CS 678 – Data Security Fall 2016 **Instructor: Prof. P. T. Chung**

Homework 1 (100 Points) (Due 10/1).
For homework assignment, individual work is encouraged; Small group work is permitted, you may work with group and have a group formed by 2~3 team members; For any case, no plagiarism is allowed and Technical Writing with citations should be followed for preparing essay style questions. ***Please submit your work to pingtsaichung@gmail.com***
(i.e., ptchung@ieee.org) on* 9/30 *and hand in one hard copy in class on 10/1. *For group work, please list names of your co-workers in your homework cover sheet, only one submission is necessary.* ***Note that please show intermediate steps to get your final answers, if applied.*** *Thank you.*

I. Reading Assignments:

1.Read – Textbook Chapter 1 - Introduction, and Chapter 8 – Cryptography

2. Read Notes on Introduction and Notes on Conventional Encryption.

II. Homework Assignments:

Problem 1: (Computer Security) Each user on a computer system has a password, which is six to eight characters long, where each character is an uppercase letter or a digit. Each password must contain at least one digit. How many possible passwords are there (10 Points)?

Problem 2: (Confidentiality and Data Integrity) Do the problems R-1.4 and R-1.5. (20 Points)

Problem R-1.4. What are some of the techniques that are used to achieve confidentiality?
Problem R-1.5. What is the most efficient technique for achieving data integrity?

Consider an automated teller machine (ATM) in which users provide a personal identification number (PIN) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system. In each case, indicate the degree of importance of the requirement.

Problem 3: (The C.I.A. and A.A.A. Concepts) Do the problems R-1.9 and R-1.10. (20 Points)

Problem R-1.9. With respect to the C.I.A. and A.A.A. concepts, what risks are posted by packet sniffers, which monitor all the packets that are transmitted in Wireless Internet access point?

Problem R-1.10. With respect to the C.I.A. and A.A.A. concepts, what risks are posted by someone burning songs from an online music store onto a CD, then ripping those songs into their MP3 player software system and making dozens of copies of these songs for their friends?

Problem 4: (Attack and Risks) Do the problems R-1.14 and R-1.16. (20 Points)

Problem R-1.14

Suppose the author of an online banking software system has programmed in a secret feature so that program emails him the account information for any account whose balance has just gone over $10,000. What kind of attack is this and what are some of its risks?

Problem R-1.16

Give an example of the false sense of security that can come from using the "security by obscurity" approach.

Problem 6: (Symmetric Encryption) Do the problem R-1.18. (20 Points)

Problem R-1.18

Suppose that a symmetric cryptosystem with 32-bit key length is used to encrypt messages written in English and encoded in ASCII. Given that keys are short, an attacker is using a brute-force exhaustive search method to decrypt a ciphertext of t bytes. Estimate the probability of uniquely recovering the plaintext corresponding to the ciphertext for the following values of t: 8, 64, and 512.

Problem 7: (Attacks) Do the problems R-8.2 (10 Points)

Problem R-8.2

Eve has an antenna that can pick up Alice's encrypted cell phone conversations. What type of attack is Eve employing?