(2 ½ Hours) **[Total Marks: 75]**

N.B. 1) All questions are compulsory.
2) Figures to the right indicate marks.
3) Illustrations, in-depth answers and diagrams will be appreciated.
4) Mixing of sub-questions is not allowed.

Q. 1 **Attempt ANY FOUR from the following:** **(20M)**
(a) What is an Active Attack in network security? Explain any three types of active attacks in detail.
(b) What is Computer Security and discuss its objectives?
(c) Apply the Caesar cipher to encrypt "HELLO WORLD" with key 3 and decrypt it back to the original message.
(d) Write a short note on AES.
(e) Explain Monoalphabetic substitution with an example.
(f) Differentiate between stream cipher and block cipher.

Q. 2 **Attempt ANY FOUR from the following:** **(20M)**
(a) Describe how Public-Key Infrastructure (PKI) helps in secure communications?
(b) Write a short note on Kerberos.
(c) What is HMAC? How it works?
(d) Explain the Diffie-Hellman key exchange algorithm with an example.
(e) Define a Digital Signature and describe how it works?
(f) Explain the various fields of an X.509 certificate.

Q. 3 **Attempt ANY FOUR from the following:** **(20M)**
(a) Write a short note on packet filtering firewall.
(b) Describe how PGP secures email messages and discuss its main features.
(c) What is a DDoS attack? Explain its working and impact.
(d) Explain the different techniques of Intrusion Detection Systems.
(e) Explain the key components of IPSec.
(f) Describe the purpose and main features of the Secure Electronic Transaction protocol.

Q. 4 **Attempt ANY FIVE from the following:** **(15M)**
(a) What is SSL? Describe its working mechanism.
(b) Differentiate between Cryptography and Steganography.
(c) What is Virus? Describe different types of Viruses.
(d) Compare S/MIME and PGP in email security.
(e) Discuss the role of firewalls in protecting organizational networks.
(f) Define an intruder and intrusion.

****

muquestionpapers.com