**CSCI 475/585:  Information Security and Privacy**

**Homework 1 Assignment**

**Please follow the requirements and due date specified in the Syllabus to submit your work.**

**Please also include a comment to tell me:**

How much time did you spend on this assignment? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. You have a smartphone, and have many fancy apps installed on it.
2. Please give examples of confidentiality, integrity, and availability requirements associated with your smartphone and your data on it.  And in each case, please also indicate the degree of importance (i.e., high/moderate/low levels of impact from a potential security breach) of the requirement. (20 points)
3. Which of your installed apps is least trustworthy for you and why? Note that please feel free to skip this sub-question if you are not comfortable to share this information with the class due to security, privacy, or any other reasons.
4. Our IT infrastructure at Mines needs to be well protected. Please list and briefly define categories of passive and active network security attacks that may target our IT infrastructure. What are our emphases in dealing with these two different types of attacks? (20 points)
5. What are the two basic types of transformation operations used in modern ciphers such as DES and AES? Why both types of transformation operations are needed by DES and AES? (20 points)
6. Suppose that someone suggests the following way to confirm that the two of you are both in possession of the same secret key. You create a random bit string the length of the key, XOR it with the key, and send the result over the channel. Your partner XORs the incoming block with the key (which should be the same as your key) and sends it back. You check, and if what you receive is your original random string, you have verified that your partner has the same secret key, yet neither of you has ever transmitted the key. Is there a flaw in this scheme? Please briefly explain your answer. (20 points)
7. What are the fundamental differences between the two widely used ciphers AES and RSA? Please also identify two examples in your real online activities, in which AES and RSA are used, respectively. (20 points)