Read the paper titled " How to Memorize a Random 60-Bit String" by Ghazvinnijad and Knight. After reviewing this publication answer the following:

1- Are eight character passwords secure?
2- How many eight character passwords can be formed with the 94 possible numbers, letters and symbols that can be typed on a keyboard?
3- How long would it take to crack this large number of passwords with today's (do some research) password testing abilities?
4- What if one character is added to the password sequence making it nine instead of eight. How much extra time would be required to brute force this password?
5- Using the same speed you retrieved above how long would it take to crack a 44-bit password? How about a 60-bit password? Which of the two are computationally secure in light of the resources and speed available today, if either?
6- What is the main disadvantage of using a 60-bit password? How do the authors overcome this disadvantage?
7- If you find the 60 bit password to be computationally insecure suggest a new n-bit password length and using the table provided in the paper, which method of binary sequence to text string would you choose and why?