ITS 413 – QUIZ 4

First name: _____ Last name: _____

ID: _____ Total Marks: _____
out of 10

Question 1 [3 marks]

a) IPsec in tunnelling mode can be used to create a Virtual Private Network from your Home PC to a company network. Draw a diagram that shows the Home PC, Company Router and Company PC, and indicate on the diagram:

   a. Tunnel end-points

   b. The traffic that is encrypted

b) Explain the advantage of using IPsec in tunnelling mode for a VPN, as opposed to using IPsec end-to-end (transport mode).

Question 2 [4 marks]

a) In TOR the original source Proxy encrypts a packet (onion) with different keys before sending. If there are three TOR routers used between the source Proxy and destination Proxy, illustrate the order in which the original data is encrypted. Assume the routers are R1, R2 and R3, where R1 is the first router and so on.

b) List the TOR nodes from part (a), and identify the keys that each node owns (or knows).

c) Explain what type of anonymity TOR provides, and using the above example, how it provides the anonymity.

Question 3 [3 marks]

a) Apinat wants to send Swit a message. Write the name of the security service that is needed for each of the following cases:

   a. Swit wants to be certain that the message came from Apinat, and not from Surasit.

      Service: _____

   b. Apinat wants to be certain that Surasit cannot read the message.

      Service: _____

   c. Swit wants to be certain that Surasit has not changed the original message sent by Apinat.

      Service: _____

b) If Napatsorn performs the following actions, then indicate if it is a Passive or Active attack (circle the correct answer):

   a. Napatsorn captures the message, and at a later time, sends it again to Pharanyu.
      ACTIVE / PASSIVE

   b. Napatsorn captures the message, and makes observations about how Warakorn and Pharanyu are communicating. ACTIVE / PASSIVE

   c. Napatsorn pretends to be Warakorn, sending a message to Pharanyu.
      ACTIVE / PASSIVE