ITS 413 – QUIZ 4 ANSWERS

First name: ______________________________ Last name: ___________________________

ID: _____________________________ Total Marks: ____________
out of 10

Question 1 [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: AUTHENTICATION

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

Service: CONFIDENTIALITY

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

Service: INTEGRITY

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

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

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

Question 2 [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).

Home PC ------------------- Company Router ----------------Company PC

Tunnel end-points are Home PC and Company Router

Traffic is encrypted from Home PC to Company Router

Advantage of using tunelling mode is that any PC can use the secure connection without complex configuration of IPsec. Also allows network administrator to control what security options are used for VPN (as opposed to giving individual users control).

Question 3 [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.

Packet is encrypted with Proxy Destination key, then R3 key, then R2 key, then R1 key.

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

Proxy Source: Keys of Proxy Destination, R1, R2, R3

R1: Key of R1

R2: R2

R3: R3

Proxy Dest: Proxy Dest

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

Stops other people in network from knowing who is communicating; that is, no-one knows that A and B are communicating. This is because each router only knows about the immediate previous node and immediate next node, since information about other nodes in the path is encrypted with keys not available to the current router. Hence, in general, a router does not know the end destination or original source.