CSS 322 – QUIZ 5

First name: ______________________________ Last name: ___________________________

ID: _____________________________ Total Marks: ____________
out of 10

- Write your name and ID in the space provided at the top of the sheet.
- Answer the questions on this sheet(s) only, using the space given.

Question 1 [2 marks]

If the Authentication Header (AH) is used in IPsec when sending a File Transfer Protocol (FTP) message, select which pieces of information are authenticated (you may select more than one – you must get all correct to receive full marks):

a) Mutable fields (those that may change) in the IP header

b) The headers from Physical and Data Link/MAC layers

c) The Authentication Data field in the AH

d) The first 96-bits of the payload

e) The TCP header

f) The entire IP header

g) The FTP header

Question 2 [4 marks]

Multiple choice. Select the most accurate answer. Choose only one. You receive 1 mark for a correct answer. You lose 0.5 marks for an incorrect answer. 0 marks for an unanswered question.

a) If you are developing a database that stores login credentials for users (e.g. username and password), you should:

   a. Save the password as plaintext

   b. Calculate the hash of the password and save the hash value

   c. Calculate the MAC of the password using a secret key, and save the MAC

   d. Encrypt the password with AES and save the ciphertext

b) Assume a password file storing the SHA1 hashes of passwords is on a Linux PC and the file is readable by all users of that PC. A practical approach to make the PC more secure against offline password guessing is:

   a. Automatically disable access to an account if too many incorrect attempts are made.

   b. Limit the speed at which passwords can be entered at the terminal.

   c. Automatically check the passwords when initially created by users, and reject the password if it is a “weak” password.

   d. Use the MD5 hash function instead of SHA1 hash function.

c) Panita’s X.509 certificate (which is signed by the certificate authority Pongpak) contains:

   a. Only Panita’s public key (and no other keys)

   b. Only Panita’s private key (and no other keys)

   c. Panita’s public key and Pongpak’s public key

   d. Panita’s private key and Pongpak’s public key

   e. Panita’s public key and Pongpak’s private key

   f. Panita’s private key and Pongpak’s private key

d) If user **A** has a X.509 certificate signed by CA **X** and user **B** has a X.509 certificate signed by CA **Y**:

   a. **A** and **B** can never authenticate each other

   b. **A** and **B** can only authenticate each other if **X** and **Y** exchange private keys

   c. **A** and **B** can authenticate each other if **X** and **Y** trust each other and exchange their public keys

   d. **A** and **B** can authenticate each other if the **A**’s certificate is sent to **B** (and vice versa)

Question 3 [2 marks]

a) In IPsec what are two security services provided by *both* Authentication Header (AH) and Encapsulating Security Payload (ESP)?

b) What security service can be provided by ESP, but not by AH?

Question 4 [2 marks]

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

b) What can be used to convert most hash functions to MAC functions?