1.

A system allows the user to choose a password with a length of one to eight characters, inclusive. Assume that 10,000 passwords can be tested per second. The system administrators want to expire passwords once they have a probability of 0.10 of having been guessed. Determine the expected time to meet this probability under each of the following conditions.

C = number of characters in the alphabet

R = the rate of guessing

N = the total number of passwords

T = the time to reach the expected probability of having a password broken

T = N / (10R)

1. Password characters may be any alphanumeric character (“A” through “Z,” “a” through “z,” and “0” through “9”).

c = 62 and T = 2.2109 seconds

The expected time is 70 years.

b) Password characters must be digits.

c = 10 and T = 1,111 seconds

The expected time is 18 minutes

2. Describe a password/authentication system or method that has not been covered in class. Speficy in details how it works and what are the advanteges/disadvanteges in terms of security, usability, etc. You can look for such authentication methods/systems using whatever resources you can access.

The Zero-knowledge proof makes it so that a Host is able to convince another host for access without any particular secret information. The hosts would communicate several times to finalize the authentication. The client will create a random difficult problem to solve and using the information that it has the client will solve the problem and send it to the server. The server will then check the solution or ask if the problems are related. Around ten successful exchanges are required to finish the authentication process before any access is granted. The disadvantages of the zero-knowledge proof is that while Host A thinks he is proving his identity to let’s say Host B, it is possible that Host B would authenticate to a third party, Host C, using Host A’s credentials.