(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) Describe the symmetric cipher model with a neat diagram.
(b) Define security services and list any four services provided by network security.
(c) Differentiate between active and passive security attacks.
(d) Using the Playfair cipher of the 5x5 matrix, encrypt the plaintext "HELLO" using the keyword "MONARCHY".
(e) Explain steps of the RSA algorithm with an example.
(f) What is steganography? Explain how it is used to protect information.

Q. 2 **Attempt ANY FOUR from the following:** **(20M)**

(a) Explain the working principle of a public-key cryptosystem.
(b) Describe the steps involved in the Diffie-Hellman key exchange with a simple numerical example.
(c) Explain the concept of HMAC and its advantages over normal hash functions.
(d) How are digital signatures generated and verified using public-key cryptography?
(e) What are the key components of an X.509 certificate?
(f) What are the limitations of Kerberos and Public Key Infrastructure in modern networks?

Q. 3 **Attempt ANY FOUR from the following:** **(20M)**

(a) What is IPSec, and what are its main components?
(b) Explain common intrusion techniques used by attackers.
(c) Explain the working of PGP (Pretty Good Privacy) with a neat diagram.
(d) Define malicious software and list types of malware.
(e) Describe the operation of a packet-filtering firewall with an example.
(f) Explain the working of S/MIME for securing email communication.

Q. 4 **Attempt ANY FIVE from the following:** **(15M)**

(a) Define terms : i) Cryptanalysis ii) Avalanche Effect iii) Encryption
(b) Encrypt the message "Secure the documents" using the **Rail Fence Cipher** with depth 3.
(c) Explain the use of ticket-granting tickets (TGT) in Kerberos authentication.
(d) Discuss any three security requirements of a good hash function.
(e) State any three advantages of using a firewall.
(f) Explain virus countermeasures to prevent infection.

****