1. Chapter - 1 (1 Question 10 points)
   (a) Please classify each of the following as a violation of confidentiality, of integrity, of availability or of some combination of those:
      i. John copies Mary’s homework.
      ii. Paul crashes Linda’s system.
      iii. Carol changes the amount of Angelo’s check from 100 to 1000.
      iv. Gina forges Roger’s signature on a deed.
      v. Rhonda registers the domain name AddisonWesley.com and refuses to let the publishing house buy or use the domain use the name.

2. Chapter - 9 (3 Questions 30 points)
   (a) Using two substitution ciphers one after another may not be more secure than using a single substitution cipher. True or False? Explain why by means of a suitable argument or an example.
   (b) In a public-key system using RSA, you intercept the ciphertext C=13 sent to a user who's public key is e = 3, n = 33. What is the plaintext M?
   (c) Alice and Bob share a secret key of some private key system. Bob has a message he claims came from Alice and to prove this he produces a plaintext message and a ciphertext. The ciphertext decrypts to the plaintext under the secret key which Alice and Bob share. Please explain why this does not satisfy the requirements of non-repudiation of origin. How would you modify a classical cryptosystem to provide non-repudiation?

3. Chapter - 10 (2 Questions 20 points)
   (a) Can the Diffie-Hellman protocol be used for authentication? Why or why not?
   (b) What is a certificate? What are they used for? How does one check the authenticity of a certificate?

4. Chapter - 11 (1 Questions 10 points)
   (a) Describe a method by which a block cipher maybe converted to a stream cipher. Why would this be desirable?

5. Chapter - 12 (2 Questions - 20 points)
   (a) Explain how Lamport’s one-time password scheme works. Explain why the scheme is not compromised if an attacker obtains the password database in the server?
   (b) This question concerns the ability of attackers to crack UNIX passwords on a system where the password file is world-readable and contains the users’ password hashes. Two approaches for reducing the probability that a password will be guessed are: increase the size of the salt from 12 bits to 24 bits in the obvious way; or increase the length of the password to 16 characters by hashing the first 8 characters using the current hash function, the second set of 8 characters using the current hash function and the salt, and concatenating the two. Assume an attacker is attempting to guess a particular user’s password. Which method increases the estimated time of guessing the password the most? Why?

6. Chapter - 13 (1 Question - Take Home - 10 points)
   (a) Describe the security aspects of real life system that you are familiar with. Criticize the design of the security sub-system with respect to the principles outlined in Chapter 13. State how and which principles are indeed followed and which have not been followed.