[Time:2.30 Hrs] **[Marks:75]**

Please check whether you have got the right question paper.

N.B: **1. All question are compulsory.**
2. Figures to the right indicate full marks.

Q.1 **Attempt any Four of the following:** **20**

a. What are the current trends in cybersecurity, and how do they impact organizations?
b. What is the OSI Security Architecture, and how does it relate to the OSI model?
c. Define and differentiate between passive and active security attacks.
d. Discuss the role of encryption as a security mechanism.
e. What is steganography, and how is it used in data security?
f. Define stream ciphers and their characteristics.

Q.2 **Attempt any Four of the following:** **20**

a. What is key management in cryptography? why is it crucial for secure communication?
b. What are the primary goals of message authentication in cryptography?
c. How does a MAC differ from a digital signature?
d. Explain the HMAC (Hash-based Message Authentication Code)
e. Explain the role of X.509 certificates in Public Key Infrastructure (PKI).
f. Discuss the components of a PKI.

Q.3 **Attempt any Four of the following:** **20**

a. Explain the key components of PGP encryption.
b. What is IPSec, and how does it provide security at the IP layer?
c. Discuss the advantages and limitations of using PGP for email encryption.
d. What services does the Authentication Header (AH) provide?
e. What is an Electronic Mail Security? Prove an example.
f. Describe Authentication Header (AH) and Encapsulating Security Payload (ESP).

Q.4 **Attempt any Three of the following:** **15**

a. Explain the mathematical foundations of RSA.
b. Why is AES considered secure for modern encryption needs?
c. Write a short note on Kerberos.
d. Describe the process of generating and verifying a digital signature.
e. What is S/MIME, and how does it differ from PGP?
f. Explain the structure of an ESP packet.

*******END******