Code No: F-13920/N/BL/AICTE

FACULTY OF ENGINEERING

B.E. (I.T) VI - Semester (AICTE) (Main & Backlog) (New) Examination,
August / September 2024

Subject: Network Security and Cryptography

Time: 3 Hours Max. Marks: 70

Note: (i) First question is compulsory and answer any four questions from the remaining six questions. Each question carries 14 Marks.
(ii) Answer to each question must be written at one place only and in the same order as they occur in the question paper.
(iii) Missing data, if any, may be suitably assumed.

1. a) What are the different types of Security attacks?
   b) What is Security Mechanisms?
   c) Why it is important to study the Feistel Cipher Architecture?
   d) Difference between HMAC and CMAC cryptographic techniques.
   e) What is the role of Ticket Granting Server in inter realm operations of Kerberos?
   f) Define Secure Shell (SSH).
   g) What is Handshake protocol in SSL?

2. a) Explain about Ceasier cipher and Playfair cipher with example.
   b) Compare and Contrast between Symmetric and Asymmetric key cryptography.

3. a) Explain RSA algorithm with example.
   b) How man in middle attack can be performed in Diffie Hellman algorithm?

4. a) Explain with diagram a single round function of SHA-512.
   b) Explain Kerberos realm.

5. a) What are the different phases of operation in IEEE 802.11i? Explain.
   b) Draw SSL protocol stack and explain SSL Record Protocol.

6. a) Explain the functionality of S/MIME.
   b) What is the requirement of IP security? Explain the architecture of IP security.

7. a) Discuss Blowfish algorithm.
   b) Describe X. 509 certificate format.
   c) What are approaches for Digital Signatures based on Public Key Encryption?

**