CSS322 – Quiz 7

Name: _____ ID: _____ Marks: ____ (4)

Question 1 [3 marks]

Consider a computer system where the requirements for user authentication are to allow users to select any password they wish, and they are allowed to make an unlimited number of incorrect attempts. Explain a technique that you would implement to make the system more secure against online attacks. Also explain a disadvantage of that technique.

Question 2 [2 marks]

What is the entropy of my 10 character password, which was randomly chosen from the set of lowercase English characters, the space character and the underscore character?

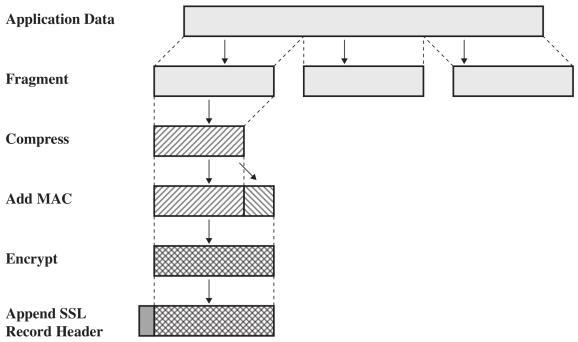
Question 3 [5 marks]

A company has developed a new protocol, called *BAHTP*, that is used by a client application on computers in shops around Bangkok to send sales information to a central server in the company main office in Rangsit. The protocol uses TCP/IP. Based on your expert knowledge of OpenSSL libraries, you have been hired by the company to modify the client/server applications so that all communications between them are secure.

(a) Draw a protocol stack of a computer using Ethernet physical and data link layers, that illustrates the protocols in use by the secure client application. [2 marks]

When using the secure application, a secure session and connection has been established. The following information is stored by the client computer for this session/connection (also shown below is the general operation of SSL record protocol):

- Session ID: id
- Compression method: null
- CipherSuite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- Master secret: s
- Server random: r_s
- Client random: r_c
- Server MAC secret: m_s
- Client MAC secret: m_c
- Server encrypt key: e_s
- Client encrypt key: e_c



(b) Write an equation that expresses the SSL record operation on a single fragment, F from the client application that produces the packet to be sent P. Use the variables above and || for the concatenate/append operator. For function names you *must* use the algorithm names (i.e. you cannot use E() for encrypt, H() for hash; refer to specific algorithms). Denote the SSL header as SSL. [3 marks]