**Chapter 6**

**Security Technology: Access Controls, Firewalls and VPNs**

1. Highlight seven biometric authentication technologies that are available for verifications of one’s identity. (7 marks)
2. Authorisation is the matching of an authenticated entity to a list of information assets. Discuss ant three ways in which authentication can be handled. (6 marks)
3. What is the purpose of a content filter on an organisation’s network? (4 marks)
4. Access control are divided into two approaches. Briefly explain these approaches. (4 marks)
5. Biometric technologies are evaluated on three basic criteria. Explain each of them. (6 marks)
6. A VPN that proposes to offer a secure and reliable capability while relying on public networks. What should any technologies and protocols used seek to provide between any two communication entities. (6 marks)
7. Briefly explain how firewall devices can be configured in several network connection architectures. (20 marks)
8. Discuss the five different categories of firewall processing modes. (25 marks)

**Chapter 7**

**Intrusion Detection and Prevention Systems**

1. Explain the two types of Intrusion Detection and Prevention System (IDPS). (10 marks)
2. Explain any countermeasures can be taken to help prevent a successful DDoS attack

on a network. (20 marks)

1. When analysing the organisation’s systems, you realise that the company does not have a defence strategy in place to prevent unauthorised access to its systems. Discuss any two types of defence strategy which can be implemented in an organisation. (10 marks)
2. What are some of the factors which should be considered when selecting a firewall? (10 marks)
3. Explain the best practices of configuring a firewall on any network. (20 marks)

6.1 As an IT Security analyst working with “Triple X”, you will need to compile a report concerning the following:

a. In clear terms, describe the functions of a proxy firewall/proxy server. (4 Marks)

b. Highlight the technical (configuration) issues that may arise in deploying this design.

(8 Marks)

c. State the benefits and drawbacks of this implementation. (8 Marks)

7.1 Given the opportunity to increase your expertise on IDPS systems, develop a report that addresses the following questions using any resources you may find on the Web.

a. Classify IDPS systems according to detection methods and highlight the drawbacks associated with each of them. (20 Marks)

b. In tabular form, identify the common parameters that are used for comparative analysis of IDPS systems manufactured by various vendors, giving a simple description of each parameter. (8 Marks)

c. Also using a table and the common parameters defined in 7.1b, compare various types of IDPS System manufactured by various vendors that you may find on the web. ***Students must compare at least 8 types of IDPS System***.

**Chapter 8**

**Cryptography**

Given the message “**PEARSON INSTITUTE OF HIGHER EDUCATION, PREVIOUSLY KNOWN AS MGI**”:

a. Encrypt this message using a columnar transposition cipher with encryption keyword **“DRAIN”.** If necessary, pad the message with A’s. (8 Marks)

b. Decrypt the message **“NAC SMT NAA AOT KEP AOT BC”** which was encrypted using a columnar transposition cipher with encryption keyword **“PLAN”**. (10 Marks)

c. Encrypt the first two words of the message in 3.1 i.e. **“PEARSON INSTITUTE”** using a vernam cipher with the key **“UVFGTYI WRTPHJYIZ”.** Use a table to justify your answer.