CS336 Homework #3

Due: Friday Sep 24, 5:00pm on BbLearn
Points: 70 pts

1. (10 points) Assume that passwords are selected from four-character combinations of 26 alphabetic characters. Assume that an adversary is able to attempt passwords at a rate of one per second.
   (a) Assuming no feedback to the adversary until each attempt has been completed, what is the expected time to discover the correct password?
   (b) Assuming feedback to the adversary flagging an error as each incorrect character is entered, what is the expected time to discover the correct password?

2. (10 points) Suppose a per-subject access control list is used. Deleting an object in such a system is inconvenient because all changes must be made to the control lists of all subjects who did have access to the object. Suggest an alternative, less costly means of handling deletion.

3. (10 points) How are passwords stored on your personal computer? Pick one from 1) the password which you use to login to the system, or 2) if you use password manager which keeps your passwords for logging into different websites. Do some research and explain how it works.

4. (20 points) AES algorithm. Use 4*4 tables to represent a state block. Explain in detail.
   (a) (AES S-box) Assume you have a State block as defined below, indicate the size of the block and find the new state after applying the AES S-box (can be found in the slides Lec8) transformation. Consider each 4-tuple below a column in the input block.
   State: D1 26 B9 3C; 59 C2 AC 42; 15 BC 42 A9; 39 DA D3 26.

   (b) (AES Add round key) Assume the round key is as indicated below. Please show the result of the last state of the round assuming that the state before adding the key is the state resulting from 4(a) above. Also, assume that the block key is written in a row format (each 4-tuple is one row of the block)
   Round Key: 36 24 A3 82; 00 00 00 00; AA B2 30 57; 11 43 1D C1.

5. (10 points) Consider a Diffie-Hellman scheme with a common prime q = 11 and a primitive root a = 2. **(Do not use calculator!)**
   - If user A has public key Ya = 9, what is A's private key Xa?
   - If user B has public key Yb = 3, what is the shared secret key K?

6. (10 points) In a public-key system using RSA, you intercept the ciphertext C = 10 sent to a user whose public key is e = 5, n = 35. What is the plaintext P? **(Do not use calculator!)**