EECE 412, Fall 2012

Quiz #3

This quiz consists of 6 **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		**3**
2		**9**
3		**6**
4		**4**
5		**1**
6		**1**
TOTAL		**24**

Name of your left neighbor: _____

Name of your right neighbor: _____

Notes:

- Make sure your handwriting is legible. If the teaching staff does not understand what your wrote, they mark your answer as if the unreadable text is missing.

- Aim to be precise and to the point. The experience of teaching this course since 2004 suggests that excessively long answers tend to correlate with lower marks.

- As in real world, stated questions and/or accompanied descriptions in this quiz are often open-ended and one has to make assumptions in order to answer them. If you do make assumptions, state them clearly and explicitly.

- The mark for this quiz will be pro-rated. That is, the best answer receiving 100% and the marks for all other answers being pro-rated accordingly. So, don't panic if you feel like you are severely short on time. Everybody is. ☺

1. **A digital signature provides for data integrity and MAC provides for data integrity. Why does a digital signature also provide for non-repudiation while MAC does not?**

2. **Suppose that Alice and Bob share a 4-digit PIN number, *X*. To establish a shared symmetric key, Bob proposes the following protocol: Bob will generate a random key *K* that he will encrypt using the PIN *X*, that is, E(*K*, *X*). Bob will send E(*K*, *X*) to Alice, who will decrypt it using the shared *X* to obtain *K*. Alice and Bob will then use the symmetric key *K* to protect their subsequent conversation.**

   Trudy can easily determine *K* by a brute force attack on *X*, so this protocol is insecure. Modify the protocol to make it more secure. Note that Alice and Bob only share 4-digit PIN *X* and they do not have access to any other symmetric or public key.

   Hint: Use Diffie-Helman.

3. **Suppose that you have *n* accounts, each of which requires a password. Trudy has a dictionary and the probability that a password appears in Trudy's dictionary is *p*.**
    a. **(1 point) If you use the same password for all accounts, what is the probability that your password appears in Trudy's dictionary?**

    b. **(2 points) If you use distinct passwords for each of your n accounts, what is the probability that at least one of your passwords appears in Trudy's dictionary? Show that if n == 1, your answer agrees with your answer to question a.**

    c. **(3 points) Which is more secure, choosing the same password for all accounts, or choosing different passwords for each account? Explain your answer.**

4. **Suppose that when a fingerprint is compared with one other (non-matching) fingerprint, the chance of a false match is 1 in 1,000. Suppose that the RCMP fingerprint database contains 10^7 fingerprints.**
    a. **(2 points) How many false matches will occur when 100,000 suspect fingerprints are each compared with the entire database? Explain your answer.**

    b. **(2 points) For any individual suspect, what is the chance of a false match? Explain your answer.**

5. **You are to choose a password policy for your large organization among the following candidate policies. Which one would you choose in order to make long cracking sessions least effective:**

    a. **Password can of any length and content, but it should contain at least one upper case letter.**

    b. **Password cannot be from the list of 50,000 most popular passwords.**

    c. **Password must be at least 9 characters long.**

6. **The evaluation of peer-pressure approach to the choice of passwords found that the approach is statistically significantly better than which of the following?**

    a. **Control condition without any motivator**

    b. **Existing motivator**

    c. **Both Control and existing motivator**

    d. **None**