CSS322 – Quiz 6

Name: ______________________________________

ID: _________________________ Mark: __________ (out of 6)

Question 1 [2 marks]

Forcing users to use certain types of passwords is one method to make passwords stronger against guesses. Two types of rules for users selecting passwords are: (a) random string; (b) pseudo-random pronounceable string. Explain the difference between them and compare them in terms of strengths against password guessing if the password must be a fixed length.

Question 2 [2 marks]

Apart from making passwords harder to guess, give two examples of techniques that can be used to make a system more secure against online password guessing. For each technique also explain a disadvantage of the technique.

Question 3 [2 marks]

a) Two users, A and B, have the certificate of their trusted CA X. Does user A know the public key of X? Explain your answer.

b) If user A sends its own certificate to B, explain how B validates the certificate.