CSS 322 – QUIZ 7

First name: ______________________________ Last name: ___________________________

ID: _____________________________ Total Marks: ____________

out of 10

Question 1 [3 marks]

User A sends a message to user B, and a digital signature is attached, as shown below.

$$A \xrightarrow{M,\ E_{PRa}[H(M)]} B$$

Explain how a malicious user C can attack this system if the hash function H() is not weak collision resistant. Your explanation should say what C needs to do, and what C gains (or achieves) from the attack, and what happens at B for the attack to be successful.

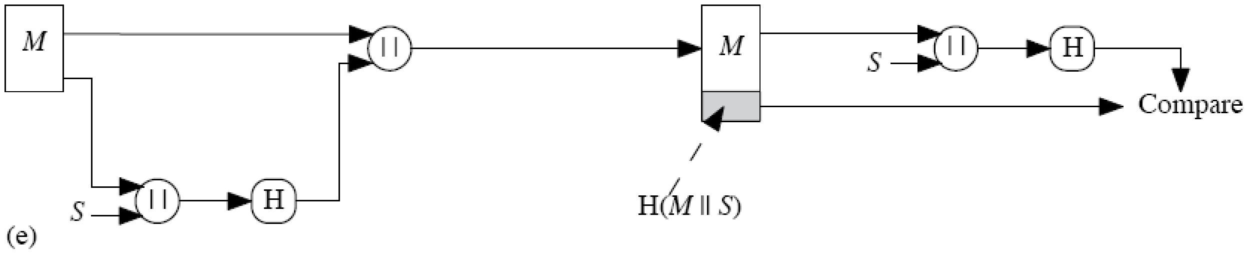
Question 2 [2 marks]

a) What is the difference between a Hash function and a Message Authentication Code (MAC) function? [1 mark]

b) What can be used to convert most hash functions to MAC functions? [1 mark]

Question 3 [3 marks]

The figure below shows a method of combining symmetric key encryption and hash functions.



a) List the security service(s) that the method provides. [1 mark]

b) Explain the attack that a malicious user can perform if the hash function, H(), does not have the one-way property. Your explanation should say what the malicious user can gain, at how the perform the attack. [2 marks]

Question 4 [2 marks]

a) How can you make a system more secure against online password guessing? [1 mark]

b) A Unix password file often contains a username and hash of the password for each user. The file is often readable by all users (that is, public). Explain how does adding a “salt” value improve security (including what type of attack it can prevent)? [1 mark]