EECE 412, Fall 2010

Quiz #3 Key

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 "big3oiv&w". Indicate below how many low case, capital case, digits, and special characters it has.**

Number of alpha characters in your password	6
Number of special characters, e.g.,)[!(#@$%^&~;:",.+_-`}{]\/?, in your password	1
Number of numeric characters in your password	1
Total number of characters in your password	8

   b. **(2 points) Compute simple 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: $\log_b(x) = \dfrac{\log_k(x)}{\log_k(b)}.$

Assumptions: 26*2= 52 alpha characters, 26 special characters, 10 numeric characters.

Theoretical entropy of the above password is $\ln_2$((52+26+10)**8) = 8 $\ln_2$(88) =8*6.5 = 51.7 ≈ 52 bits

   c. **(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 2^22 candidates per second? Explain your answer. Assume that your password hash is salted.**

Recalculate this: (2**(52-1))/(2**22) = 2**30 seconds = 2,147,483,648/3600/2 = 596,523 hours = 12,428 days, which is little bit over 34 years.

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?

- Exponential back-off
- Disconnection
- Account disabling
- Jailing
- Two-factor authentication

3. Remember that the purpose of using session key is to prevent the attacker from finding the shared key even if she breaks the session key. Such session key can be considered as "secure". Suppose R is a random challenge sent in the clear from Alice to Bob and K is a high-entropy symmetric key known to both Alice and Bob. Which of the following are secure session keys and which are not? Explain your answer:

a) $h(R \oplus K)$ is _√_ secure, __ not secure, because:

Because of one-wayness of h(•), Trudy cannot find $R \oplus K$ and therefore, K.

b) $E_K(R)$ is _√_ secure, ___ not secure, because:

Trudy cannot find S by knowing R.

c) $E_R(R \oplus K)$ is ___ secure, _√_ not secure, because:

Trudy can find K by $R \oplus D_R(S)$, since block ciphers are invertible.

d) $h(K \| R)$ is _√_ secure, ___ not secure, because:

Trudy cannot find K due to the one-wayness property of h(•).

e) $E_R(h(K \oplus R) \| K)$ is __ secure, _√_ not secure, because:

Trudy can find K by decrypting the session key and then looking up the K part of the decryption output.

f) $D_{h(R \| K)}(R)$ is _√_ secure, ___ not secure, because:

Trudy cannot find K due to the one-wayness property of h(•).