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**
TOTAL		**22**

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?**

MAC (or message authentication code) is constructed on the bases of symmetric crypto, where more than one entity poses the secret. Such possession makes it possible for either of the party to construct such a MAC. Thus, any party can easily deny that they generated a MAC.

In digital signature a private key is used to generate a signature, and the private key is known only to one party (i.e., the owner of the private/public key pair). Thus, only the owner can generate a signature, thus, cannot deny that she/he generated the signature.

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.

Alice	Bob
Generate a, p and g	Generate b
Send E(p,g, g^a mod p,X)	
	Send E(g^b mod p,X)
Calculate session key: $K_s = g^{ab} \bmod p$	Calculate session key: $K_s = g^{ab} \bmod p$
Session established with K_S	

This protocol will ensure forward perfect secrecy, since even if X is known, there is no way for Trudy to recover K_S.

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?**

p

   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.**

Let's q will define the probability that a password is NOT in the dictionary, i.e., q=1-p. Thus, the probability of all events is p+q=1. Now, the only case when we do not satisfy the requirements of the problem, i.e., at least one password in DB, is when all passwords are not in the DB. The probability of such event is q^n. Apart from this even, all cases satisfy the requirement of the task. As we previously stated, the probability of a passwords to be in the dictionary and not to be in the dictionary is 1 and equals p+q. For n passwords, this probability will be $(p+q)^n$. Thus, probability that at least one password is in the DB is $P = (p+q)^n - q^n$, where p is for the only password which is in the dictionary and q^{n-1} for other passwords that are not. If we have only one password it is easy to see that P=p.

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

Choosing a separate password for each account is more secure. This could be explained by using limits for the above formulas. In particular, let's consider the case when we use the same password for all accounts:
$\lim_{n\to\infty} P = p$, i.e., no matter what is the value of n, the limit is constant.

If we consider the case when a separate password is used for each account then:
$\lim_{n\to\infty} P = \lim_{n\to\infty}(1 - q^n) = 1 - \lim_{n\to\infty} q^n \approx 1$, since q<1, and n>>1. Thus it looks worse than having the same password. However, the case with the same password compromises ALL assets, where the other case only impacts one account. For these two cases to be comparable we have to compare them with the same outcome, i.e., ALL accounts are compromised. That is $P=p^n$
$\Rightarrow \lim_{n\to\infty} P = \lim_{n\to\infty} p^n \approx 0, p < 1 \text{ and } n \gg 1$

This shows that the probability for all accounts to be compromised in the case when separate passwords are used is significantly lower and approaches 0 very fast (in exponential manner).

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.**

Probability of false match P_f=0.001
Database N=10,000,000 = 10^7
Number of suspect n=100,000= 10^5
Total number of comparisons (every suspect with every entry in DB) $C_n = n*N = 10^{12}$
Number of false matches $N_{fm} = C_n * P_f = 10^{12-3} = 10^9$

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

Probability of false match P_f=0.001, $Q_f = 0.999$.
$P_{fm}=1-Q_f^N \approx 1 - 0 = 1$

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.**

    All others still allow very short passwords, which can be searched by brute-force in a matter of minutes.

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**