**Chapter 1**

* 1. The automatic protection which its purpose is to preserving the integrity, availability and confidentiality of systems, components or resources

1.3) The passive attack is to learn or observe the system but it would not damage the system

The active attack involves with modification of the data or information

1.4) Passive Attacks  
 - Release of Message Contents  
 The attackers would not damage with the system  
 but they would just get some contents of the  
 information.  
 - Traffic Analysis  
 The opponent purpose is to observe in deep  
 details of communication such as hosts,   
 destination, or length of messages.

Active Attacks  
 - Masquesrade  
 The authorization with the other authorized  
 sequences to get privileges.  
 - Replay  
 involves the passive capture of a data unit  
 and its subsequent retransmission to  
 produce an unauthorized effect.

- Modification of Messages  
 Modifying some contents in the message.  
 - Denial of Service  
 preventing the regular use or  
 management of communications facilities

**Problems**

1.4) (a) All are moderate because it is a public information  
 (b) Confidentiality and integrity should be high, and availability is moderate because as it is a investigation information, so it needs to be secured and make sure that the contents of it are not modified.  
 (c) Confidentiality and integrity must be high, and availability is moderate because it relates to financial information.  
 (d) Confidentiality should be high, integrity is moderate and availability is low because contract information must be considered about security first as it is a personal information. However, it also must not be modified to make sure that the information is correct.  
 (e) All are high because it is a real time system and controlling the  
distribution of electric power.

1.7) According to cookies, which is used to authorize the user next time, are stored in the text file. So, it means if there is an opponent who could access to modify or capture the text file, the authorized cookies could be modified or copied to use to access to the website as a user’s privileges. So, it could be really risky and harmful to the security of the website.

**Chapter 2**

2.2) One  
  
 2.3) Strong Encryption Algorithm, and sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure

2.4) Conventional Encryption, Public-key Encryption, and Secret Value  
  
2.7) 1. can be applied to a block of data of any size.  
 2. produces a fixed-length output.  
 3. is relatively easy to compute for any given x  
  
2.8) Plaintext, Encryption Algorithm, Public and private keys, Cipertext, and Decryption algorithm

2.10) The key which is used in conventional encryption is referred to a secret key. The two keys used public-key encryption are referred to public and private key

2.11) A method which is used to authenticate a message

2.13) Encrypt the message via using symmetric key encryption one- time key. Encrypt the one-time key using public-key encryption with receiver’s public key. Finally, attack the encrypted one-time key to encrypted message.

**Problems**  
2.5) (a) Yes (in both cases). auth(x) would not match x.  
 (b) No (in both cases). Unless the computation of auth(x) was affected by some time-stamp/sequence number.  
 (c) 1.Yes - only Alice has her private key, and only Alice's key matches the Alice's public key which is used by Bob to authenticate x.  
 2. Yes - only Alice and Bob share the secret key used to generate auth(x). While auth(x) generated by Oscar might be valid, it does not match auth(x) calculated by Bob.  
 (d) 1. Yes - auth(x) is generated with Alice's private key, and verified with Alice's public key. So only Alice can generate auth(x).  
 2. No - auth(x) is generated and verified with the secret key, which both Alice and Bob hold.