Note: choose five questions only

Q1) Define the functions for each the following:
   a- Hub, b- Gateway, c- Backbone cable, d- DQDB, e- SMTP, f- UDP.  
   (12 marks)

Q2) a- Define the Protocol stack, and explain how to provide communication between
    protocols consist of five-layers.
    b- Explain data flow types with examples (using the design in your examples).  
    (12 marks)

Q3) Give short answers for the following:-
    a- The basic processes for network layer in TCP/IP protocol.
    c- The differences between connection-oriented and connectionless.
    d- The advantage for Maximum Transmission Unit (MTU).
    e- Explain the transport layer functions.  
    (12 marks)

Q4) a- Explain the principles that were applied to arrive at the seven layers in OSI model.
    b- Define mesh topology and give example to find the number of physical links in a
    fully connected mesh network with n nodes.  
    (12 marks)

Q5) a- LANs are distinguished from other networks by some characteristics, what are they?
    b- Explain the main types for Baseband Coaxial Cable.  
    (12 marks)

Q6) a- Comparison of the OSI and TCP Reference Models.
    b- Comparison of Fiber Optics and Copper Wire.  
    (12 marks)
access control: A record containing information that identifies a user, including a secret password. User accounts are associated with some form of secret, such as a password, PIN, biometric hash, or a device like a smart card that contains a larger, more secure password than a human could remember. To the system, there is no concept of a human; there is only secret, information tied to that secret, and information to which that secret has access.

Boot sector: Boot sector viruses were the original viruses, and they spread by the only common means of sharing information in the early days of computers—on floppy disks.

The requirements that must satisfy in cryptosystem.

Sol: 1) The enciphering and deciphering transformations must be efficient for all keys.

2) The system must be easy to use.

3) The security of the system should depend only on the secrecy of the keys and not on the secrecy of the algorithms E or D.

Define the virus and explain virus propagation.

Sol: Virus is any program that automatically replicates itself, programs will spread them and which will simply cause them to lie dormant? Usually, they don't. Viruses only know the program that was running when they were first executed (like Internet Explorer) and the program that started that program. When a virus is first executed, it attaches itself to the beginning of the current program.

The condition that must considered in firewalls.

1- The firewall must be ease to use, has powerful graphical user Interfaces (GUI), which simplifies the job of installation, configuration, and management

2- The firewall must has high performance, should be fast enough so users do not feel the screening of packets. The volume of data throughput and transmission speed associated with the product should be consistent with the company’s bandwidth to the Internet
3. The firewall must be flexible, should be open enough to accommodate the security policy of the company, as well as to allow for changes in the features. Remember that a security policy should a very seldom change, but security procedures should always be reviewed, especially in light of new Internet and web centric application

explain password authentication, and show the ways that password authentication fail in it.

Sol: The process of determining a user's identity in order to allow access

1. replay attack: An attack in which a secret value like a hash is captured and then reused at a later time to gain access to a system

2. Password Hashing: To prevent hackers from capturing your password from your computer's hard disk or while it transits the network, passwords can be encrypted using a one-way function or hashing algorithm to keep them from being revealed

Explain the virus propagation and give the common types for virus attacks.

sol:
When a virus is first executed, it attaches itself to the beginning of the current program. The next time that program is run, the virus takes the information about the program that started the current program to determine what file it should infect next and attaches itself to the beginning of that program. In this way, the virus propagates one step closer to the beginning of the chain each time the programs in the startup chain are launched.

- worms

Viruses that spread over a network automatically without human intervention. Viruses also attach themselves to each program that the current program launches. In most cases this is nothing—most applications can’t launch other programs. But some do, and when those applications are found, the virus automatically spreads.

The graphic that follows shows how a virus attached to Internet Explorer can propagate back to the program that launched it (Word), then back to Windows Explorer, and from there to other applications.
It’s important to note that viruses require human activity—booting a floppy, executing a program, or opening an attachment—in order to activate and spread. Viruses that can spread without human activity are referred to as worms. Worms typically exploit buffer overrun attacks against common Internet services like mail or web.

**Vectors that hackers exploit to access your network.**

Sol: There are only four ways for a hacker to access your network:

1. By connecting over the Internet
2. By using a computer on your network directly
3. By dialing in via a Remote Access Service (RAS) server
4. By connecting via a nonsecure wireless network