CSC4222/6222: Assignment 1

Hard copy due at 12:30 pm, Sep. 12

---

1. 1) Explain the concepts of C.I.A and the tools to achieve C.I.A, respectively.
   2) What are the differences between message confidentiality and message integrity? Can you have confidentiality without integrity? Can you have integrity without confidentiality? Justify your answer.
   3) Please Specify and explain which concept(s) each of following cases violates.
   a. John copies Mary's homework.
   b. Paul crashes Linda's system.
   c. Carol changes the amount of Angelo's check from $100 to $1,000.
   d. Gina forges Roger's signature on a deed.
   e. Rhonda registers the domain name "AddisonWesley.com" and refuses to let the publishing house buy or use that domain name.
   f. Jonah obtains Peter's credit card number and has the credit card company cancel the card and replace it with another card bearing a different account number.
   g. Henry spoofs Julie's IP address to gain access to her computer.
   h. Jonah sends Peter an e-mail with a 2MB attachment, knowing that Peter's remaining quota for his e-mail account is 2.1MB.
   i. Anna registers the domain name "JohnSmith.com" and refuses to let John Smith buy or use the domain name.

2. Compare and contrast symmetric encryption with public-key encryption, including the strengths and weaknesses of each.

3. What is Authenticity and the tools to achieve Authenticity?
   Please Explain: Can Bob violate an agreement with his digital signature or not?

4. Please describe the concept of the following methods of Threats & Attacks and give a protecting method.
   a. Alteration
   b. Denial-of-Services
   c. Correlation and Traceback

5. Please explain what if a newly designed system without the following Security Principles:
   a. Fail-Safe Default
   b. Complete Mediation
   c. Separation of Privilege

6. Suppose Alice wants to send an email to Bob. Bob has a public-private key pair

(KB+, KB-), and Alice has Bob's certificate. But Alice does not have a public, private key pair. Alice and Bob (and the entire world) share the same hash function H(.).

a. In this situation, is it possible to design a scheme so that Bob can verify that Alice created the message? If so, show how with a block diagram for Alice and Bob.

b. Is it possible to design a scheme that provides confidentiality for sending the message from Alice to Bob? If so, show how with a block diagram for Alice and Bob.

7. **a.** Can you "decrypt" a hash of a message to get the original message? Explain your answer.

   b. In what way does the public-key encrypted message hash provide a better digital signature than the public-key encrypted message?

8. Bob thinks that generating and storing a random salt value for each userid is a waste. Instead, he is proposing that his system administrators use a cryptographic hash of the userid as its salt. Describe whether this choice impacts the security of salted passwords and include an analysis of the respective search space sizes.

9. Suppose you could use all 128 characters in the ASCII character set in a password. What is the number of 8-character passwords that could be constructed from such a character set? How long, on average, would it take an attacker to guess such a password if he could test a password every nanosecond?

10. **a.** Barack often sends funny jokes to Hillary. He does not care about confidentiality of these messages but wants to get credit for the jokes and prevent Bill from claiming authorship of or modifying them. How can this be achieved using public-key cryptography?

    b. As public-key cryptography is computationally intensive and drains the battery of Barack's device, he comes up with an alternative approach. First, he shares a secret key k with Hillary but not with Bill. Next, together with a joke x, he sends over the value d = h(k||x), where h is a cryptographic hash function. Does value d provide assurance to Hillary that Barack is the author of x and that x was not modified by Bill? Justify your answer.