CSS 322 – QUIZ 3A

First name: _____ Last name: _____

ID: _____ Total Marks: _____
out of 5

- 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 [4 marks]

Multiple choice – choose the most accurate answer (only choose one answer):

End-to-end encryption:

a) Requires encryption and decryption to occur at every device in the path (e.g. routers and switches)

b) Can hide the network (e.g. Internet Protocol) and link layer headers so that attackers cannot determine the destination IP address

c) Makes it easy to hide your traffic patterns (compared to link-level encryption)

d) Allows users to create a secure connection without having to trust network operators

If using the Linear Congruential Pseudo Random Number Generator to generate random numbers:

$$X_{n+1} = (aX_n + c) \bmod m$$

a) An attacker knowing the generator parameter values and previous random number, can predict the next random number.

b) The same sequence of numbers will never be repeated.

c) Reducing the size of the modulus *m*, gives a better random sequence.

d) The same sequence of numbers is generated, even if the initial value of X_0 is changed.

When encrypting using the Counter Mode of operation for block ciphers:

a) The ciphertext of one block depends on the output ciphertext from the previous block

b) The encryption algorithm (e.g. DES) in multiple blocks can be applied in parallel

c) Repetitions of the input plaintext will lead to repetitions of the output ciphertext

d) The ciphertext is less secure than when using Cipher Block Chaining

The use of a Key Distribution Centre (KDC):

a) Requires a new Master key to be created for every interaction between user A and the KDC

b) Requires one Master Key for every user

c) Requires one Master Key for every pair of users

d) Requires data to be sent between a pair of users to be encrypted with a Master Key

Question 2 [1 mark]

True or False:

a) Triple DES is more secure than DES, and more efficient than Double DES. T / F

b) The aim of the RC4 stream cipher is to make the ciphertext look random. T / F