Chapter 1

- **Define computer security.**
  - **Measure and control that ensure confidentiality and availability and integrity of information system assets including hardware, software and information being processed, stored and communicated.**
- **What is the difference between passive and active security threats?**

Passive security	Active security
Attempts to learn or make use of information from system but does not affect system resources	Attempts to alert system resources or affect their operations
Release of message content, traffic analysis	Reply, masquerade, modification of massages, denial of service

- **List and briefly define categories of security services.**
  - **Network attack surface: vulnerability over an enterprise network, wide-area network or the internet.**
  - **Software attack surface: vulnerability in application, utility, or operating system code.**
  - **Humane attack surface: vulnerability created by personnel or outsiders, such as social engineering, trusted insiders, human error**

Chapter 2

- **What are the essential ingredients of a symmetric cipher?**
  - **Plaintext**
  - **Encryption algorithm**
  - **Public key**
  - **Ciphertext**
  - **Decryption algorithm**
- **How many keys are required for two people to communicate via a symmetric cipher?**
  - **1 key**
- **What are the two principal requirements for the secure use of symmetric encryption?**
  - Strong encryption algorithms
  - Sender and receiver must have copies of secret key and keep key secure.
- **List three approaches to message authentication.**
  - Message authentication with symmetric keys
  - Message authentication without message encryption
  - Secure hash function

What is a message authentication code?

- One of authentication techniques involve the use of secret key to generate a small block

Briefly describe the three schemes illustrated in Figure 2.4

- That is appended to the messages. This technique assumes that 2 communicating parties, say A and B, share a common secret key K_{AB}.

What properties must a hash function have to be useful for message authentication?

- Can be applied to block of data of any size
- H(x) is relatively easy to compute for any given x
- Product a fixed-length output
- One-way or pre-image resistant
- Infeasible to find y != x such that H(x) = H(y)
- Collision resistant or strong collision resistance

What are the principal ingredients of a public-key cryptosystem?

- Easy to create key pairs
- Easy for sender knowing public key to encrypt messages
- Easy for receiver knowing private key to decrypt messages
- Useful if either key can be used for each role
- Infeasible for opponent to recover original message

List and briefly define three uses of a public-key cryptosystem

- Digital signature: provide only the signature function
- Symmetric key : like RSA, Diffie-Hellman
- Encryption of secret key : based on mathematical function like RSA

What is the difference between a private key and a secret key?

- Secret key -> used in symmetric encryption systems
- Private key -> used in asymmetric encryption systems

What is a digital signature?

- It provides only the signature function, can't use for encryption or key exchange

What is a public-key certificate?

- It contains public key plus user id of the key owner and CA

How can public-key encryption be used to distribute a secret key?

- Using key exchange method

Chapter 3

In general terms, what are four means of authenticating a user's identity?

- Something you know
- Something you have
- Something you are
- Something you do

- **List and briefly describe the principal threats to the secrecy of passwords.**
  - Offline dictionary attack
  - Password guessing
  - Rain bows table
  - Specific account attack
  - Popular password attack
  - Workstation hijacking
- **What are two common techniques used to protect a password file?**
  - restrict access to the password file using standard access control measures.
  - Complex password
- **List and briefly describe four common techniques for selecting or assigning passwords.**
  - User education
  - Complex password
  - reactive password checking
  - computer generated passwords
- **Explain the difference between a simple memory card and a smart card.**

Simple memory card	Smart card
Can stored but not process data	Contains an entire microprocessor (processor, memory, I/O ports)
Like magnetic stripe card	Like eID

- **List and briefly describe the principal physical characteristics used for biometric identification.**
  - Fingerprint: have been used as a mean of identification for centuries
  - Iris: unique physical characteristic is the detailed structure of the iris
  - Facial characteristics: are the most common means of human-to-human identification
  - Signature: Each individual has a unique style of handwriting and this is reflected especially in the signature
  - Hand geometry: system identify features of hands

Chapter 7

- **Define a denial-of-service (DoS) attack.**
  - An action that prevents or impairs the authorized use of networks, system or application by exhausting resources such as CPU, memory, bandwidth, disk space
- **What types of resources are targeted by such attacks?**
  - System resources
  - Applications resources
  - Network bandwidth
- **What is the goal of a flooding attack?**
  - Overload network capacity on some links to a server
- **What types of packets are commonly used for flooding attacks?**
  - UPD flood
  - TCP Syn flood
  - ICMP flood
- **Why do many DoS attacks use packets with spoofed source addresses?**
  - To reflect flow of packets and the ability to identify the attacker are reduced.
- **Define a distributed denial-of-service (DDoS) attack.**
  - Attack use multiple systems to generate attacks
- **What architecture does a DDoS attack typically use?**
  - A DDoS attack typically uses a botnet architecture, which is a network of compromised computers or devices that are controlled by an attacker to flood a target system with traffic and overwhelm its resources.
- **Define a reflection attack.**
  - It uses to generate enough volume packets to flood the link to the target system without alerting
- **Define an amplification attack.**
  - Exploit DNS behavior to convert small response to much larger response
- **What is the primary defense against many DoS attacks, and where is it implemented?**
  - Attack prevention and preemption (before attack)
  - Attack detection and filters (during attack)
  - Attack source track back identification (during and after attack)
  - Attack reaction (after attack)

- **What defenses are possible against TCP SYN spoofing attacks?**
  - Send TCP packets to target system
  - Total volume of packets is the aim of attack rather than the system code
- **What do the terms slashdotted and flash crowd refer to? What is the relation between these instances of legitimate network overload and the consequences of a DoS attack?**
  - used to describe such occurrences
  - There is very little that can be done to prevent this type of either accidental or deliberate overload without also compromising network performance
- **What defenses are possible to prevent an organization's systems being used as intermediaries in an amplification attack?**
  - Block spoofed source addresses
  - Filters may be used
  - Use modified TCP connection handle code
  - Blocked IP direct broadcast
  - Block suspicious services
  - Good general system security practices
  - Manage application attacks with a form of graphical puzzle(captcha)
- **What steps should be taken when a DoS attack is detected?**
  - Antispoofing, direct broadcast
  - Identify network monitors and ids
  - Identify type of attacks
  - Have ISP trace packet flow
  - Implement plan
  - Update incident response plan