SCR3443 – Sem I 2012/13
Tutorial 1: Introduction to Cryptography

1. Which security service(s) are guaranteed when using each of the following methods to send mail at the post office?
   a) Regular mail
   b) Regular mail with delivery confirmation
   c) Regular mail with delivery and recipient signature
   d) Certified mail
   e) Insured mail
   f) Registered mail

2. Define the type of security attack in each of the following cases:
   a) A student breaks into a professor's office to obtain a copy of the next day's test.
   b) A student gives a check for $10 to buy a used book. Later she finds that the check was cashed for $100.
   c) A student sends hundreds of e-mails per day to another student using phony return e-mail address.

2. Which security mechanism(s) are provided in each of the following cases?
   a) A school demands student identification and a password to let students log into the school server.
   b) A school server disconnects a student if she is logged into the system for more than two hours.
   c) A professor refuses to send students their grades by e-mail unless they provide student identification they were pre-assigned by the professor.
   d) A bank requires the customer's signature for a withdrawal.

3. Which technique (cryptography or steganography) is used in each of the following cases for confidentiality?
   a) A student writes the answers to a test on a small piece of paper, rolls up the paper, and inserts in a ball-point pen, and passes the pen to another student.
   b) To send a message, a spy replaces each character in the message with a symbol that was agreed upon in advance as a character's replacement.
   c) A company uses special ink on its checks to prevent forgeries.
   d) A graduate student uses watermarks to protect her thesis, which is posted on her website.

4. What type of security mechanism(s) are provided when a personal signs a form he has filled out to apply for a credit card?
5. What is the difference between a "Known-Plaintext" attack and a "Chosen-Plaintext" attack? Which one is more easy and beneficial from a cryptanalyst point of view and why? Justify your answer.
6. Conduct an Internet searching for information on cryptography flaws and document them. Explain the consequences of each of the flaws and suggest method or technique to overcome the flaws. Note: Use the knowledge that you have learn in Computer Security lectures.