CS5285 – Lecture 1 Tutorial Questions

1. Complete the five blank spaces in the following table.

Service		Algorithm	Threat
Confidentiality	Encryption	AES	
	MAC	HMAC	
Non-repudiation		RSA/DSA	

2.a) Availability is seen as a basic security service. Briefly explain what this service does and give an example of the type of behavior it prevents in e-commerce.

2.b) Availability was not seen as a security service in the late 1980s when network/communication security services were written into prominent standards – but it is today. What do you think changed?

3. You are hired to work for an online newspaper as IT security advisor. They have several problems: At the moment they use a username and password to allow paying subscribers to view the news content, but they have found that some of their customers have shared their passwords and unauthorized people are viewing content; some criminals, listening to network traffic has obtained customer payment data during the subscription process; and a rival newspaper has been modifying the content between their servers and the client causing some customers to leave. Explain to your new employer what authentication, confidentiality and integrity are and tell them which of these concepts apply to each of the problems they are having.

4.a) You are working for a software vendor. Customer purchase and then download the software from your company. Recently the company has been losing customers as they do not trust the downloaded software. They say it is possible that hackers could change the software after it is sent from your server and that they need proof that the software they received has not been modified. What security service do you need? What mechanism could you use?

4.b) Customers start to falsely claim that they have not received software and want their money back! What security service do you need? What mechanism could you use?

5.a) You are asked to implement a new security mechanism to provided confidentiality for online-chat messages. How could you use standards in building your solution?

5.b) What reason would you give your boss/client when asked why you are using existing standards and not developing your own solution from the beginning?