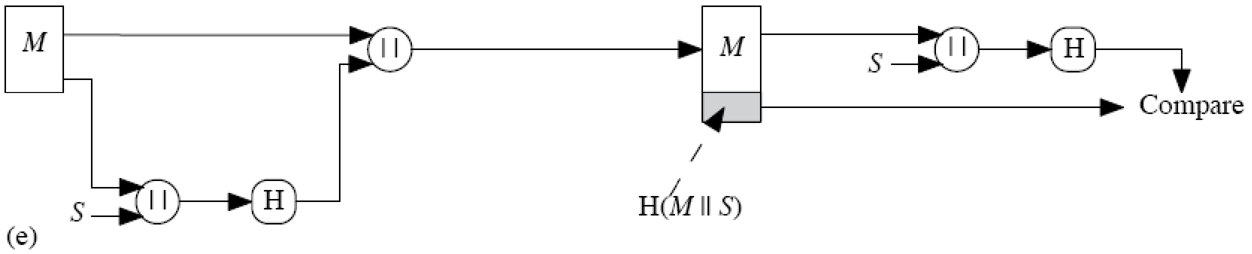
e) Confidentiality using DES and authentication using a Hash function [3 marks]



f) Confidentiality using DES and authentication using a Hash function and RSA [3 marks]



g) Authentication only (no confidentiality), using a Hash function and no encryption [3 marks]


M
||
S
||
H
M
S
||
H
Compare
H(M || S)
(e)