CSS322 – Quiz 7

Name: ____

ID: ______________________________ Mark: __________ (out of 10)

Question 1 [2 marks]

Multiple choice. Select the most accurate answer. Choose only one.

i. If Transport Layer Security is used to secure data (e.g. web pages) between a client and server, TLS uses:

a) Public key algorithms for data confidentiality and MD5 or SHA1 for data integrity

b) Message authentication codes for data integrity and symmetric key algorithms for data confidentiality

c) Symmetric key algorithms for key exchange and message authentication codes for authentication

d) Public key algorithms for key exchange and Diffie-Hellman for data integrity

ii. TLS:

a) Can provide confidentiality for any Internet application

b) Can provide data integrity for any Internet application

c) Is used by HTTPS to provide web security

d) Is used by IPsec to provide network security

Question 3 [6 marks]

An application on PC1 is sending data to an application on PC2. The route from PC1 to PC2 is via R1, R2, R3 and R4, in that order. You can identify the IP address of a node by its name, e.g. the IP address of R1 is "R1". Assume IPsec Encapsulating Security Payload (with Authentication) is used, and the application uses TCP.

Assume IPsec is used in transport mode between the PC's.

a) Draw the structure of a packet received by router R1 by completing the diagram below (that is, complete the packet headers between IP and App). [1 mark]

IP Header		App Header	App Data	ESP Trailer	ESP Auth

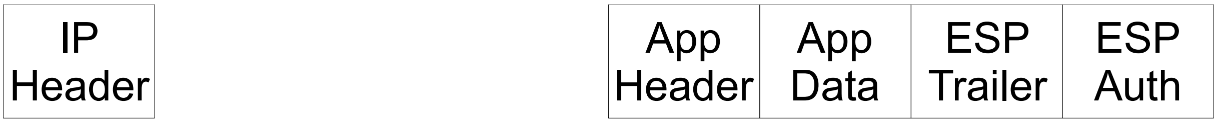
b) For the packet in part (a), what is the destination address in the outer IP header? [0.5 mark]

c) Which parts of the packet are encrypted? [1 mark]

d) If a field in the original IP header is modified by a malicious user, will PC2 detect that modification? Explain your answer. [1 mark]

Assume IPsec is used in tunnelling mode, from router R1 to PC2.

e) Draw the structure of a packet received by router R4 by completing the diagram below. [1 mark]



f) For the packet in part (e), what is the destination address in the outer IP header? [0.5 mark]

g) Which parts of the packet are encrypted? [1 mark]

Question 3 [2 marks]

Explain an advantage of using IPsec in tunnelling mode between two LAN routers to provide a Virtual Private Network (as opposed to using end-to-end encryption between hosts).