EECE 412, Fall 2009

Quiz #3

This quiz consists of 4 **pages. Please check that you have a complete copy. You may use both sides of each sheet if needed.**

Your Family name: ________________

Your Given name: ________________

Your student ID: ________________

#	Points	Out of
1		7
2		4
3		4
TOTAL		15

Name of your left neighbor: ________________

Name of your right neighbor: ________________

ATTENTION: When necessary, make reasonable assumptions and state them clearly in your solutions.

1. **Strength of your password.**
   a. **(1 point) Assume that your online banking password is “6LopxHi!”. Indicate below how many low case, capital case, digits, and special characters it has.**

Number of alpha characters in your password	
Number of special characters, e.g.,)[!(#@$%^&~;:”,.+_-`}{]\/?, in your password	
Number of numeric characters in your password	
Total number of characters in your password	

   b. **(2 points) Compute** <u>**theoretical**</u> **entropy of the password. State clearly your assumptions about the size of the special character space and any other assumptions. Explain your answer.**

   Possible helpful reminder: $\log_b(x) = \frac{\log_k(x)}{\log_k(b)}$.

   c. **(2 points) Compute** <u>**effective**</u> **entropy of the password. State clearly your assumptions about the size of the special character space and any other assumptions. Explain your answer.**

   Possible helpful reminder: $\log_b(x) = \frac{\log_k(x)}{\log_k(b)}$.

d. **(1 points) How long, on average, will it take for an attacker to "crack" your password if she can use her computing resources to test 2^21 candidates per second? Consider only the theoretical entropy of your password. Explain your answer. Assume that your password hash is salted.**

e. **(1 points) How long, on average, will it take for an attacker to "crack" your password if she can use her computing resources to test 2^21 candidates per second? Consider only the effective entropy of your password. Explain your answer. Assume that your password hash is salted.**

2. **Assuming the attacker cannot perform an off-line dictionary attack, list the techniques that your bank can employ for reducing the chance of your account being compromised through an on-line dictionary attack?**

3. **Compare and contrast ACLs and capability lists.**